



3Com[®] Switch S7900E Family

Command Reference Guide

S7902E
S7903E
S7906E
S7906E-V
S7910

www.3Com.com
Part Number: 10016576 Rev. AA
Published: April 2008

3Com Corporation
350 Campus Drive
Marlborough, MA
USA 01752-3064

Copyright © 2006-2008, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

Cisco is a registered trademark of Cisco Systems, Inc.

Funk RADIUS is a registered trademark of Funk Software, Inc.

Aegis is a registered trademark of Aegis Group PLC.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

CONTENTS

ABOUT THIS GUIDE

Conventions	41
Related Documentation	41

1 LOGIN COMMANDS

activation-key	59
authentication-mode	60
auto-execute command	61
databits	62
display telnet client configuration	62
display user-interface	63
display users	64
escape-key	65
flow-control	66
free user-interface	66
history-command max-size	67
idle-timeout	67
lock	68
modem	69
modem auto-answer	69
modem timer answer	70
parity	70
protocol inbound	71
screen-length	71
send	72
service-type	73
set authentication password	74
shell	75
speed	75
stopbits	76
sysname	77
telnet	77
telnet ipv6	78
telnet client source	78
telnet server enable	79
terminal type	80
user-interface	80
user privilege level	81

2 USER LOGIN COMMANDS

acl 83
snmp-agent community 83
snmp-agent group 84
snmp-agent usm-user 85

3 ETHERNET PORT CONFIGURATION COMMANDS

broadcast-suppression 89
description 90
display brief interface 90
display interface 92
display loopback-detection 94
display port-group manual 95
display storm-constrain 96
duplex 97
flow-control 97
flow-interval 98
group-member 98
interface 99
jumboframe enable 99
link-delay 100
loopback 101
loopback-detection control enable 101
loopback-detection enable 102
loopback-detection interval-time 103
loopback-detection per-vlan enable 103
mdi 104
multicast-suppression 105
port-group 106
reset counters interface 106
shutdown 107
speed 107
storm-constrain 108
storm-constrain control 109
storm-constrain enable log 110
storm-constrain enable trap 110
storm-constrain interval 111
unicast-suppression 111

4 PORT ISOLATION CONFIGURATION COMMANDS

display port-isolate group 113
port-isolate enable 113

5 MAC ADDRESS TABLE CONFIGURATION COMMANDS

display mac-address 115
display mac-address aging-time 116

display mac-address mac-learning 116
mac-address 117
mac-address 118
mac-address mac-learning disable 119
mac-address max-mac-count 120
mac-address timer 121

6 VLAN CONFIGURATION COMMANDS

description 123
display interface Vlan-interface 123
display vlan 124
interface Vlan-interface 125
ip address 126
shutdown 127
vlan 128

7 PORT-BASED VLAN CONFIGURATION COMMANDS

port 129
port access vlan 129
port hybrid pvid vlan 130
port hybrid vlan 131
port link-type 132
port trunk permit vlan 133
port trunk pvid vlan 133

8 PROTOCOL-BASED VLAN CONFIGURATION COMMANDS

display protocol-vlan interface 135
display protocol-vlan vlan 135
port hybrid protocol-vlan 136
protocol-vlan 137

9 IP-SUBNET-BASED VLAN CONFIGURATION COMMANDS

display ip-subnet-vlan interface 141
display ip-subnet-vlan vlan 141
ip-subnet-vlan 142
port hybrid ip-subnet-vlan vlan 143

10 ISOLATE-USER-VLAN CONFIGURATION COMMANDS

display isolate-user-vlan 145
isolate-user-vlan 146
isolate-user-vlan enable 147

11 VOICE VLAN CONFIGURATION COMMANDS

display voice vlan oui 149

display voice vlan state 149
voice vlan 150
voice vlan aging 151
voice vlan enable 151
voice vlan mac-address 152
voice vlan mode auto 154
voice vlan security enable 154

12 QINQ CONFIGURATION COMMANDS

classifier behavior 157
if-match customer-vlan-id 157
nest top-most vlan-id 158
qinq enable 158
qinq ethernet-type customer-tag 159
qinq ethernet-type service-tag 160
qos apply policy 161
qos policy 161
traffic behavior 162
traffic classifier 162

13 BPDU TUNNELING CONFIGURATION COMMANDS

bpdu-tunnel dot1q stp 165
bpdu-tunnel dot1q enable 166
bpdu-tunnel tunnel-dmac 167

14 MSTP CONFIGURATION COMMANDS

active region-configuration 169
check region-configuration 169
display stp 170
display stp abnormal-port 172
display stp down-port 173
display stp history 174
display stp region-configuration 175
display stp root 175
display stp tc 176
instance 177
region-name 178
reset stp 178
revision-level 179
stp 179
stp bpdu-protection 180
stp bridge-diameter 181
stp compliance 182
stp config-digest-snooping 183
stp cost 183
stp edged-port 184

stp loop-protection 185
stp max-hops 186
stp mcheck 186
stp mode 187
stp no-agreement-check 188
stp pathcost-standard 188
stp point-to-point 189
stp port-log 190
stp port priority 191
stp priority 192
stp region-configuration 193
stp root primary 193
stp root secondary 194
stp root-protection 195
stp tc-protection 196
stp tc-protection threshold 196
stp timer forward-delay 197
stp timer hello 198
stp timer max-age 199
stp timer-factor 200
stp transmit-limit 200
vlan-mapping modulo 201

15 LINK AGGREGATION CONFIGURATION COMMANDS

display lacp system-id 203
display link-aggregation interface 203
display link-aggregation service-type 205
display link-aggregation summary 205
display link-aggregation verbose 206
lacp port-priority 208
lacp system-priority 208
link-aggregation group description 209
link-aggregation group mode 209
link-aggregation group service-type 210
port link-aggregation group 210
port-group aggregation 211
reset lacp statistics 211

16 GARP/GVRP CONFIGURATION COMMANDS

display garp statistics 213
display garp timer 213
garp timer 214
garp timer leaveall 215
reset garp statistics 216

17 GVRP CONFIGURATION COMMANDS

display gvrp local-vlan interface 217
display gvrp state 217
display gvrp statistics 218
display gvrp status 218
display gvrp vlan-operation interface 219
gvrp 219
gvrp registration 220

18 IP ADDRESSING CONFIGURATION COMMANDS

display ip interface 223
display ip interface brief 225
ip address 225

19 IP PERFORMANCE CONFIGURATION COMMANDS

display fib 227
display fib ip-address 229
display fib statistics 229
display icmp statistics 230
display ip socket 231
display ip statistics 232
display tcp statistics 233
display tcp status 235
display udp statistics 236
ip forward-broadcast 237
ip forward-broadcast 238
ip redirects enable 238
ip ttl-expires enable 239
ip unreachable enable 239
reset ip statistics 240
reset tcp statistics 240
reset udp statistics 240
tcp timer fin-timeout 241
tcp timer syn-timeout 241
tcp window 242

20 IP SOURCE GUARD COMMANDS

display ip check source 243
display user-bind 244
ip check source 245
user-bind 245

21 ROUTING OVERVIEW COMMANDS

display ip relay-route 247
display ip relay-tunnel 247

display ip routing-table 248
display ip routing-table acl 252
display ip routing-table ip-address 254
display ip routing-table ip-prefix 256
display ip routing-table protocol 257
display ip routing-table statistics 258
display ipv6 relay-route 259
display ipv6 relay-tunnel 259
display ipv6 routing-table 260
display ipv6 routing-table acl 261
display ipv6 routing-table ipv6-address 261
display ipv6 routing-table ipv6-address1 ipv6-address2 263
display ipv6 routing-table ipv6-prefix 263
display ipv6 routing-table protocol 264
display ipv6 routing-table statistics 265
display ipv6 routing-table verbose 265
reset ip routing-table statistics protocol 266
reset ipv6 routing-table statistics 267

22 STATIC ROUTING CONFIGURATION COMMANDS

delete static-routes all 269
ip route-static 269
ip route-static default-preference 271

23 RIP CONFIGURATION COMMANDS

checkzero 273
default cost 273
default-route originate 274
display rip 275
display rip database 276
display rip interface 277
display rip route 278
filter-policy export 279
filter-policy import 280
host-route 281
import-route 282
maximum load-balancing 283
network 283
peer 284
preference 284
reset rip statistics 285
rip 285
rip authentication-mode 286
rip input 287
rip metricin 287
rip metricout 288
rip mib-binding 288

- rip output 289
- rip poison-reverse 289
- rip split-horizon 290
- rip summary-address 290
- rip version 291
- silent-interface 292
- summary 293
- timers 293
- validate-source-address 294
- version 295

24 OSPF CONFIGURATION COMMANDS

- abr-summary 297
- area 298
- asbr-summary 298
- authentication-mode 299
- bandwidth-reference 300
- default 300
- default-cost 301
- default-route-advertise 302
- description 303
- display ospf abr-asbr 303
- display ospf asbr-summary 304
- display ospf brief 305
- display ospf cumulative 307
- display ospf error 308
- display ospf interface 310
- display ospf lsdb 311
- display ospf nexthop 313
- display ospf peer 313
- display ospf peer statistics 315
- display ospf request-queue 316
- display ospf retrans-queue 317
- display ospf routing 318
- display ospf vlink 319
- enable log 320
- filter 320
- filter-policy export 321
- filter-policy import 322
- host-advertise 322
- import-route 323
- log-peer-change 324
- lsa-arrival-interval 325
- lsa-generation-interval 325
- lsdb-overflow-limit 326
- maximum load-balancing 327
- maximum-routes 327

- network 328
- nssa 328
- ospf 329
 - ospf authentication-mode 330
 - ospf cost 331
 - ospf dr-priority 332
 - ospf mib-binding 332
 - ospf mtu-enable 333
 - ospf network-type 334
 - ospf timer dead 335
 - ospf timer hello 335
 - ospf timer poll 336
 - ospf timer retransmit 336
 - ospf trans-delay 337
- peer 338
- preference 338
- reset ospf counters 339
- reset ospf process 339
- reset ospf redistribution 340
- rfc1583 compatible 340
- silent-interface 341
- snmp-agent trap enable ospf 341
- spf-schedule-interval 343
- stub 344
- stub-router 344
- vlink-peer 345

25 IS-IS CONFIGURATION COMMANDS

- area-authentication-mode 347
- auto cost enable 348
- bandwidth-reference 348
- circuit-cost 349
- cost-style 350
- default-route-advertise 351
- display isis brief 352
- display isis interface 353
- display isis license 354
- display isis lsdb 356
- display isis mesh-group 357
- display isis name-table 357
- display isis peer 358
- display isis route 359
- display isis spf-log 360
- display isis statistics 361
- domain-authentication-mode 362
- filter-policy export 363
- filter-policy import 365

flash-flood 365
import-route 366
import-route isis level-2 into level-1 368
isis 368
isis authentication-mode 369
isis circuit-level 370
isis circuit-type 371
isis cost 371
isis dis-name 372
isis dis-priority 373
isis enable 373
isis mesh-group 374
isis silent 375
isis small-hello 375
isis timer csnp 376
isis timer hello 377
isis timer holding-multiplier 377
isis timer lsp 378
isis timer retransmit 379
is-level 380
is-name 380
is-name map 381
is-snmp-traps enable 381
log-peer-change 382
lsp-fragments-extend 382
lsp-length originate 383
lsp-length receive 384
maximum load-balancing 384
network-entity 385
preference 386
reset isis all 386
reset isis peer 387
set-overload 387
spf-slice-size 388
summary 389
timer isp-generation 390
timer lsp-max-age 391
timer lsp-refresh 392
timer spf 392
virtual-system 393

26 BGP CONFIGURATION COMMANDS

aggregate 395
balance 396
bestroute as-path-neglect 397
bestroute compare-med 397
bestroute med-confederation 398

- bgp 398
 - compare-different-as-med 399
 - confederation id 399
 - confederation nonstandard 400
 - confederation peer-as 401
 - dampening 401
 - default ipv4-unicast 402
 - default local-preference 403
 - default med 403
 - default-route imported 404
 - display bgp group 405
 - display bgp network 406
 - display bgp paths 406
 - display bgp peer 407
 - display bgp routing-table 409
 - display bgp routing-table as-path-acl 410
 - display bgp routing-table cidr 410
 - display bgp routing-table community 411
 - display bgp routing-table community-list 412
 - display bgp routing-table dampened 412
 - display bgp routing-table dampening parameter 413
 - display bgp routing-table different-origin-as 414
 - display bgp routing-table flap-info 414
 - display bgp routing-table peer 415
 - display bgp routing-table regular-expression 416
 - display bgp routing-table statistic 416
 - ebgp-interface-sensitive 417
 - filter-policy export 417
 - filter-policy import 418
 - group 419
 - import-route 419
 - log-peer-change 420
 - network 420
 - peer advertise-community 421
 - peer advertise-ext-community 422
 - peer allow-as-loop 422
 - peer as-number 423
 - peer as-path-acl 424
 - peer capability-advertise conventional 424
 - peer capability-advertise route-refresh 425
 - peer connect-interface 425
 - peer default-route-advertise 426
 - peer description 427
 - peer ebgp-max-hop 427
 - peer enable 428
 - peer fake-as 429
 - peer filter-policy 429
 - peer group 430

peer ignore 430
peer ip-prefix 431
peer keep-all-routes 432
peer log-change 432
peer next-hop-local 433
peer password 433
peer preferred-value 434
peer public-as-only 435
peer reflect-client 436
peer route-limit 436
peer route-policy 437
peer route-update-interval 438
peer substitute-as 438
peer timer 439
preference 439
reflect between-clients 440
reflector cluster-id 441
refresh bgp 441
reset bgp 442
reset bgp dampening 443
reset bgp flap-info 443
reset bgp ipv4 all 444
router-id 444
summary automatic 445
synchronization 445
timer 446

27 ROUTING POLICY COMMON CONFIGURATION COMMANDS

apply as-path 447
apply comm-list delete 448
apply community 448
apply cost 449
apply cost-type 450
apply extcommunity 450
apply isis 451
apply local-preference 452
apply origin 452
apply preference 453
apply preferred-value 454
apply tag 454
display ip as-path 455
display ip community-list 455
display ip extcommunity-list 456
display route-policy 456
if-match as-path 457
if-match community 458
if-match cost 458

if-match extcommunity 459
if-match interface 460
if-match route-type 460
if-match tag 461
ip as-path 462
ip community-list 463
ip extcommunity-list 464
route-policy 464

28 IPv4 ROUTING POLICY CONFIGURATION COMMANDS

apply ip-address next-hop 467
display ip ip-prefix 467
if-match acl 468
if-match ip 469
if-match ip-prefix 469
ip ip-prefix 470
reset ip ip-prefix 471

29 IPv6 STATIC ROUTING CONFIGURATION COMMANDS

delete ipv6 static-routes all 473
ipv6 route-static 473

30 IPv6 RIPNG CONFIGURATION COMMANDS

checkzero 475
default cost 475
display ripng 476
display ripng database 477
display ripng interface 478
display ripng route 479
filter-policy export 479
filter-policy import 480
import-route 481
maximum load-balancing 481
preference 482
ripng 483
ripng default-route 483
ripng enable 484
ripng metricin 485
ripng metricout 485
ripng poison-reverse 486
ripng split-horizon 486
ripng summary-address 487
timers 487

31 IPv6 OSPFV3 CONFIGURATION COMMANDS

abr-summary 489
area 490
default cost 490
default-cost 491
display ospfv3 491
display ospfv3 interface 493
display ospfv3 lsdb 494
display ospfv3 lsdb statistic 496
display ospfv3 next-hop 497
display ospfv3 peer 497
display ospfv3 peer statistic 499
display ospfv3 request-list 500
display ospfv3 retrans-list 501
display ospfv3 routing 503
display ospfv3 statistic 504
display ospfv3 topology 505
display ospfv3 vlink 506
filter-policy export 506
filter-policy import 507
import-route 508
log-peer-change 509
maximum load-balancing 510
ospfv3 510
ospfv3 area 511
ospfv3 cost 511
ospfv3 dr-priority 512
ospfv3 mtu-ignore 512
ospfv3 timer dead 513
ospfv3 timer hello 514
ospfv3 timer retransmit 514
ospfv3 trans-delay 515
preference 515
router-id 516
silent-interface 517
spf timers 517
stub 518
vlink-peer 519

32 IPv6 IS-IS CONFIGURATION COMMANDS

display isis route ipv6 521
ipv6 default-route-advertise 523
ipv6 enable 523
ipv6 filter-policy export 524
ipv6 filter-policy import 525
ipv6 import-route 526
ipv6 import-route isisv6 level-2 into level-1 527

ipv6 maximum load-balancing 527
ipv6 preference 528
ipv6 summary 529
isis ipv6 enable 529

33 IPv6 BGP CONFIGURATION COMMANDS

balance 531
bestroute as-path-neglect 531
bestroute compare-med 532
bestroute med-confederation 532
compare-different-as-med 533
dampening 534
default local-preference 535
default med 535
default-route imported 536
display bgp ipv6 group 536
display bgp ipv6 network 537
display bgp ipv6 paths 538
display bgp ipv6 peer 539
display bgp ipv6 routing-table 540
display bgp ipv6 routing-table as-path-acl 541
display bgp ipv6 routing-table community 542
display bgp ipv6 routing-table community-list 543
display bgp ipv6 routing-table dampened 543
display bgp ipv6 routing-table dampening parameter 544
display bgp ipv6 routing-table different-origin-as 544
display bgp ipv6 routing-table flap-info 545
display bgp ipv6 routing-table peer 546
display bgp ipv6 routing-table regular-expression 547
display bgp ipv6 routing-table statistic 547
filter-policy export 548
filter-policy import 548
group 549
import-route 550
ipv6-family 550
network 551
peer advertise-community 552
peer advertise-ext-community 552
peer allow-as-loop 553
peer as-number 553
peer as-path-acl 554
peer capability-advertise route-refresh 555
peer connect-interface 555
peer default-route-advertise 556
peer description 557
peer ebgp-max-hop 557
peer fake-as 558

- peer filter-policy 558
- peer group 559
- peer ignore 560
- peer ipv6-prefix 560
- peer keep-all-routes 561
- peer log-change 562
- peer next-hop-local 562
- peer preferred-value 563
- peer public-as-only 564
- peer reflect-client 564
- peer route-limit 565
- peer route-policy 565
- peer route-update-interval 566
- peer substitute-as 567
- peer timer 567
- preference 568
- reflect between-clients 569
- reflector cluster-id 570
- refresh bgp ipv6 570
- reset bgp ipv6 571
- reset bgp ipv6 dampening 571
- reset bgp ipv6 flap-info 572
- router-id 572
- synchronization 573
- timer 574

34 IPV6 ROUTING POLICY CONFIGURATION COMMANDS

- apply ipv6 next-hop 575
- display ip ipv6-prefix 575
- if-match ipv6 576
- ip ipv6-prefix 577
- reset ip ipv6-prefix 578

35 IPV6 BASICS CONFIGURATION COMMANDS

- display dns ipv6 dynamic-host 579
- display dns ipv6 server 579
- display ipv6 fib 580
- display ipv6 host 581
- display ipv6 interface 582
- display ipv6 neighbors 583
- display ipv6 neighbors count 585
- display ipv6 pathmtu 585
- display ipv6 socket 586
- display ipv6 statistics 587
- display tcp ipv6 statistics 590
- display tcp ipv6 status 592

display udp ipv6 statistics 593
dns server ipv6 594
ipv6 594
ipv6 address 595
ipv6 address auto link-local 595
ipv6 address eui-64 596
ipv6 address link-local 596
ipv6 host 597
ipv6 icmp-error 597
ipv6 icmpv6 multicast-echo-reply enable 598
ipv6 nd autoconfig managed-address-flag 598
ipv6 nd autoconfig other-flag 599
ipv6 nd dad attempts 599
ipv6 nd hop-limit 600
ipv6 nd ns retrans-timer 600
ipv6 nd nud reachable-time 601
ipv6 nd ra halt 602
ipv6 nd ra interval 602
ipv6 nd ra prefix 603
ipv6 nd ra router-lifetime 604
ipv6 neighbor 604
ipv6 neighbors max-learning-num 605
ipv6 pathmtu 606
ipv6 pathmtu age 606
reset dns ipv6 dynamic-host 607
reset ipv6 neighbors 607
reset ipv6 pathmtu 607
reset ipv6 statistics 608
reset tcp ipv6 statistics 608
reset udp ipv6 statistics 608
tcp ipv6 timer fin-timeout 609
tcp ipv6 timer syn-timeout 609
tcp ipv6 window 610

36 IPv6 Dual Stack Configuration Commands

ipv6 611
ipv6 address 611
ipv6 address auto link-local 612
ipv6 address eui-64 612
ipv6 address link-local 613

37 IPv6 Tunneling Configuration Commands

aggregation-group 615
destination 616
display interface tunnel 617
display ipv6 interface tunnel 618
interface tunnel 619

mtu 619
source 620
tunnel-protocol 621

38 IGMP SNOOPING CONFIGURATION COMMANDS

display igmp-snooping group 623
display igmp-snooping statistics 624
drop-unknown 625
fast-leave 625
group-policy 626
host-aging-time 627
igmp-snooping 628
igmp-snooping drop-unknown 628
igmp-snooping enable 629
igmp-snooping fast-leave 629
igmp-snooping general-query source-ip 630
igmp-snooping group-limit 631
igmp-snooping group-policy 632
igmp-snooping host-aging-time 633
igmp-snooping host-join 633
igmp-snooping last-member-query-interval 635
igmp-snooping max-response-time 635
igmp-snooping overflow-replace 636
igmp-snooping querier 637
igmp-snooping query-interval 637
igmp-snooping router-aging-time 638
igmp-snooping source-deny 638
igmp-snooping special-query source-ip 639
igmp-snooping static-group 640
igmp-snooping static-router-port 641
igmp-snooping version 641
last-member-query-interval 642
max-response-time 642
overflow-replace 643
report-aggregation 644
reset igmp-snooping group 644
reset igmp-snooping statistics 645
router-aging-time 645
source-deny 646

39 MULTICAST VLAN CONFIGURATION COMMANDS

display multicast-vlan 647
multicast-vlan enable 647
multicast-vlan subvlan 648

40 IGMP CONFIGURATION COMMANDS

- display igmp group 651
- display igmp group port-info 652
- display igmp interface 653
- display igmp routing-table 654
- fast-leave 655
- igmp 656
- igmp enable 656
- igmp fast-leave 657
- igmp group-policy 658
- igmp last-member-query-interval 659
- igmp max-response-time 659
- igmp require-router-alert 660
- igmp robust-count 660
- igmp send-router-alert 661
- igmp static-group 662
- igmp timer other-querier-present 663
- igmp timer query 663
- igmp version 664
- last-member-query-interval 664
- max-response-time 665
- require-router-alert 665
- reset igmp group 666
- reset igmp group port-info 667
- robust-count 668
- send-router-alert 668
- timer other-querier-present 669
- timer query 670
- version 670

41 PIM CONFIGURATION COMMANDS

- auto-rp enable 671
- bsr-policy 671
- c-bsr 672
- c-bsr admin-scope 673
- c-bsr global 673
- c-bsr group 674
- c-bsr hash-length 675
- c-bsr holdtime 675
- c-bsr interval 676
- c-bsr priority 676
- c-rp 677
- c-rp advertisement-interval 678
- c-rp holdtime 679
- crp-policy 679
- display pim bsr-info 680
- display pim claimed-route 681

display pim control-message counters 682
display pim grafts 683
display pim interface 684
display pim join-prune 686
display pim neighbor 687
display pim routing-table 688
display pim rp-info 690
hello-option dr-priority 691
hello-option holdtime 692
hello-option lan-delay 692
hello-option neighbor-tracking 693
hello-option override-interval 693
holdtime assert 694
holdtime join-prune 695
jp-pkt-size 695
jp-queue-size 696
pim 696
pim bsr-boundary 697
pim dm 697
pim hello-option dr-priority 698
pim hello-option holdtime 698
pim hello-option lan-delay 699
pim hello-option neighbor-tracking 700
pim hello-option override-interval 700
pim holdtime assert 701
pim holdtime join-prune 701
pim require-genid 702
pim sm 702
pim state-refresh-capable 703
pim timer graft-retry 703
pim timer hello 704
pim timer join-prune 704
pim triggered-hello-delay 705
probe-interval 705
register-policy 706
register-suppression-timeout 706
register-whole-checksum 707
reset pim control-message counters 707
source-lifetime 708
source-policy 708
spt-switch-threshold 709
ssm-policy 710
state-refresh-interval 711
state-refresh-rate-limit 711
state-refresh-ttl 712
static-rp 712
timer hello 713
timer join-prune 714

42 MSDP CONFIGURATION COMMANDS

cache-sa-enable 715
display msdp brief 715
display msdp peer-status 716
display msdp sa-cache 718
display msdp sa-count 719
encap-data-enable 720
import-source 721
msdp 721
originating-rp 722
peer connect-interface 722
peer description 723
peer mesh-group 724
peer minimum-ttl 724
peer request-sa-enable 725
peer sa-cache-maximum 725
peer sa-policy 726
peer sa-request-policy 727
reset msdp peer 728
reset msdp sa-cache 728
reset msdp statistics 728
shutdown 729
static-rpf-peer 729
timer retry 730

43 MULTICAST ROUTING CONFIGURATION COMMANDS

display multicast boundary 733
display multicast forwarding-table 734
display multicast routing-table 736
display multicast routing-table static 737
display multicast rpf-info 738
ip rpf-route-static 739
mtracert 740
multicast boundary 742
multicast forwarding-table downstream-limit 743
multicast forwarding-table route-limit 743
multicast load-splitting 744
multicast longest-match 744
multicast routing-enable 745
reset multicast forwarding-table 745
reset multicast routing-table 746

44 802.1X CONFIGURATION COMMANDS

display dot1x 749
dot1x 751
dot1x authentication-method 752

dot1x guest-vlan 753
dot1x handshake 755
dot1x max-user 755
dot1x multicast-trigger 756
dot1x port-control 757
dot1x port-method 758
dot1x quiet-period 759
dot1x retry 759
dot1x supp-proxy-check 760
dot1x timer 761
reset dot1x statistics 763

45 EAD FAST DEPLOYMENT CONFIGURATION COMMANDS

dot1x free-ip 765
dot1x timer ead-timeout 766
dot1x url 766

46 MAC AUTHENTICATION CONFIGURATION COMMANDS

display mac-authentication 769
mac-authentication 770
mac-authentication domain 771
mac-authentication timer 772
mac-authentication user-name-format 773
reset mac-authentication statistics 774

47 AAA CONFIGURATION COMMANDS

access-limit 775
accounting default 775
accounting lan-access 777
accounting login 777
accounting optional 778
accounting portal 779
attribute 780
authentication default 781
authentication lan-access 782
authentication login 783
authentication portal 783
authorization command 784
authorization default 785
authorization lan-access 786
authorization login 787
authorization portal 788
cut connection 788
display connection 789
display domain 790
display local-user 792

- domain 793
- domain default 794
- idle-cut 794
- level 795
- local-user 796
- local-user password-display-mode 796
- password 797
- self-service-url 798
- service-type 799
- service-type ftp 800
- state 800
- work-directory 801

48 RADIUS CONFIGURATION COMMANDS

- data-flow-format 803
- display radius scheme 803
- display radius statistics 805
- display stop-accounting-buffer 807
- key 808
- nas-ip 809
- primary accounting 810
- primary authentication 810
- radius client 811
- radius nas-ip 812
- radius scheme 813
- radius trap 813
- reset radius statistics 814
- reset stop-accounting-buffer 814
- retry 815
- retry realtime-accounting 816
- retry stop-accounting 817
- secondary accounting 818
- secondary authentication 818
- security-policy-server 819
- server-type 820
- state 820
- stop-accounting-buffer enable 821
- timer quiet 822
- timer realtime-accounting 823
- timer response-timeout 823
- user-name-format 824

49 HWTACACS CONFIGURATION COMMANDS

- data-flow-format 827
- display hwtacacs 827
- display stop-accounting-buffer 829
- hwtacacs nas-ip 829

- hwtacacs scheme 830
- key 831
- nas-ip 831
- primary accounting 832
- primary authentication 833
- primary authorization 834
- reset hwtacacs statistics 834
- reset stop-accounting-buffer 835
- retry stop-accounting 835
- secondary accounting 836
- secondary authentication 837
- secondary authorization 837
- stop-accounting-buffer enable 838
- timer quiet 839
- timer realtime-accounting 839
- timer response-timeout 840
- user-name-format 841

50 WEB AUTHENTICATION CONFIGURATION COMMANDS

- display portal acl 843
- display portal connection statistics 844
- display portal free-rule 846
- display portal interface 847
- display portal server 848
- display portal server statistics 849
- display portal tcp-cheat statistics 850
- display portal user 851
- portal auth-network 852
- portal delete-user 853
- portal free-rule 853
- portal server 854
- portal server method 855
- reset portal connection statistics 856
- reset portal server statistics 856
- reset portal tcp-cheat statistics 857

51 SSH CONFIGURATION COMMANDS

- display public-key local 859
- display public-key peer 860
- display sftp client source 861
- display ssh client source 861
- display ssh server 862
- display ssh server-info 863
- display ssh user-information 863
- peer-public-key end 864
- public-key-code begin 864

public-key-code end 865
public-key local create 866
public-key local destroy 866
public-key local export rsa 867
public-key peer 868
public-key peer import sshkey 868
sftp 869
sftp client ipv6 source 870
sftp client source 870
sftp ipv6 871
sftp server enable 872
sftp server idle-timeout 872
ssh client authentication server 873
ssh client first-time enable 873
ssh client ipv6 source 874
ssh client source 875
ssh server authentication-retries 875
ssh server authentication-timeout 876
ssh server compatible-ssh1x enable 876
ssh server enable 877
ssh server rekey-interval 877
ssh user 878
ssh2 879
ssh2 ipv6 880

52 ARP CONFIGURATION COMMANDS

arp max-learning-num 883
arp static 883
arp timer aging 884
display arp 885
display arp ip-address 886
display arp timer aging 887
naturemask-arp enable 887
reset arp 887

53 GRATUITOUS ARP CONFIGURATION COMMANDS

gratuitous-arp-sending enable 889
gratuitous-arp-learning enable 889

54 ARP SOURCE SUPPRESSION CONFIGURATION COMMANDS

arp source-suppression enable 891
arp source-suppression limit 891
display arp source-suppression 892

55 ARP SPOOFING PROTECTION CONFIGURATION COMMANDS

arp resolving-route enable 893

56 PROXY ARP CONFIGURATION COMMANDS

proxy-arp enable 895

local-proxy-arp enable 895

display proxy-arp 896

display local-proxy-arp 896

57 DHCP SERVER CONFIGURATION COMMANDS

bims-server 897

bootfile-name 898

dhcp enable 898

dhcp select server global-pool 899

dhcp server detect 899

dhcp server forbidden-ip 900

dhcp server ip-pool 900

dhcp server ping packets 901

dhcp server ping timeout 901

dhcp server relay information enable 902

display dhcp server conflict 902

display dhcp server expired 903

display dhcp server free-ip 904

display dhcp server forbidden-ip 904

display dhcp server ip-in-use 904

display dhcp server statistics 905

display dhcp server tree 906

dns-list 908

domain-name 908

expired 909

gateway-list 909

nbns-list 910

netbios-type 911

network 911

option 912

reset dhcp server conflict 913

reset dhcp server ip-in-use 913

reset dhcp server statistics 914

static-bind client-identifier 914

static-bind ip-address 915

static-bind mac-address 916

tftp-server domain-name 917

tftp-server ip-address 917

voice-config 918

58 DHCP RELAY AGENT CONFIGURATION COMMANDS

dhcp enable 921
dhcp relay address-check 921
dhcp relay information enable 922
dhcp relay information format 922
dhcp relay information strategy 923
dhcp relay release 924
dhcp relay security static 924
dhcp relay security tracker 925
dhcp relay server-detect 926
dhcp relay server-group 926
dhcp relay server-select 927
dhcp select relay 927
display dhcp relay 928
display dhcp relay security 928
display dhcp relay security statistics 929
display dhcp relay security tracker 930
display dhcp relay server-group 930
display dhcp relay statistics 931
reset dhcp relay statistics 932

59 DHCP CLIENT CONFIGURATION COMMANDS

display dhcp client 933
ip address dhcp-alloc 934

60 DHCP SNOOPING CONFIGURATION COMMANDS

dhcp-snooping 937
dhcp-snooping information enable 938
dhcp-snooping information format 938
dhcp-snooping information strategy 939
dhcp-snooping trust 940
display dhcp-snooping 940
display dhcp-snooping trust 941
reset dhcp-snooping 941

61 COMMON ACL CONFIGURATION COMMANDS

display acl resource 943
display time-range 944
time-range 945

62 IPV4 ACL CONFIGURATION COMMANDS

acl 947
acl copy 948
acl name 949
description 950

- display acl 950
- reset acl counter 951
- rule 952
- rule 953
- rule 957
- rule comment 958
- step 959

63 IPv6 ACL CONFIGURATION COMMANDS

- acl ipv6 961
- acl ipv6 copy 962
- acl ipv6 name 963
- description 964
- display acl ipv6 964
- reset acl ipv6 counter 965
- rule 966
- rule 967
- rule comment 970
- step 971

64 BANDWIDTH MANAGEMENT CONFIGURATION COMMANDS

- display qos lr interface 973
- qos lr outbound 973

65 QOS TRAFFIC CLASSES CONFIGURATION COMMANDS

- display traffic classifier 975
- if-match 975
- traffic classifier 978

66 TRAFFIC BEHAVIOR CONFIGURATION COMMANDS

- accounting 981
- car 981
- display traffic behavior 983
- filter 984
- nest 984
- redirect 985
- remark customer-vlan-id 985
- remark dot1p 986
- remark drop-precedence 987
- remark dscp 987
- remark ip-precedence 988
- remark local-precedence 989
- remark service-vlan-id 989
- traffic behavior 990

67 QoS POLICY CONFIGURATION COMMANDS

classifier behavior 991
display qos policy 991
display qos policy global 992
display qos policy interface 993
display qos vlan-policy 994
qos apply policy 995
qos apply policy global 997
qos policy 997
qos vlan-policy 998
reset qos policy global 999
reset qos vlan-policy 999

68 CONGESTION MANAGEMENT CONFIGURATION COMMANDS

display qos sp interface 1001
display qos wrr interface 1001
qos sp 1002
qos wrr 1003

69 PRIORITY MAPPING TABLE CONFIGURATION COMMANDS

display qos map-table 1005
qos map-table 1006
import 1006

70 PORT PRIORITY CONFIGURATION COMMANDS

qos priority 1009

71 PORT PRIORITY TRUST MODE CONFIGURATION COMMANDS

display qos trust interface 1011
qos trust 1011

72 TRAFFIC MIRRORING CONFIGURATION COMMANDS

mirror-to 1013

73 PORT MIRRORING CONFIGURATION COMMANDS

display mirroring-group 1015
mirroring-group 1016
mirroring-group mirroring-port 1017
mirroring-group monitor-egress 1018
mirroring-group monitor-port 1019
mirroring-group remote-probe vlan 1020
mirroring-port 1020
monitor-port 1021

74 SNMP CONFIGURATION COMMANDS

display snmp-agent local-switch fabricid 1023
display snmp-agent community 1023
display snmp-agent group 1024
display snmp-agent mib-view 1025
display snmp-agent statistics 1026
display snmp-agent sys-info 1027
display snmp-agent trap-list 1028
display snmp-agent usm-user 1029
enable snmp trap updown 1029
snmp-agent calculate-password 1030
snmp-agent 1031
snmp-agent community 1031
snmp-agent group 1032
snmp-agent local-switch fabricid 1033
snmp-agent log 1034
snmp-agent mib-view 1035
snmp-agent packet max-size 1035
snmp-agent sys-info 1036
snmp-agent target-host 1037
snmp-agent trap enable 1038
snmp-agent trap if-mib link extended 1039
snmp-agent trap life 1040
snmp-agent trap queue-size 1041
snmp-agent trap source 1041
snmp-agent usm-user { v1 | v2c } 1042
snmp-agent usm-user v3 1043

75 RMON CONFIGURATION COMMANDS

display rmon alarm 1047
display rmon event 1048
display rmon eventlog 1048
display rmon history 1049
display rmon prialarm 1050
display rmon statistics 1051
rmon alarm 1053
rmon event 1054
rmon history 1055
rmon prialarm 1056
rmon statistics 1058

76 NTP CONFIGURATION COMMANDS

display ntp-service sessions 1061
display ntp-service status 1062
display ntp-service trace 1063
ntp-service access 1064

ntp-service authentication enable 1065
ntp-service authentication-keyid 1065
ntp-service broadcast-client 1066
ntp-service broadcast-server 1066
ntp-service in-interface disable 1067
ntp-service max-dynamic-sessions 1068
ntp-service multicast-client 1068
ntp-service multicast-server 1069
ntp-service refclock-master 1069
ntp-service reliable authentication-keyid 1070
ntp-service source-interface 1070
ntp-service unicast-peer 1071
ntp-service unicast-server 1072

77 DNS CONFIGURATION COMMANDS

display dns domain 1075
display dns dynamic-host 1075
display dns proxy table 1076
display dns server 1077
display ip host 1077
dns domain 1078
dns proxy enable 1078
dns resolve 1079
dns server 1079
ip host 1080
reset dns dynamic-host 1080

78 FILE SYSTEM CONFIGURATION COMMANDS

cd 1083
copy 1083
delete 1084
dir 1084
execute 1085
file prompt 1086
fixdisk 1086
format 1087
mkdir 1087
more 1088
mount 1088
move 1089
pwd 1089
rename 1090
reset recycle-bin 1090
rmdir 1091
umount 1091
undelete 1092

79 CONFIGURATION FILE MANAGEMENT COMMANDS

backup startup-configuration 1093
display saved-configuration 1093
display startup 1094
reset saved-configuration 1095
restore startup-configuration 1096
save 1096
slave auto-update config 1097
startup saved-configuration 1098

80 FTP SERVER CONFIGURATION COMMANDS

display ftp-server 1099
display ftp-user 1099
free ftp user 1100
ftp server enable 1100
ftp timeout 1101
ftp update 1101

81 FTP CLIENT CONFIGURATION COMMANDS

ascii 1103
binary 1103
bye 1104
cd 1104
cdup 1105
close 1105
debugging 1105
delete 1106
dir 1107
disconnect 1107
display ftp client configuration 1108
ftp 1108
ftp client source 1109
ftp ipv6 1110
get 1111
lcd 1112
ls 1112
mkdir 1113
open 1113
open ipv6 1114
passive 1115
put 1115
pwd 1116
quit 1116
remotehelp 1116
rmdir 1118
user 1118

verbose 1119

82 TFTP CLIENT CONFIGURATION COMMANDS

display tftp client configuration 1121
tftp-server acl 1121
tftp 1122
tftp client source 1123
tftp ipv6 1124

83 SFTP CONFIGURATION COMMANDS

bye 1127
cd 1127
cdup 1128
delete 1128
dir 1128
exit 1129
get 1129
help 1130
ls 1130
mkdir 1131
put 1131
pwd 1132
quit 1132
remove 1133
rename 1133
rmdir 1133

84 INFORMATION CENTER CONFIGURATION COMMANDS

display channel 1135
display info-center 1136
display logbuffer 1138
display logbuffer summary 1140
display logfile buffer 1140
display logfile summary 1141
display trapbuffer 1141
info-center channel name 1142
info-center console channel 1143
info-center enable 1143
info-center logbuffer 1144
info-center logfile enable 1144
info-center logfile frequency 1145
info-center logfile size-quota 1145
info-center logfile switch-directory 1146
info-center loghost 1146
info-center loghost source 1147
info-center monitor channel 1148

info-center snmp channel 1149
info-center source 1149
info-center synchronous 1151
info-center timestamp 1152
info-center timestamp loghost 1153
info-center trapbuffer 1153
logfile save 1154
reset logbuffer 1155
reset trapbuffer 1155
terminal debugging 1155
terminal logging 1156
terminal monitor 1156
terminal trapping 1157

85 BASIC CONFIGURATION COMMANDS

clock datetime 1159
clock summer-time one-off 1159
clock summer-time repeating 1160
clock timezone 1162
command-privilege 1163
display clipboard 1164
display clock 1164
display current-configuration 1165
display diagnostic-information 1166
display history-command 1167
display hotkey 1167
display this 1168
display version 1169
header 1170
hotkey 1171
quit 1173
return 1173
super 1173
super password 1175
sysname 1176
system-view 1176

86 SYSTEM MAINTENANCE COMMANDS

ping 1177
ping ipv6 1178
tracert 1180
tracert ipv6 1181

87 SYSTEM DEBUGGING COMMANDS

debugging 1183
display debugging 1184

88 SYSTEM MANAGEMENT COMMANDS

boot-loader 1185
bootrom 1185
display cpu-usage 1186
display boot-loader 1188
display device 1188
display device manuinfo 1190
display environment 1191
display fan 1191
display memory 1192
display power 1192
display schedule reboot 1193
display switch-mode status 1193
display transceiver alarm interface 1194
display transceiver diagnosis interface 1196
display transceiver interface 1197
display transceiver manuinfo interface 1198
reboot 1199
reset unused porttag 1199
schedule reboot at 1200
schedule reboot delay 1201
shutdown-interval 1202
switch-mode (for Fabric) 1203
switch-mode (for I/O Module) 1204
temperature-limit 1205

89 POE CONFIGURATION COMMANDS

apply poe-profile 1207
apply poe-profile interface 1207
display poe device 1208
display poe interface 1209
display poe interface power 1212
display poe power-usage 1214
display poe pse 1215
display poe-power 1216
display poe-power ac-input state 1218
display poe-power alarm 1218
display poe-power dc-output state 1219
display poe-power dc-output value 1220
display poe-power status 1220
display poe-power supervision-module 1221
display poe-power switch state 1222
display poe-profile 1222
display poe-profile interface 1224
poe enable 1225
poe enable pse 1226
poe legacy enable 1226

po e max-power 1226
po e max-power 1227
po e mode 1228
po e pd-description 1229
po e pd-policy priority 1229
po e power max-value 1230
po e priority 1230
po e priority 1231
po e pse-policy priority 1232
po e update 1232
po e utilization-threshold 1233
po e-power input-threshold 1233
po e-power output-threshold 1234
po e-profile 1234

90 IPv4 VRRP CONFIGURATION COMMANDS

display vrrp 1237
display vrrp statistics 1238
reset vrrp statistics 1240
vrrp vrid authentication-mode 1240
vrrp method 1241
vrrp ping-enable 1242
vrrp un-check ttl 1242
vrrp vrid preempt-mode 1243
vrrp vrid priority 1244
vrrp vrid timer advertise 1244
vrrp vrid track 1245
vrrp vrid virtual-ip 1246

91 IPv6 VRRP CONFIGURATION COMMANDS

display vrrp ipv6 1249
display vrrp ipv6 statistics 1250
reset vrrp ipv6 statistics 1252
vrrp ipv6 vrid authentication-mode 1252
vrrp ipv6 method 1253
vrrp ipv6 ping-enable 1254
vrrp ipv6 vrid preempt-mode 1254
vrrp ipv6 vrid priority 1255
vrrp ipv6 vrid timer advertise 1256
vrrp ipv6 vrid track 1257
vrrp ipv6 vrid virtual-ip 1257

92 REDUNDANCY CONFIGURATION COMMANDS

display switchover state 1259
ha slave-ignore-version-check 1259
slave auto-update config 1260

slave restart 1260
slave switchover 1261
slave switchover { enable | disable } 1261

93 RRPP CONFIGURATION COMMANDS

control-vlan 1263
display rrpp brief 1263
display rrpp statistics 1265
display rrpp verbose 1267
reset rrpp statistics 1268
ring 1269
ring enable 1271
rrpp domain 1272
rrpp enable 1272
timer 1273

ABOUT THIS GUIDE

This guide describes the 3Com® Switch S7900E and how to install hardware, configure and boot software, and maintain software and hardware. This guide also provides troubleshooting and support information for your switch.

This guide is intended for Qualified Service personnel who are responsible for configuring, using, and managing the switches. It assumes a working knowledge of local area network (LAN) operations and familiarity with communication protocols that are used to interconnect LANs.



Always download the Release Notes for your product from the 3Com World Wide Web site and check for the latest updates to software and product documentation:

<http://www.3com.com>

Conventions

Table 1 lists icon conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Related Documentation

The following manuals offer additional information necessary for managing your Switch S7900E:

- *Switch S7900E Family Getting Started Guide*— Provides instructions for installing your switch.
- *Switch S7900E Family Command Reference Guide* — Provides detailed descriptions of command line interface (CLI) commands, that you require to manage your Switch S7900E.
- *Switch S7900E Family Configuration Guide*— Describes how to configure your Switch S7900E using the supported protocols and CLI commands.

- *Switch S7900E Family Release Notes* — Contains the latest information about your product. If information in this guide differs from information in the release notes, use the information in the *Release Notes*.

These documents are available in Adobe Acrobat Reader Portable Document Format (PDF) on the CD-ROM that accompanies your router or on the 3Com World Wide Web site:

<http://www.3com.com/>

ALPHABETICAL LISTING OF COMMANDS

abr-summary 297
abr-summary 489
access-limit 775
accounting 981
accounting default 775
accounting lan-access 777
accounting login 777
accounting optional 778
accounting portal 779
acl 83
acl 947
acl copy 948
acl ipv6 961
acl ipv6 copy 962
acl ipv6 name 963
acl name 949
activation-key 59
active region-configuration 169
aggregate 395
aggregation-group 615
apply as-path 447
apply comm-list delete 448
apply community 448
apply cost 449
apply cost-type 450
apply extcommunity 450
apply ip-address next-hop 467
apply ipv6 next-hop 575
apply isis 451
apply local-preference 452
apply origin 452
apply poe-profile 1207
apply poe-profile interface 1207
apply preference 453
apply preferred-value 454
apply tag 454
area 298
area 490
area-authentication-mode 347
arp max-learning-num 883
arp resolving-route enable 893
arp source-suppression enable 891
arp source-suppression limit 891
arp static 883
arp timer aging 884
asbr-summary 298
ascii 1103
attribute 780
authentication default 781
authentication lan-access 782
authentication login 783
authentication portal 783
authentication-mode 299
authentication-mode 60
authorization command 784
authorization default 785
authorization lan-access 786
authorization login 787
authorization portal 788
auto cost enable 348
auto-execute command 61
auto-rp enable 671
backup startup-configuration 1093
balance 396
balance 531
bandwidth-reference 300
bandwidth-reference 348
bestroute as-path-neglect 397
bestroute as-path-neglect 531
bestroute compare-med 397
bestroute compare-med 532
bestroute med-confederation 398
bestroute med-confederation 532
bgp 398
bims-server 897
binary 1103
bootfile-name 898
boot-loader 1185
bootrom 1185
bpdu-tunnel dot1q enable 166
bpdu-tunnel dot1q stp 165
bpdu-tunnel tunnel-dmac 167
broadcast-suppression 89
bsr-policy 671
bye 1104
bye 1127
cache-sa-enable 715
car 981

c-bsr 672
c-bsr admin-scope 673
c-bsr global 673
c-bsr group 674
c-bsr hash-length 675
c-bsr holdtime 675
c-bsr interval 676
c-bsr priority 676
cd 1083
cd 1104
cd 1127
cdup 1105
cdup 1128
check region-configuration 169
checkzero 273
checkzero 475
circuit-cost 349
classifier behavior 157
classifier behavior 991
clock datetime 1159
clock summer-time one-off 1159
clock summer-time repeating 1160
clock timezone 1162
close 1105
command-privilege 1163
compare-different-as-med 399
compare-different-as-med 533
confederation id 399
confederation nonstandard 400
confederation peer-as 401
control-vlan 1263
copy 1083
cost-style 350
c-rp 677
c-rp advertisement-interval 678
c-rp holdtime 679
crp-policy 679
cut connection 788
dampening 401
dampening 534
databits 62
data-flow-format 803
data-flow-format 827
debugging 1105
debugging 1183
default 300
default cost 273
default cost 475
default cost 490
default ipv4-unicast 402
default local-preference 403
default local-preference 535
default med 403
default med 535
default-cost 301
default-cost 491
default-route imported 404
default-route imported 536
default-route originate 274
default-route-advertise 302
default-route-advertise 351
delete 1084
delete 1106
delete 1128
delete ipv6 static-routes all 473
delete static-routes all 269
description 123
description 303
description 90
description 950
description 964
destination 616
dhcp enable 898
dhcp enable 921
dhcp relay address-check 921
dhcp relay information enable 922
dhcp relay information format 922
dhcp relay information strategy 923
dhcp relay release 924
dhcp relay security static 924
dhcp relay security tracker 925
dhcp relay server-detect 926
dhcp relay server-group 926
dhcp relay server-select 927
dhcp select relay 927
dhcp select server global-pool 899
dhcp server detect 899
dhcp server forbidden-ip 900
dhcp server ip-pool 900
dhcp server ping packets 901
dhcp server ping timeout 901
dhcp server relay information enable 902
dhcp-snooping 937
dhcp-snooping information enable 938
dhcp-snooping information format 938
dhcp-snooping information strategy 939
dhcp-snooping trust 940
dir 1084

dir 1107
dir 1128
disconnect 1107
display acl 950
display acl ipv6 964
display acl resource 943
display arp 885
display arp ip-address 886
display arp source-suppression 892
display arp timer aging 887
display bgp group 405
display bgp ipv6 group 536
display bgp ipv6 network 537
display bgp ipv6 paths 538
display bgp ipv6 peer 539
display bgp ipv6 routing-table 540
display bgp ipv6 routing-table
as-path-acl 541
display bgp ipv6 routing-table
community 542
display bgp ipv6 routing-table
community-list 543
display bgp ipv6 routing-table
dampened 543
display bgp ipv6 routing-table
dampening parameter 544
display bgp ipv6 routing-table
different-origin-as 544
display bgp ipv6 routing-table
flap-info 545
display bgp ipv6 routing-table peer
546
display bgp ipv6 routing-table
regular-expression 547
display bgp ipv6 routing-table
statistic 547
display bgp network 406
display bgp paths 406
display bgp peer 407
display bgp routing-table 409
display bgp routing-table as-path-acl
410
display bgp routing-table cidr 410
display bgp routing-table community
411
display bgp routing-table
community-list 412
display bgp routing-table dampened
412
display bgp routing-table dampening
parameter 413
display bgp routing-table
different-origin-as 414
display bgp routing-table flap-info
414
display bgp routing-table peer 415
display bgp routing-table
regular-expression 416
display bgp routing-table statistic 416
display boot-loader 1188
display brief interface 90
display channel 1135
display clipboard 1164
display clock 1164
display connection 789
display cpu-usage 1186
display current-configuration 1165
display debugging 1184
display device 1188
display device manuinfo 1190
display dhcp client 933
display dhcp relay 928
display dhcp relay security 928
display dhcp relay security statistics
929
display dhcp relay security tracker
930
display dhcp relay server-group 930
display dhcp relay statistics 931
display dhcp server conflict 902
display dhcp server expired 903
display dhcp server forbidden-ip 904
display dhcp server free-ip 904
display dhcp server ip-in-use 904
display dhcp server statistics 905
display dhcp server tree 906
display dhcp-snooping 940
display dhcp-snooping trust 941
display diagnostic-information 1166
display dns domain 1075
display dns dynamic-host 1075
display dns ipv6 dynamic-host 579
display dns ipv6 server 579
display dns proxy table 1076
display dns server 1077
display domain 790
display dot1x 749
display environment 1191
display fan 1191
display fib 227
display fib ip-address 229
display fib statistics 229

display ftp client configuration 1108
display ftp-server 1099
display ftp-user 1099
display garp statistics 213
display garp timer 213
display gvrp local-vlan interface 217
display gvrp state 217
display gvrp statistics 218
display gvrp status 218
display gvrp vlan-operation interface 219
display history-command 1167
display hotkey 1167
display hwtacacs 827
display icmp statistics 230
display igmp group 651
display igmp group port-info 652
display igmp interface 653
display igmp routing-table 654
display igmp-snooping group 623
display igmp-snooping statistics 624
display info-center 1136
display interface 92
display interface tunnel 617
display interface Vlan-interface 123
display ip as-path 455
display ip check source 243
display ip community-list 455
display ip extcommunity-list 456
display ip host 1077
display ip interface 223
display ip interface brief 225
display ip ip-prefix 467
display ip ipv6-prefix 575
display ip relay-route 247
display ip relay-tunnel 247
display ip routing-table 248
display ip routing-table acl 252
display ip routing-table ip-address 254
display ip routing-table ip-prefix 256
display ip routing-table protocol 257
display ip routing-table statistics 258
display ip socket 231
display ip statistics 232
display ip-subnet-vlan interface 141
display ip-subnet-vlan vlan 141
display ipv6 fib 580
display ipv6 host 581
display ipv6 interface 582
display ipv6 interface tunnel 618
display ipv6 neighbors 583
display ipv6 neighbors count 585
display ipv6 pathmtu 585
display ipv6 relay-route 259
display ipv6 relay-tunnel 259
display ipv6 routing-table 260
display ipv6 routing-table acl 261
display ipv6 routing-table ipv6-address 261
display ipv6 routing-table ipv6-address1 ipv6-address2 263
display ipv6 routing-table ipv6-prefix 263
display ipv6 routing-table protocol 264
display ipv6 routing-table statistics 265
display ipv6 routing-table verbose 265
display ipv6 socket 586
display ipv6 statistics 587
display isis brief 352
display isis interface 353
display isis license 354
display isis lsdb 356
display isis mesh-group 357
display isis name-table 357
display isis peer 358
display isis route 359
display isis route ipv6 521
display isis spf-log 360
display isis statistics 361
display isolate-user-vlan 145
display lacp system-id 203
display link-aggregation interface 203
display link-aggregation service-type 205
display link-aggregation summary 205
display link-aggregation verbose 206
display local-proxy-arp 896
display local-user 792
display logbuffer 1138
display logbuffer summary 1140
display logfile buffer 1140
display logfile summary 1141
display loopback-detection 94
display mac-address 115
display mac-address aging-time 116
display mac-address mac-learning

116
display mac-authentication 769
display memory 1192
display mirroring-group 1015
display msdp brief 715
display msdp peer-status 716
display msdp sa-cache 718
display msdp sa-count 719
display multicast boundary 733
display multicast forwarding-table 734
display multicast routing-table 736
display multicast routing-table static 737
display multicast rpf-info 738
display multicast-vlan 647
display ntp-service sessions 1061
display ntp-service status 1062
display ntp-service trace 1063
display ospf abr-asbr 303
display ospf asbr-summary 304
display ospf brief 305
display ospf cumulative 307
display ospf error 308
display ospf interface 310
display ospf lsdb 311
display ospf nexthop 313
display ospf peer 313
display ospf peer statistics 315
display ospf request-queue 316
display ospf retrans-queue 317
display ospf routing 318
display ospf vlink 319
display ospfv3 491
display ospfv3 interface 493
display ospfv3 lsdb 494
display ospfv3 lsdb statistic 496
display ospfv3 next-hop 497
display ospfv3 peer 497
display ospfv3 peer statistic 499
display ospfv3 request-list 500
display ospfv3 retrans-list 501
display ospfv3 routing 503
display ospfv3 statistic 504
display ospfv3 topology 505
display ospfv3 vlink 506
display pim bsr-info 680
display pim claimed-route 681
display pim control-message counters 682
display pim grafts 683
display pim interface 684
display pim join-prune 686
display pim neighbor 687
display pim routing-table 688
display pim rp-info 690
display poe device 1208
display poe interface 1209
display poe interface power 1212
display poe power-usage 1214
display poe pse 1215
display poe-power 1216
display poe-power ac-input state 1218
display poe-power alarm 1218
display poe-power dc-output state 1219
display poe-power dc-output value 1220
display poe-power status 1220
display poe-power supervision-module 1221
display poe-power switch state 1222
display poe-profile 1222
display poe-profile interface 1224
display portal acl 843
display portal connection statistics 844
display portal free-rule 846
display portal interface 847
display portal server 848
display portal server statistics 849
display portal tcp-cheat statistics 850
display portal user 851
display port-group manual 95
display port-isolate group 113
display power 1192
display protocol-vlan interface 135
display protocol-vlan vlan 135
display proxy-arp 896
display public-key local 859
display public-key peer 860
display qos lr interface 973
display qos map-table 1005
display qos policy 991
display qos policy global 992
display qos policy interface 993
display qos sp interface 1001
display qos trust interface 1011
display qos vlan-policy 994
display qos wrr interface 1001
display radius scheme 803

display radius statistics 805
display rip 275
display rip database 276
display rip interface 277
display rip route 278
display ripng 476
display ripng database 477
display ripng interface 478
display ripng route 479
display rmon alarm 1047
display rmon event 1048
display rmon eventlog 1048
display rmon history 1049
display rmon prialarm 1050
display rmon statistics 1051
display route-policy 456
display rrp brief 1263
display rrp statistics 1265
display rrp verbose 1267
display saved-configuration 1093
display schedule reboot 1193
display sftp client source 861
display snmp-agent community 1023
display snmp-agent group 1024
display snmp-agent local-switch
fabricid 1023
display snmp-agent mib-view 1025
display snmp-agent statistics 1026
display snmp-agent sys-info 1027
display snmp-agent trap-list 1028
display snmp-agent usm-user 1029
display ssh client source 861
display ssh server 862
display ssh server-info 863
display ssh user-information 863
display startup 1094
display stop-accounting-buffer 807
display stop-accounting-buffer 829
display storm-constrain 96
display stp 170
display stp abnormal-port 172
display stp down-port 173
display stp history 174
display stp region-configuration 175
display stp root 175
display stp tc 176
display switch-mode status 1193
display switchover state 1259
display tcp ipv6 statistics 590
display tcp ipv6 status 592
display tcp statistics 233
display tcp status 235
display telnet client configuration 62
display tftp client configuration 1121
display this 1168
display time-range 944
display traffic behavior 983
display traffic classifier 975
display transceiver alarm interface
1194
display transceiver diagnosis interface
1196
display transceiver interface 1197
display transceiver manuinfo
interface 1198
display trapbuffer 1141
display udp ipv6 statistics 593
display udp statistics 236
display user-bind 244
display user-interface 63
display users 64
display version 1169
display vlan 124
display voice vlan oui 149
display voice vlan state 149
display vrrp 1237
display vrrp ipv6 1249
display vrrp ipv6 statistics 1250
display vrrp statistics 1238
dns domain 1078
dns proxy enable 1078
dns resolve 1079
dns server 1079
dns server ipv6 594
dns-list 908
domain 793
domain default 794
domain-authentication-mode 362
domain-name 908
dot1x 751
dot1x authentication-method 752
dot1x free-ip 765
dot1x guest-vlan 753
dot1x handshake 755
dot1x max-user 755
dot1x multicast-trigger 756
dot1x port-control 757
dot1x port-method 758
dot1x quiet-period 759
dot1x retry 759
dot1x supp-proxy-check 760
dot1x timer 761

dot1x timer ead-timeout 766
dot1x url 766
drop-unknown 625
duplex 97
ebgp-interface-sensitive 417
enable log 320
enable snmp trap updown 1029
encap-data-enable 720
escape-key 65
execute 1085
exit 1129
expired 909
fast-leave 625
fast-leave 655
file prompt 1086
filter 320
filter 984
filter-policy export 279
filter-policy export 321
filter-policy export 363
filter-policy export 417
filter-policy export 479
filter-policy export 506
filter-policy export 548
filter-policy import 280
filter-policy import 322
filter-policy import 365
filter-policy import 418
filter-policy import 480
filter-policy import 507
filter-policy import 548
fixdisk 1086
flash-flood 365
flow-control 66
flow-control 97
flow-interval 98
format 1087
free ftp user 1100
free user-interface 66
ftp 1108
ftp client source 1109
ftp ipv6 1110
ftp server enable 1100
ftp timeout 1101
ftp update 1101
garp timer 214
garp timer leaveall 215
gateway-list 909
get 1111
get 1129
gratuitous-arp-learning enable 889
gratuitous-arp-sending enable 889
group 419
group 549
group-member 98
group-policy 626
gvrp 219
gvrp registration 220
ha slave-ignore-version-check 1259
header 1170
hello-option dr-priority 691
hello-option holdtime 692
hello-option lan-delay 692
hello-option neighbor-tracking 693
hello-option override-interval 693
help 1130
history-command max-size 67
holdtime assert 694
holdtime join-prune 695
host-advertise 322
host-aging-time 627
host-route 281
hotkey 1171
hwtacacs nas-ip 829
hwtacacs scheme 830
idle-cut 794
idle-timeout 67
if-match 975
if-match acl 468
if-match as-path 457
if-match community 458
if-match cost 458
if-match customer-vlan-id 157
if-match extcommunity 459
if-match interface 460
if-match ip 469
if-match ip-prefix 469
if-match ipv6 576
if-match route-type 460
if-match tag 461
igmp 656
igmp enable 656
igmp fast-leave 657
igmp group-policy 658
igmp last-member-query-interval 659
igmp max-response-time 659
igmp require-router-alert 660
igmp robust-count 660
igmp send-router-alert 661
igmp static-group 662
igmp timer other-querier-present 663
igmp timer query 663

- igmp version 664
- igmp-snooping 628
 - igmp-snooping drop-unknown 628
 - igmp-snooping enable 629
 - igmp-snooping fast-leave 629
 - igmp-snooping general-query source-ip 630
 - igmp-snooping group-limit 631
 - igmp-snooping group-policy 632
 - igmp-snooping host-aging-time 633
 - igmp-snooping host-join 633
 - igmp-snooping last-member-query-interval 635
 - igmp-snooping max-response-time 635
 - igmp-snooping overflow-replace 636
 - igmp-snooping querier 637
 - igmp-snooping query-interval 637
 - igmp-snooping router-aging-time 638
 - igmp-snooping source-deny 638
 - igmp-snooping special-query source-ip 639
 - igmp-snooping static-group 640
 - igmp-snooping static-router-port 641
 - igmp-snooping version 641
- import 1006
 - import-route 282
 - import-route 323
 - import-route 366
 - import-route 419
 - import-route 481
 - import-route 508
 - import-route 550
 - import-route isis level-2 into level-1 368
 - import-source 721
- info-center channel name 1142
- info-center console channel 1143
- info-center enable 1143
- info-center logbuffer 1144
- info-center logfile enable 1144
- info-center logfile frequency 1145
- info-center logfile size-quota 1145
- info-center logfile switch-directory 1146
- info-center loghost 1146
- info-center loghost source 1147
- info-center monitor channel 1148
- info-center snmp channel 1149
- info-center source 1149
- info-center synchronous 1151
- info-center timestamp 1152
- info-center timestamp loghost 1153
- info-center trapbuffer 1153
- instance 177
- interface 99
 - interface tunnel 619
 - interface Vlan-interface 125
- ip address 126
 - ip address 225
 - ip address dhcp-alloc 934
 - ip as-path 462
 - ip check source 245
 - ip community-list 463
 - ip extcommunity-list 464
 - ip forward-broadcast 237
 - ip forward-broadcast 238
 - ip host 1080
 - ip ip-prefix 470
 - ip ipv6-prefix 577
 - ip redirects enable 238
 - ip route-static 269
 - ip route-static default-preference 271
 - ip rpf-route-static 739
 - ip ttl-expires enable 239
 - ip unreachable enable 239
 - ip-subnet-vlan 142
- ipv6 594
 - ipv6 611
 - ipv6 address 595
 - ipv6 address 611
 - ipv6 address auto link-local 595
 - ipv6 address auto link-local 612
 - ipv6 address eui-64 596
 - ipv6 address eui-64 612
 - ipv6 address link-local 596
 - ipv6 address link-local 613
 - ipv6 default-route-advertise 523
 - ipv6 enable 523
 - ipv6 filter-policy export 524
 - ipv6 filter-policy import 525
 - ipv6 host 597
 - ipv6 icmp-error 597
 - ipv6 icmpv6 multicast-echo-reply enable 598
 - ipv6 import-route 526
 - ipv6 import-route isisv6 level-2 into level-1 527
 - ipv6 maximum load-balancing 527
 - ipv6 nd autoconfig managed-address-flag 598

ipv6 nd autoconfig other-flag 599
ipv6 nd dad attempts 599
ipv6 nd hop-limit 600
ipv6 nd ns retrans-timer 600
ipv6 nd nud reachable-time 601
ipv6 nd ra halt 602
ipv6 nd ra interval 602
ipv6 nd ra prefix 603
ipv6 nd ra router-lifetime 604
ipv6 neighbor 604
ipv6 neighbors max-learning-num
605
ipv6 pathmtu 606
ipv6 pathmtu age 606
ipv6 preference 528
ipv6 route-static 473
ipv6 summary 529
ipv6-family 550
isis 368
isis authentication-mode 369
isis circuit-level 370
isis circuit-type 371
isis cost 371
isis dis-name 372
isis dis-priority 373
isis enable 373
isis ipv6 enable 529
isis mesh-group 374
isis silent 375
isis small-hello 375
isis timer csnp 376
isis timer hello 377
isis timer holding-multiplier 377
isis timer lsp 378
isis timer retransmit 379
is-level 380
is-name 380
is-name map 381
isolate-user-vlan 146
isolate-user-vlan enable 147
is-snmp-traps enable 381
jp-pkt-size 695
jp-queue-size 696
jumboframe enable 99
key 808
key 831
lACP port-priority 208
lACP system-priority 208
last-member-query-interval 642
last-member-query-interval 664
lcd 1112
level 795
link-aggregation group description
209
link-aggregation group mode 209
link-aggregation group service-type
210
link-delay 100
local-proxy-arp enable 895
local-user 796
local-user password-display-mode
796
lock 68
logfile save 1154
log-peer-change 324
log-peer-change 382
log-peer-change 420
log-peer-change 509
loopback 101
loopback-detection control enable
101
loopback-detection enable 102
loopback-detection interval-time 103
loopback-detection per-vlan enable
103
ls 1112
ls 1130
lsa-arrival-interval 325
lsa-generation-interval 325
lsdb-overflow-limit 326
lsp-fragments-extend 382
lsp-length originate 383
lsp-length receive 384
mac-address 117
mac-address 118
mac-address mac-learning disable
119
mac-address max-mac-count 120
mac-address timer 121
mac-authentication 770
mac-authentication domain 771
mac-authentication timer 772
mac-authentication
user-name-format 773
maximum load-balancing 283
maximum load-balancing 327
maximum load-balancing 384
maximum load-balancing 481
maximum load-balancing 510
maximum-routes 327
max-response-time 642
max-response-time 665

mdi 104
mirroring-group 1016
mirroring-group mirroring-port 1017
mirroring-group monitor-egress 1018
mirroring-group monitor-port 1019
mirroring-group remote-probe vlan 1020
mirroring-port 1020
mirror-to 1013
mkdir 1087
mkdir 1113
mkdir 1131
modem 69
modem auto-answer 69
modem timer answer 70
monitor-port 1021
more 1088
mount 1088
move 1089
msdp 721
mtracert 740
mtu 619
multicast boundary 742
multicast forwarding-table downstream-limit 743
multicast forwarding-table route-limit 743
multicast load-splitting 744
multicast longest-match 744
multicast routing-enable 745
multicast-suppression 105
multicast-vlan enable 647
multicast-vlan subvlan 648
nas-ip 809
nas-ip 831
naturemask-arp enable 887
nbns-list 910
nest 984
nest top-most vlan-id 158
netbios-type 911
network 283
network 328
network 420
network 551
network 911
network-entity 385
nssa 328
ntp-service access 1064
ntp-service authentication enable 1065
ntp-service authentication-keyid 1065
ntp-service broadcast-client 1066
ntp-service broadcast-server 1066
ntp-service in-interface disable 1067
ntp-service max-dynamic-sessions 1068
ntp-service multicast-client 1068
ntp-service multicast-server 1069
ntp-service refclock-master 1069
ntp-service reliable authentication-keyid 1070
ntp-service source-interface 1070
ntp-service unicast-peer 1071
ntp-service unicast-server 1072
open 1113
open ipv6 1114
option 912
originating-rp 722
ospf 329
ospf authentication-mode 330
ospf cost 331
ospf dr-priority 332
ospf mib-binding 332
ospf mtu-enable 333
ospf network-type 334
ospf timer dead 335
ospf timer hello 335
ospf timer poll 336
ospf timer retransmit 336
ospf trans-delay 337
ospfv3 510
ospfv3 area 511
ospfv3 cost 511
ospfv3 dr-priority 512
ospfv3 mtu-ignore 512
ospfv3 timer dead 513
ospfv3 timer hello 514
ospfv3 timer retransmit 514
ospfv3 trans-delay 515
overflow-replace 643
parity 70
passive 1115
password 797
peer 284
peer 338
peer advertise-community 421
peer advertise-community 552
peer advertise-ext-community 422
peer advertise-ext-community 552
peer allow-as-loop 422

peer allow-as-loop 553
peer as-number 423
peer as-number 553
peer as-path-acl 424
peer as-path-acl 554
peer capability-advertise
conventional 424
peer capability-advertise
route-refresh 425
peer capability-advertise
route-refresh 555
peer connect-interface 425
peer connect-interface 555
peer connect-interface 722
peer default-route-advertise 426
peer default-route-advertise 556
peer description 427
peer description 557
peer description 723
peer ebgp-max-hop 427
peer ebgp-max-hop 557
peer enable 428
peer fake-as 429
peer fake-as 558
peer filter-policy 429
peer filter-policy 558
peer group 430
peer group 559
peer ignore 430
peer ignore 560
peer ip-prefix 431
peer ipv6-prefix 560
peer keep-all-routes 432
peer keep-all-routes 561
peer log-change 432
peer log-change 562
peer mesh-group 724
peer minimum-ttl 724
peer next-hop-local 433
peer next-hop-local 562
peer password 433
peer preferred-value 434
peer preferred-value 563
peer public-as-only 435
peer public-as-only 564
peer reflect-client 436
peer reflect-client 564
peer request-sa-enable 725
peer route-limit 436
peer route-limit 565
peer route-policy 437
peer route-policy 565
peer route-update-interval 438
peer route-update-interval 566
peer sa-cache-maximum 725
peer sa-policy 726
peer sa-request-policy 727
peer substitute-as 438
peer substitute-as 567
peer timer 439
peer timer 567
peer-public-key end 864
pim 696
pim bsr-boundary 697
pim dm 697
pim hello-option dr-priority 698
pim hello-option holdtime 698
pim hello-option lan-delay 699
pim hello-option neighbor-tracking
700
pim hello-option override-interval
700
pim holdtime assert 701
pim holdtime join-prune 701
pim require-genid 702
pim sm 702
pim state-refresh-capable 703
pim timer graft-retry 703
pim timer hello 704
pim timer join-prune 704
pim triggered-hello-delay 705
ping 1177
ping ipv6 1178
poe enable 1225
poe enable pse 1226
poe legacy enable 1226
poe max-power 1226
poe max-power 1227
poe mode 1228
poe pd-description 1229
poe pd-policy priority 1229
poe power max-value 1230
poe priority 1230
poe priority 1231
poe pse-policy priority 1232
poe update 1232
poe utilization-threshold 1233
poe-power input-threshold 1233
poe-power output-threshold 1234
poe-profile 1234
port 129
port access vlan 129

port hybrid ip-subnet-vlan vlan 143
port hybrid protocol-vlan 136
port hybrid pvid vlan 130
port hybrid vlan 131
port link-aggregation group 210
port link-type 132
port trunk permit vlan 133
port trunk pvid vlan 133
portal auth-network 852
portal delete-user 853
portal free-rule 853
portal server 854
portal server method 855
port-group 106
port-group aggregation 211
port-isolate enable 113
preference 284
preference 338
preference 386
preference 439
preference 482
preference 515
preference 568
primary accounting 810
primary accounting 832
primary authentication 810
primary authentication 833
primary authorization 834
probe-interval 705
protocol inbound 71
protocol-vlan 137
proxy-arp enable 895
public-key local create 866
public-key local destroy 866
public-key local export rsa 867
public-key peer 868
public-key peer import sshkey 868
public-key-code begin 864
public-key-code end 865
put 1115
put 1131
pwd 1089
pwd 1116
pwd 1132
qinq enable 158
qinq ethernet-type customer-tag 159
qinq ethernet-type service-tag 160
qos apply policy 161
qos apply policy 995
qos apply policy global 997
qos lr outbound 973
qos map-table 1006
qos policy 161
qos policy 997
qos priority 1009
qos sp 1002
qos trust 1011
qos vlan-policy 998
qos wrr 1003
quit 1116
quit 1132
quit 1173
radius client 811
radius nas-ip 812
radius scheme 813
radius trap 813
reboot 1199
redirect 985
reflect between-clients 440
reflect between-clients 569
reflector cluster-id 441
reflector cluster-id 570
refresh bgp 441
refresh bgp ipv6 570
region-name 178
register-policy 706
register-suppression-timeout 706
register-whole-checksum 707
remark customer-vlan-id 985
remark dot1p 986
remark drop-precedence 987
remark dscp 987
remark ip-precedence 988
remark local-precedence 989
remark service-vlan-id 989
remotehelp 1116
remove 1133
rename 1090
rename 1133
report-aggregation 644
require-router-alert 665
reset acl counter 951
reset acl ipv6 counter 965
reset arp 887
reset bgp 442
reset bgp dampening 443
reset bgp flap-info 443
reset bgp ipv4 all 444
reset bgp ipv6 571
reset bgp ipv6 dampening 571
reset bgp ipv6 flap-info 572
reset counters interface 106

reset dhcp relay statistics 932
reset dhcp server conflict 913
reset dhcp server ip-in-use 913
reset dhcp server statistics 914
reset dhcp-snooping 941
reset dns dynamic-host 1080
reset dns ipv6 dynamic-host 607
reset dot1x statistics 763
reset garp statistics 216
reset hwtacacs statistics 834
reset igmp group 666
reset igmp group port-info 667
reset igmp-snooping group 644
reset igmp-snooping statistics 645
reset ip ip-prefix 471
reset ip ipv6-prefix 578
reset ip routing-table statistics
protocol 266
reset ip statistics 240
reset ipv6 neighbors 607
reset ipv6 pathmtu 607
reset ipv6 routing-table statistics 267
reset ipv6 statistics 608
reset isis all 386
reset isis peer 387
reset lacp statistics 211
reset logbuffer 1155
reset mac-authentication statistics
774
reset msdp peer 728
reset msdp sa-cache 728
reset msdp statistics 728
reset multicast forwarding-table 745
reset multicast routing-table 746
reset ospf counters 339
reset ospf process 339
reset ospf redistribution 340
reset pim control-message counters
707
reset portal connection statistics 856
reset portal server statistics 856
reset portal tcp-cheat statistics 857
reset qos policy global 999
reset qos vlan-policy 999
reset radius statistics 814
reset recycle-bin 1090
reset rip statistics 285
reset rrp statistics 1268
reset saved-configuration 1095
reset stop-accounting-buffer 814
reset stop-accounting-buffer 835
reset stp 178
reset tcp ipv6 statistics 608
reset tcp statistics 240
reset trapbuffer 1155
reset udp ipv6 statistics 608
reset udp statistics 240
reset unused porttag 1199
reset vrrp ipv6 statistics 1252
reset vrrp statistics 1240
restore startup-configuration 1096
retry 815
retry realtime-accounting 816
retry stop-accounting 817
retry stop-accounting 835
return 1173
revision-level 179
rfc1583 compatible 340
ring 1269
ring enable 1271
rip 285
rip authentication-mode 286
rip input 287
rip metricin 287
rip metricout 288
rip mib-binding 288
rip output 289
rip poison-reverse 289
rip split-horizon 290
rip summary-address 290
rip version 291
ripng 483
ripng default-route 483
ripng enable 484
ripng metricin 485
ripng metricout 485
ripng poison-reverse 486
ripng split-horizon 486
ripng summary-address 487
rmdir 1091
rmdir 1118
rmdir 1133
rmon alarm 1053
rmon event 1054
rmon history 1055
rmon prialarm 1056
rmon statistics 1058
robust-count 668
route-policy 464
router-aging-time 645
router-id 444
router-id 516

router-id 572
rppp domain 1272
rppp enable 1272
rule 952
rule 953
rule 957
rule 966
rule 967
rule comment 958
rule comment 970
save 1096
schedule reboot at 1200
schedule reboot delay 1201
screen-length 71
secondary accounting 818
secondary accounting 836
secondary authentication 818
secondary authentication 837
secondary authorization 837
security-policy-server 819
self-service-url 798
send 72
send-router-alert 668
server-type 820
service-type 73
service-type 799
service-type ftp 800
set authentication password 74
set-overload 387
sftp 869
sftp client ipv6 source 870
sftp client source 870
sftp ipv6 871
sftp server enable 872
sftp server idle-timeout 872
shell 75
shutdown 107
shutdown 127
shutdown 729
shutdown-interval 1202
silent-interface 292
silent-interface 341
silent-interface 517
slave auto-update config 1097
slave auto-update config 1260
slave restart 1260
slave switchover { enable | disable }
1261
slave switchover 1261
snmp-agent 1031
snmp-agent calculate-password
1030
snmp-agent community 1031
snmp-agent community 83
snmp-agent group 1032
snmp-agent group 84
snmp-agent local-switch fabricid
1033
snmp-agent log 1034
snmp-agent mib-view 1035
snmp-agent packet max-size 1035
snmp-agent sys-info 1036
snmp-agent target-host 1037
snmp-agent trap enable 1038
snmp-agent trap enable ospf 341
snmp-agent trap if-mib link extended
1039
snmp-agent trap life 1040
snmp-agent trap queue-size 1041
snmp-agent trap source 1041
snmp-agent usm-user { v1 | v2c }
1042
snmp-agent usm-user 85
snmp-agent usm-user v3 1043
source 620
source-deny 646
source-lifetime 708
source-policy 708
speed 107
speed 75
spf timers 517
spf-schedule-interval 343
spf-slice-size 388
spt-switch-threshold 709
ssh client authentication server 873
ssh client first-time enable 873
ssh client ipv6 source 874
ssh client source 875
ssh server authentication-retries 875
ssh server authentication-timeout
876
ssh server compatible-ssh1x enable
876
ssh server enable 877
ssh server rekey-interval 877
ssh user 878
ssh2 879
ssh2 ipv6 880
ssm-policy 710
startup saved-configuration 1098
state 800
state 820

state-refresh-interval 711
state-refresh-rate-limit 711
state-refresh-ttl 712
static-bind client-identifier 914
static-bind ip-address 915
static-bind mac-address 916
static-rp 712
static-rpf-peer 729
step 959
step 971
stop-accounting-buffer enable 821
stop-accounting-buffer enable 838
stopbits 76
storm-constrain 108
storm-constrain control 109
storm-constrain enable log 110
storm-constrain enable trap 110
storm-constrain interval 111
stp 179
stp bpdu-protection 180
stp bridge-diameter 181
stp compliance 182
stp config-digest-snooping 183
stp cost 183
stp edged-port 184
stp loop-protection 185
stp max-hops 186
stp mcheck 186
stp mode 187
stp no-agreement-check 188
stp pathcost-standard 188
stp point-to-point 189
stp port priority 191
stp port-log 190
stp priority 192
stp region-configuration 193
stp root primary 193
stp root secondary 194
stp root-protection 195
stp tc-protection 196
stp tc-protection threshold 196
stp timer forward-delay 197
stp timer hello 198
stp timer max-age 199
stp timer-factor 200
stp transmit-limit 200
stub 344
stub 518
stub-router 344
summary 293
summary 389
summary automatic 445
super 1173
super password 1175
switch-mode (for Fabric) 1203
switch-mode (for I/O Module) 1204
synchronization 445
synchronization 573
sysname 1176
sysname 77
system-view 1176
tcp ipv6 timer fin-timeout 609
tcp ipv6 timer syn-timeout 609
tcp ipv6 window 610
tcp timer fin-timeout 241
tcp timer syn-timeout 241
tcp window 242
telnet 77
telnet client source 78
telnet ipv6 78
telnet server enable 79
temperature-limit 1205
terminal debugging 1155
terminal logging 1156
terminal monitor 1156
terminal trapping 1157
terminal type 80
tftp 1122
tftp client source 1123
tftp ipv6 1124
tftp-server acl 1121
tftp-server domain-name 917
tftp-server ip-address 917
timer 1273
timer 446
timer 574
timer hello 713
timer isp-generation 390
timer join-prune 714
timer lsp-max-age 391
timer lsp-refresh 392
timer other-querier-present 669
timer query 670
timer quiet 822
timer quiet 839
timer realtime-accounting 823
timer realtime-accounting 839
timer response-timeout 823
timer response-timeout 840
timer retry 730
timer spf 392
time-range 945

timers 293
timers 487
tracert 1180
tracert ipv6 1181
traffic behavior 162
traffic behavior 990
traffic classifier 162
traffic classifier 978
tunnel-protocol 621
umount 1091
undelete 1092
unicast-suppression 111
user 1118
user privilege level 81
user-bind 245
user-interface 80
user-name-format 824
user-name-format 841
validate-source-address 294
verbose 1119
version 295
version 670
virtual-system 393
vlan 128
vlan-mapping modulo 201
vlink-peer 345
vlink-peer 519
voice vlan 150
voice vlan aging 151
voice vlan enable 151
voice vlan mac-address 152
voice vlan mode auto 154
voice vlan security enable 154
voice-config 918
vrrp ipv6 method 1253
vrrp ipv6 ping-enable 1254
vrrp ipv6 vrid authentication-mode 1252
vrrp ipv6 vrid preempt-mode 1254
vrrp ipv6 vrid priority 1255
vrrp ipv6 vrid timer advertise 1256
vrrp ipv6 vrid track 1257
vrrp ipv6 vrid virtual-ip 1257
vrrp method 1241
vrrp ping-enable 1242
vrrp un-check ttl 1242
vrrp vrid authentication-mode 1240
vrrp vrid preempt-mode 1243
vrrp vrid priority 1244
vrrp vrid timer advertise 1244
vrrp vrid track 1245
vrrp vrid virtual-ip 1246
work-directory 801

1

LOGIN COMMANDS

activation-key

Syntax **activation-key** *character*

undo activation-key

View AUX interface view

Parameters *character*: Shortcut key for starting terminal sessions, a character or its ASCII decimal equivalent in the range 0 to 127; or a string of 1 to 3 characters.

Description Use the **activation-key** command to define a shortcut key for starting a terminal session.

Use the **undo activation-key** command to restore the default shortcut key.

You can use a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters to define a shortcut key. In the latter case, the system takes only the first character to define the shortcut key. For example, if you input an ASCII code value 97, the system will set the shortcut key to <a>; if you input the string **b@c**, the system will set the shortcut key to .

You may use the **display current-configuration** command to verify the shortcut key you have defined.

By default, pressing **Enter** key will start a terminal session.

Examples # Set the shortcut key for starting terminal sessions to <s>.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] activation-key s
```

To verify the configuration, do the following:

Exit the terminal session on the aux port, and enter <s> at the prompt of "Please press ENTER". You will see the terminal session being started.

```
[Sysname-ui-aux0] return
<Sysname> quit
*****
* Copyright (c) 2004-2007 3Com Corporation All rights reserved.      *
* Without the owner's prior written consent,                          *
*****
```

```
* no decompiling or reverse-switch fabricering shall be allowed.      *
*****
User interface aux0 is available.
```

```
Please press ENTER.
```

```
<Sysname>
%Apr 28 04:33:11:611 2005 Sysname SHELL/5/LOGIN: Console login from aux0
```

authentication-mode

Syntax `authentication-mode { none | password | scheme [command-authorization] }`

View User interface view

Parameters **none**: Does not authenticate users.

password: Authenticates users using the local password.

scheme: Authenticates users locally or remotely using usernames and passwords.

command-authorization: Performs command authorization on TACACS authentication server.

Description Use the **authentication-mode** command to specify the authentication mode.

- If you specify the **password** keyword to authenticate users using the local password, remember to set the local password using the **set authentication password { cipher | simple } password** command.
- If you specify the **scheme** keyword to authenticate users locally or remotely using usernames and passwords, the actual authentication mode depends on other related configuration. Refer to “HWTACACS Configuration Commands” on page 827 for more information.
- If this command is executed with the **command-authorization** keywords specified, authorization is performed on the TACACS server whenever you attempt to execute a command, and the command can be executed only when you pass the authorization. Normally, a TACACS server contains a list of the commands available to different users.

After you specify to perform local password authentication, when a user logs in through the Console port, a user can log into the switch even if the password is not configured on the switch. But for a VTY user interface, a password is needed for a user to log into the switch through it under the same condition.

By default, users logging in through the Console port are not authenticated, whereas modem users and Telnet users are authenticated.



CAUTION: For VTY user interface, if you want to set the login authentication mode to **none** or **password**, you must first verify that the SSH protocol is not supported by the user interface. Otherwise, your configuration will fail. Refer to “protocol inbound” on page 71.

Examples # Configure to authenticate users using the local password.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] authentication-mode password
```

auto-execute command

Syntax **auto-execute command** *text*

undo auto-execute command

View User interface view

Parameters *text*: Command to be executed automatically.

Description Use the **auto-execute command** command to set the command that is executed automatically after a user logs in.

Use the **undo auto-execute command** command to disable the specified command from being automatically executed.

Use these two commands in the VTY user interface only.

Normally, the **telnet** command is specified to be executed automatically to enable the user to Telnet to a specific network device automatically.

By default, no command is automatically executed.



CAUTION:

- *The **auto-execute command** command may cause you unable to perform common configuration in the user interface, so use it with caution.*
- *Before executing the **auto-execute command** command and save your configuration, make sure you can log into the switch in other modes and cancel the configuration.*

Examples # Configure the **telnet** 10.110.100.1 command to be executed automatically after users log into VTY 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] auto-execute command telnet 10.110.100.1
% This action will lead to configuration failure through ui-vty0. Are you sure?[Y/N]y
```

After the above configuration, when a user logs onto the device through VTY 0, the device automatically executes the configured command and logs off the current user.

databits

Syntax `databits { 5 | 6 | 7 | 8 }`

undo databits

View AUX interface view

Parameters **5:** Five data bits.

6: Six data bits.

7: Seven data bits.

8: Eight data bits.

Description Use the **databits** command to set the databits for the user interface.

Use the **undo databits** command to revert to the default data bits.

The default data bits is 8.



3Com S7900E Family only support data bits 7 and 8. To establish the connection again, you need to modify the configuration of the termination emulation utility running on your PC accordingly.

Examples # Set the data bits to 7.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] databits 7
```

display telnet client configuration

Syntax `display telnet client configuration`

View Any view

Parameter None

Description Use the **display telnet client configuration** command to display the source IP address or source interface configured for the current device.

Example # Display the source IP address or source interface configured for the current device.

```
<Sysname> display telnet client configuration
The source IP address is 1.1.1.1.
```

display user-interface

Syntax `display user-interface [type number | number] [summary]`

View Any view

Parameters *type*: User interface type.

number: Absolute or relative index of the user interface. This argument can be an absolute user interface index (if you do not provide the *type* argument) or a relative user interface index (if you provide the *type* argument).

summary: Displays the summary information about a user interface.

Description Use the **display user-interface** command to view information about the specified or all user interfaces.

When the **summary** keyword is absent, the command will display the type of the user interface, the absolute or relative number, the speed, the user privilege level, the authentication mode and the physical location.

When the **summary** keyword is present, the command will display all the number and type of user interfaces under use and without use.

Examples # Display the information about user interface 0.

```
<Sysname> display user-interface 0
  Idx  Type      Tx/Rx      Modem Privi Auth  Int
F 0    AUX 0      9600      -     3    N    -

+      : Current user-interface is active.
F      : Current user-interface is active and work in async mode.
Idx    : Absolute index of user-interface.
Type   : Type and relative index of user-interface.
Privi  : The privilege of user-interface.
Auth   : The authentication mode of user-interface.
Int    : The physical location of UIs.
A      : Authenticate use AAA.
L      : Authentication use local database.
N      : Current UI need not authentication.
P      : Authenticate use current UI's password.
```

Table 2 Descriptions on the fields of the display user-interface command

Filed	Description
+	The information displayed is about the current user interface.
F	The information displayed is about the current user interface. And the current user interface operates in asynchronous mode.
Idx	The absolute index of the user interface
Type	User interface type and the relative index
Tx/Rx	Transmission speed of the user interface
Modem	Indicates whether or not a modem is used.
Privi	The available command level

Table 2 Descriptions on the fields of the display user-interface command

Filed	Description
Auth	The authentication mode
Int	The physical position of the user interface

display users

Syntax `display users [all]`

View Any view

Parameters **all**: Displays the information about all user interfaces.

Description Use the **display users** command to display the information about user interfaces. If you do not specify the **all** keyword, only the information about the current user interface is displayed.

Examples # Display the information about the current user interface.

```
<Sysname> display users
The user application information of the user interface(s):
  Idx   UI      Delay   Type Userlevel
  1    VTY 0    00:11:45 TEL    3
  2    VTY 1    00:16:35 TEL    3
  3    VTY 2    00:16:54 TEL    3
+ 4    VTY 3    00:00:00 TEL    3

Following are more details.
VTY 0   :
        Location: 192.168.0.123
VTY 1   :
        Location: 192.168.0.43
VTY 2   :
        Location: 192.168.0.2
VTY 3   :
        User name: user
        Location: 192.168.0.33
+       : Current operation user.
F       : Current operation user work in async mode.
```

Table 3 Descriptions on the fields of the display users command

Field	Description
+	The information displayed is about the current user interface.
F	The information is about the current user interface, and the current user interface operates in asynchronous mode.
UI	The numbers in the left sub-column are the absolute user interface indexes, and those in the right sub-column are the relative user interface indexes.
Delay	The period in seconds the user interface idles for.
Type	User type
Userlevel	The level of the commands available to the users logging into the user interface

Table 3 Descriptions on the fields of the display users command

Field	Description
Location	The IP address form which the user logs in.
User name	The login name of the user that logs into the user interface.

escape-key

Syntax `escape-key { default | character }`

undo escape-key

View User interface view

Parameters **default:** Restores the default escape key combination <Ctrl + C>.

character: Specifies the shortcut key for aborting a task, a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters.

Description Use the **escape-key** command to define a shortcut key for aborting tasks.

Use the **undo escape-key** command to restore the default shortcut key.

You can use a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters to define a shortcut key. But in fact, only the first character functions as the shortcut key. For example, if you enter an ASCII value 113, the system will use its corresponding character <q> as the shortcut key; if you input the string **q@c**, the system will use the first letter <q> as the shortcut key.

By default, you can use <Ctrl + C> to terminate a task. You can use the **display current-configuration** command to verify the shortcut key you have defined.

Examples # Define <Q> as the escape key.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] escape-key Q
```

To verify the configuration, do the following:

Run the **ping** command to test the connection.

```
<Sysname> ping -c 20 125.241.23.46
PING 125.241.23.46: 56 data bytes, press Q to break
Request time out

--- 125.241.23.46 ping statistics ---
 2 packet(s) transmitted
 0 packet(s) received
100.00% packet loss
```

Enter <Q>, if the ping task is terminated and return to the current view, the configuration is correct.

<Sysname>

flow-control

Syntax **flow-control** { **hardware** | **none** | **software** }

undo flow-control

View AUX interface view

Parameters **hardware**: Configures to perform hardware flow control.

none: Configures no flow control.

software: Configures to perform software flow control.

Description Using **flow-control** command, you can configure the flow control mode on AUX port. Using **undo flow-control** command, you can restore the default flow control mode.

By default, the value is **none**. That is, no flow control will be performed.



*3Com S7900E Family only support **none** keyword.*

Examples # Configure software flow control on AUX port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] flow-control none
```

free user-interface

Syntax **free user-interface** [*type*] *number*

View User view

Parameters *type*: User interface type.

number: Absolute user interface index or relative user interface index.

- Relative user interface index: If you provide the *type* argument, *number* indicates the user interface index of the type. When the type is AUX, the *number* is 0; when the type is VTY, the *number* ranges from 0 to 4.
- Absolute user interface index: If you do not provide the *type* argument, *number* indicates absolute user interface index, which ranges from 0 to 5.

Description Use the **free user-interface** command to clear a specified user interface. If you execute this command, the corresponding user interface will be disconnected.

Note that the current user interface can not be cleared.

Examples # Log into user interface 0 and clear user interface 1.

```
<Sysname> free user-interface 1
Are you sure to free user-interface vty0
[Y/N]y
[OK]
```

After you execute this command, user interface 1 will be disconnected. The user in it must log in again to connect to the switch.

history-command max-size

Syntax **history-command max-size** *value*

undo history-command max-size

View User interface view

Parameters *value*: Size of the history command buffer. This argument ranges from 0 to 256 and defaults to 10. That is, the history command buffer can store 10 commands by default.

Description Use the **history-command max-size** command to set the size of the history command buffer.

Use the **undo history-command max-size** command to revert to the default history command buffer size.

Examples # Set the size of the history command buffer to 20 to enable it to store up to 20 commands.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] history-command max-size 20
```

idle-timeout

Syntax **idle-timeout** *minutes* [*seconds*]

undo idle-timeout

View User interface view

Parameters *minutes*: Number of minutes. This argument ranges from 0 to 35,791.

seconds: Number of seconds. This argument ranges from 0 to 59.

Description Use the **idle-timeout** command to set the timeout time. The connection to a user interface is terminated if no operation is performed in the user interface within the specified period.

Use the **undo idle-timeout** command to revert to the default timeout time.

You can use the **idle-timeout 0** command to disable the timeout function.

The default timeout time is 10 minutes.

Examples # Set the timeout time of AUX 0 to 1 minute.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] idle-timeout 1 0
```

lock

Syntax **lock**

View User view

Parameters None

Description Use the **lock** command to lock the current user interface to prevent unauthorized users from operating the user interface.

With the execution of this command, the system prompts to enter and confirm the password (up to 16 characters), and then locks the user interface.

To cancel the lock, press the **Enter** key and enter the correct password.

By default, the system will not lock the current user interface automatically.

Examples # Lock the current user interface.

```
<Sysname> lock
Please input password<1 to 16> to lock current user terminal interface:
Password:
Again:
```

```
locked !
```

Cancel the lock.

```
Password:
<Sysname>
```

modem

Syntax **modem** [**both** | **call-in** | **call-out**]
undo modem [**both** | **call-in** | **call-out**]

View AUX interface view

Parameters **both**: Allows both incoming and outgoing calls.

call-in: Allows incoming calls only.

call-out: Allows outgoing calls only.

Description Use the **modem** command to enable the switch-side modem to accept incoming calls, initiate outgoing calls, or both.

Use the **undo modem** command to remove the modem dial-up configuration.

By default, modem calls are not allowed.

Examples # Enable the modem to accept both incoming and outgoing calls.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem both
```

modem auto-answer

Syntax **modem auto-answer**
undo modem auto-answer

View AUX interface view

Parameters None

Description Use the **modem auto-answer** command to configure the switch-side modem to operate in the auto-answer mode.

Use the **undo modem auto-answer** command to restore the default.

By default, the switch-side modem operates in the manual answer mode.

Examples # Configure the switch-side modem to operate in the auto-answer mode.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem auto-answer
```

modem timer answer

- Syntax** **modem timer answer** *seconds*
- undo modem timer answer**
- View** AUX interface view
- Parameters** *seconds*: Timeout time in seconds, ranging from 1 to 60. The default is 30 seconds.
- Description** Use the **modem timer answer** command to set the maximum amount of time that the modem waits for the carrier signal after the off-hook action during incoming call connection setup.
- Use the **undo modem timer answer** command to restore the default.
- Examples** # Set the maximum amount of time that the switch-side modem waits for the carrier signal after the off-hook action to 45 seconds.
- ```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem timer answer 45
```

---

**parity**

- Syntax** **parity** { **even** | **mark** | **none** | **odd** | **space** }
- undo parity**
- View** AUX interface view
- Parameters** **even**: Performs even checks.
- mark**: Performs mark checks.
- none**: Does not check.
- odd**: Performs odd checks.
- space**: Performs space checks.
- Description** Use the **parity** command to set the check mode of the user interface.
- Use the **undo parity** command to revert to the default check mode.
- No check is performed by default.



3Com S7900E Ethernet switches support the **even**, **none**, and **odd** check modes only. To establish the connection again, you need to modify the configuration of the termination emulation utility running on your PC accordingly.

**Examples** # Set to perform mark checks.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] parity mark
```

## protocol inbound

**Syntax** **protocol inbound** { **all** | **ssh** | **telnet** }

**View** VTY interface view

**Parameters** **all**: Supports both Telnet protocol and SSH protocol.

**ssh**: Supports SSH protocol.

**telnet**: Supports Telnet protocol.

**Description** Use the **protocol inbound** command to configure the user interface to support specified protocols.

Both Telnet and SSH protocols are supported by default.

**Related command:** **user-interface** vty.



*CAUTION: If you want to configure the user interface to support SSH, to ensure a successful login, you must first configure the authentication mode to scheme on the user interface. If you set the authentication mode to password or none, the **protocol inbound ssh** command will fail. Refer to “authentication-mode” on page 60.*

**Examples** # Configure VTY 0 to support only SSH protocol.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] protocol inbound ssh
```

## screen-length

**Syntax** **screen-length** *screen-length*

**undo screen-length**

**View** User interface view

**Parameters** *screen-length*: Number of lines the screen can contain. This argument ranges from 0 to 512 and defaults to 24.

**Description** Use the **screen-length** command to set the number of lines the terminal screen can contain.

Use the **undo screen-length** command to revert to the default number of lines.

You can use the **screen-length 0** command to disable the function to display information in pages.

**Examples** # Set the number of lines the terminal screen can contain to 20.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] screen-length 20
```

## send

**Syntax** **send** { **all** | *number* | *type number* }

**View** User view

**Parameters** **all**: Specifies to send messages to all user interfaces.

*type*: User interface type.

*number*: Absolute user interface index or relative user interface index.

- Relative user interface index: If you provide the *type* argument, the *number* argument indicates the user interface index of the type. When the type is AUX, *number* is 0; when the type is VTY, *number* ranges from 0 to 4.
- Absolute user interface index: If you do not provide the *type* argument, the *number* argument indicates the absolute user interface index, and ranges from 0 to 5.

**Description** Use the **send** command to send messages to a specified user interface or all user interfaces.

**Examples** # Send messages to all user interfaces.

```
<Sysname> send all
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
hello^Z
Send message? [Y/N]y
<Sysname>

***Message from vty0 to vty0

```

```
hello
<Sysname>
```

---

## service-type

**Syntax** **service-type** { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }\* [ **level** *level* ] }

**undo service-type** { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }\* }

**View** Local user view

**Parameters** **ftp**: Specifies the users to be of FTP type.

**lan-access**: Specifies the users to be of LAN-access type, which normally means Ethernet users, such as 802.1x users.

**ssh**: Specifies the users to be of SSH type.

**telnet**: Specifies the users to be of Telnet type.

**terminal**: Makes terminal services available to users logging in through the Console port.

**level** *level*: Specifies the user level for Telnet users, Terminal users, or SSH users. The *level* argument ranges from 0 to 3 and defaults to 0.

**Description** Use the **service-type** command to specify the login type and the corresponding available command level.

Use the **undo service-type** command to cancel login type configuration.

Commands fall into four command levels: visit, monitor, system, and manage, which are described as follows:

- Visit level: Commands of this level are used to diagnose network and change the language mode of user interface, such as the **ping**, **tracert**. The **Telnet** command is also of this level. Commands of this level cannot be saved in configuration files.
- Monitor level: Commands of this level are used to maintain the system, to debug service problems, and so on. The **display** and **debugging** command are of monitor level. Commands of this level cannot be saved in configuration files.
- System level: Commands of this level are used to configure services. Commands concerning routing and network layers are of system level. You can utilize network services by using these commands.
- Manage level: Commands of this level are for the operation of the entire system and the system supporting modules. Services are supported by these commands. Commands concerning file system, file transfer protocol (FTP), trivial file transfer protocol (TFTP), downloading using XModem, user management, and level setting are of administration level.

**Examples** # Configure commands of level 0 are available to the users logging in using the user name of **zbr**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user zbr
[Sysname-luser-zbr] service-type telnet level 0
```

# To verify the above configuration, you can quit the system, log in again using the user name of **zbr**, and then list the available commands, as listed in the following.

```
[Sysname] quit
<Sysname> ?
User view commands:
 cluster Run cluster command
 ping Ping function
 quit Exit from current command view
 super Set the current user priority level
 telnet Establish one TELNET connection
 tracert Trace route function
 undo Undo a command or set to its default status
```

---

## set authentication password

**Syntax** **set authentication password** { **cipher** | **simple** } *password*

**undo set authentication password**

**View** User interface view

**Parameters** **cipher**: Specifies to display the local password in encrypted text when you display the current configuration.

**simple**: Specifies to display the local password in plain text when you display the current configuration.

*password*: Password. The password must be in plain text if you specify the **simple** keyword in the **set authentication password** command. If you specify the **cipher** keyword, the password can be in either encrypted text or plain text. Whether the password is in encrypted text or plain text depends on the password string entered. Strings containing up to 16 characters (such as 123) are regarded as plain text passwords and are converted to the corresponding 24-character encrypted password (such as !TP<\*EMUHL,408'W7TH!Q!!). A encrypted password must contain 24 characters and must be in ciphered text (such as !TP<\*EMUHL,408'W7TH!Q!!).

**Description** Use the **set authentication password** command to set the local password.

Use the **undo set authentication password** command to remove the local password.

Note that only plain text passwords are expected when users are authenticated.



*By default, modem users and Telnet users need to provide their passwords to log in. If no password is set, the “Login password has not been set!” message appears on the terminal when users log in.*

**Examples** # Set the local password of VTY 0 to “123”.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] set authentication password simple 123
```

---

## shell

**Syntax** **shell**

**undo shell**

**View** User interface view

**Parameters** None

**Description** Use the **shell** command to make terminal services available for the user interface.

Use the **undo shell** command to make terminal services unavailable to the user interface.

By default, terminal services are available in all user interfaces.

Note the following when using the **undo shell** command:

- This command is available in all user interfaces except the AUX user interface, because the AUX port (also the Console) is exclusively used for configuring the switch.
- This command is unavailable in the current user interface.
- This command prompts for confirmation when being executed in any valid user interface.

**Examples** # Log into user interface 0 and make terminal services unavailable in VTY 0 through VTY 4.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] undo shell
% Disable ui-vty0-4 , are you sure ? [Y/N]y
```

---

## speed

**Syntax** **speed** *speed-value*

**undo speed****View** AUX interface view**Parameters** *speed-value*: Transmission speed (in bps). This argument can be 300, 600, 1200, 2400, 4800, 9600, 19,200, 38,400, 57,600, 115,200 and defaults to 9,600.**Description** Use the **speed** command to set the transmission speed of the user interface.  
Use the **undo speed** command to revert to the default transmission speed.

*After you use the **speed** command to configure the transmission speed of the AUX user interface, you must change the corresponding configuration of the terminal emulation program running on the PC, to keep the configuration consistent with that on the switch.*

**Examples** # Set the transmission speed of the AUX user interface to 9600 bps.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] speed 9600
```

**stopbits****Syntax** **stopbits** { 1 | 1.5 | 2 }**undo stopbits****View** AUX interface view**Parameters** **1**: Sets the stop bits to 1.  
**1.5**: Sets the stop bits to 1.5.  
**2**: Sets the stop bits to 2.**Description** Use the **stopbits** command to set the stop bits of the user interface.  
Use the **undo stopbits** command to revert to the default stop bits.  
By default, the stop bits is 1.

*The stopbits cannot be 1.5 on an S7900E Ethernet switch.*

**Examples** # Set the stop bits to 2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
```



```
[Sysname] user-interface aux 0
[Sysname-ui-aux0] stopbits 2
```

---

## sysname

**Syntax** **sysname** *string*

**undo sysname**

**View** System view

**Parameters** *string*: System name of the switch. This argument can contain 1 to 30 characters and defaults to **3Com**.

**Description** Use the **sysname** command to set a system name for the switch.

Use the **undo sysname** command to revert to the default system name.

The CLI prompt reflects the system name of a switch. For example, if the system name of a switch is "3Com", then the prompt of user view is <S7900E>.

**Examples** # Set the system name of the switch to **ABC**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sysname ABC
[ABC]
```

---

## telnet

**Syntax** **telnet** *remote-system* [ *port-number* ] [ **source** { **ip** *ip-address* | **interface** *interface-type interface-number* } ]

**View** User view

**Parameters** *remote-system*: IP address or host name of the remote system. The host name is a string of 1 to 20 characters, which can be specified using the **ip host** command.

*port-number*: TCP port number assigned to Telnet service on the remote system, in the range 0 to 65535.

*ip-address*: Source IP address of the packets sent by the Telnet client.

*interface-type interface-number*: Type and number of the interface through which the Telnet client sends packets.

**Description** Use the **telnet** command to Telnet to another switch from the current switch to manage the former remotely. You can terminate a Telnet connection by pressing <Ctrl + K>.

**Related commands:** **display tcp status, display ip host.**

**Examples** # Telnet to the switch with the host name of **Sysname2** and IP address of 129.102.0.1 from the current switch (with the host name of **Sysname1**).

```
<Sysname1> telnet 129.102.0.1
Trying 129.102.0.1 ...
Press CTRL+K to abort
Connected to 129.102.0.1 ...

* Copyright (c) 2004-2007 3Com Corporation All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-switch fabricering shall be allowed. *

<Sysname2>
```

## telnet ipv6

**Syntax** **telnet ipv6** *remote-system* [ **-i** *interface-type interface-number* ] [ *port-number* ]

**View** User view

**Parameters** *remote-system*: IPv6 address or host name of the remote system. An IPv6 address can be up to 46 characters; a host name is a string of 1 to 20 characters.

**-i interface-type interface-number**: Specifies the outbound interface by interface type and interface number. The outbound interface is required when the destination address is a local link address.

*port-number*: TCP port number assigned to Telnet service on the remote system, in the range 0 to 65535 and defaults to 23.

**Description** Use the **telnet ipv6** command to telnet to a remote device for remote management. You can terminate a Telnet connection by pressing <Ctrl + K>.

**Examples** # Telnet to the device with IPv6 address 3001::1.

```
<Sysname> telnet ipv6 3001::1
Trying 3001::1 ...
Press CTRL+K to abort
Connected to 3001::1 ...

* Copyright (c) 2004-2007 3Com Corporation All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-switch fabricering shall be allowed. *

<Sysname>
```

## telnet client source

**Syntax** **telnet client source** { **ip** *ip-address* | **interface** *interface-type interface-number* }

**undo telnet client source****View** System view**Parameters** None**Description** Use the **telnet client source** command to specify the source IP address or source interface for the Telnet packets to be sent.Use the **undo telnet client source** command to remove the source IP address or source interface configured for Telnet packets.

By default, source IP address or source interface of the Telnet packets sent is not configured.

**Examples** # Specify the source IP address for Telnet packets.

```
<Sysname> system-view
[Sysname] telnet client source ip 129.102.0.2
```

# Remove the source IP address configured for Telnet packets.

```
[Sysname] undo telnet client source
```

**telnet server enable****Syntax** **telnet server enable**  
**undo telnet server enable****View** System view**Parameters** None**Description** Use the **telnet server enable** command to make the switch to operate as a Telnet Server.Use the **undo telnet server enable** command disable the switch from operating as a Telnet server.

By default, a switch does not operate as a Telnet server.

**Examples** # Make the switch to operate as a Telnet Server.

```
<Sysname> system-view
[Sysname] telnet server enable
% Start Telnet server
```

# Disable the switch from operating as a Telnet server.

```
[Sysname] undo telnet server enable
% Close Telnet server
```

---

## terminal type

**Syntax** `terminal type { ansi | vt100 }`

`undo terminal type`

**View** User interface view

**Parameters** **ansi**: Specifies the terminal display type to ANSI.

**vt100**: Specifies the terminal display type to VT100.

**Description** Use the **terminal type** command to configure the type of terminal display.

Use the **undo terminal type** command to restore the default.

Currently, the system support two types of terminal display: ANSI and VT100.

By default, the terminal display type is ANSI. The device must use the same display type as the terminal. If the terminal uses VT 100, the device should also use VT 100.

**Examples** # Set the terminal display type to VTY 100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] terminal type vt100
```

---

## user-interface

**Syntax** `user-interface [ type ] first-number [ last-number ]`

**View** System view

**Parameters** *type*: User interface type.

*first-number*: User interface index, which identifies the first user interface to be configured.

*last-number*: User interface index, which identifies the last user interface to be configured.

**Description** Use the **user-interface** command to enter one or more user interface views to perform configuration.

**Examples** # Enter VTY 0 user interface view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
```

```
[Sysname] user-interface vty 0
[Sysname-ui-vty0]
```

---

## user privilege level

**Syntax** `user privilege level level`

`undo user privilege level`

**View** User interface view

**Parameters** *level*: Command level ranging from 0 to 3.

**Description** Use the **user privilege level** command to configure the command level available to the users logging into the user interface.

Use the **undo user privilege level** command to revert to the default command level.

By default, the commands of level 3 are available to the users logging into the AUX user interface. The commands of level 0 are available to the users logging into VTY user interfaces.

**Examples** # Configure that commands of level 0 are available to the users logging into VTY 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] user privilege level 0
```

# You can verify the above configuration by Telnetting to VTY 0 and displaying the available commands, as listed in the following.

```
<Sysname> ?
User view commands:
 cluster Run cluster command
 language-mode Specify the language environment
 ping Ping function
 quit Exit from current command view
 super Set the current user priority level
 telnet Establish one TELNET connection
 tracert Trace route function
 undo Undo a command or set to its default status
```



# 2

## USER LOGIN COMMANDS

---

### acl

**Syntax** `acl [ ipv6 ] acl-number { inbound | outbound }`  
`undo acl [ ipv6 ] { inbound | outbound }`

**View** User interface view

**Parameters** *acl-number*: ACL number ranging from 2000 to 4999, where:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Layer 2 ACLs

**ipv6** *acl-number*: IPv6 ACL number ranging from 2000 to 3999.

**inbound**: Filters the users Telnetting to the current switch.

**outbound**: Filters the users Telnetting to other switches from the current switch.

**Description** Use the **acl** command to apply an ACL to filter Telnet users.

Use the **undo acl** command to disable the switch from filtering Telnet users using the ACL.

Note that if you use Layer 2 ACL rules, you can only choose the **inbound** keyword in the command here.

**Examples** # Apply ACL 2000 to filter users Telnetting to the current switch (assuming that ACL 2,000 already exists.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

---

### snmp-agent community

**Syntax** `snmp-agent community { read | write } community-name [ mib-view view-name | acl acl-number ]*`

**undo snmp-agent community** *community-name*

**View** System view

**Parameters** **read**: Specifies that the community has read-only permission in the specified view.

**write**: Specifies that the community has read/write permission in the specified view.

*community-name*: Community name, a string of 1 to 32 characters.

**mib-view**: Sets the name of the MIB view accessible to the community.

*view-name*: MIB view name, a string of 1 to 32 characters.

**acl** *acl-number*: Specifies the ACL number. The *acl-number* argument ranges from 2,000 to 2,999.

**Description** Use the **snmp-agent community** command to set a community name and to enable users to access the switch through SNMP. You can also optionally use this command to apply an ACL to filter network management users.

Use the **undo snmp-agent community** command to cancel community-related configuration for the specified community.

By default, SNMPv1 and SNMPv2c access a switch by community names.

**Examples** # Set the community name to "h3c", enable users to access the switch in the name of the community (with read-only permission), and apply ACL 2,000 to filter network management users (assuming that ACL 2000 already exists.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent community read h3c acl 2000
```

## snmp-agent group

**Syntax** **snmp-agent group** { **v1** | **v2c** } *group-name* [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ]

**undo snmp-agent group** { **v1** | **v2c** } *group-name*

**snmp-agent group v3** *group-name* [ **authentication** | **privacy** ] [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ]

**undo snmp-agent group v3** *group-name* [ **authentication** | **privacy** ]

**View** System view

**Parameters** **v1**: Specifies to adopt v1 security scheme.



**v2c:** Specifies to adopt v2c security scheme.

**v3:** Specifies to adopt v3 security scheme.

*group-name:* Group name, a string of 1 to 32 characters.

**authentication:** Specifies to authenticate SNMP data without encrypting the data.

**privacy:** Authenticates and encrypts packets.

**read-view:** Sets a read-only view.

*read-view:* Name of the view to be set to read-only, a string of 1 to 32 characters.

**write-view:** Sets a readable & writable view.

*write-view:* Name of the view to be set to readable & writable, a string of 1 to 32 characters.

**notify-view:** Sets a notifying view.

*notify-view:* Name of the view to be set to a notifying view, a string of 1 to 32 characters.

**acl *acl-number*:** Specifies an ACL. The *acl-number* argument ranges from 2000 to 2999.

**Description** Use the **snmp-agent group** command to configure a SNMP group. You can also optionally use this command to apply an ACL to filter network management users.

Use the **undo snmp-agent group** command to remove a specified SNMP group.

**Examples** # Create a SNMP group named **h3c** and apply ACL 2001 to filter network management users (assuming that ACL 2001 already exists).

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent group v1 h3c acl 2001
```

---

## snmp-agent usm-user

**Syntax** **snmp-agent usm-user** { **v1** | **v2c** } *user-name* *group-name* [ **acl** *acl-number* ]

**undo snmp-agent usm-user** { **v1** | **v2c** } *user-name* *group-name*

**snmp-agent usm-user v3** *user-name* *group-name* [ **authentication-mode** { **md5** | **sha** } *auth-password* [ **privacy-mode** { **des56** | **aes128** } *priv-password* ] ] [ **acl** *acl-number* ]

**undo snmp-agent usm-user v3** *user-name* *group-name* { **local** | **switch** **fabricid** *switch fabricid-string* }

**View** System view

**Parameters** **v1**: Specifies to adopt v1 security scheme.

**v2c**: Specifies to adopt v2c security scheme.

**v3**: Specifies to adopt v3 security scheme.

*user-name*: User name, a string of 1 to 32 characters.

*group-name*: Group name the user corresponds to, a string of 1 to 32 characters.

**authentication-mode**: Specifies to authenticate users.

**md5**: Specifies the authentication protocol to be HMAC-MD5-96.

**sha**: Specifies the authentication protocol to be HMAC-SHA-96.

*auth-password*: Authentication password. This argument can be of 1 to 64 characters.

**privacy**: Specifies to encrypt data.

**des56**: Specifies the privacy protocol to be Data Encryption Standard (DES for short).

**aes128**: Specifies the privacy protocol to be Advanced Encryption Standard (AES for short).

*priv-password*: Encrypting password, a string of 1 to 64 characters.

**acl** *acl-number*: Specifies the ACL number. The *acl-number* argument ranges from 2,000 to 2,999.

**local**: Specifies the user to be a local user entity.

**switch fabricid**: Specifies the ID of the switch fabric associated with the user.

*switch fabricid-string*: Engine ID string, 10 to 64 even number of hexadecimal numbers. Odd number of hexadecimal numbers, all-zero, or all-F hexadecimal numbers are all regarded as invalid parameters.

**Description** Use the **snmp-agent usm-user** command to add a user to a specified SNMP group. You can also optionally use this command to apply an ACL to filter network management users.

Use the **undo snmp-agent usm-user** command to remove a user from the corresponding SNMP group. The operation also frees the user from the corresponding ACL-related configuration.

**Examples** # Add the user named **h3c** to the SNMP group named **h3cgroup**, specifying to authenticate the user, specifying the authentication protocol to be HMAC-MD5-96, the authentication password to be **abc**, and applying ACL 2002 to filter network management users (assuming that ACL 2002 already exists).

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent usm-user v3 h3c h3cgroup authentication-mode md
5 abc acl 2002
```



# 3

## ETHERNET PORT CONFIGURATION COMMANDS

---

### broadcast-suppression

**Syntax** **broadcast-suppression** { *ratio* | **pps** *max-pps* }

**undo broadcast-suppression**

**View** Ethernet port view, port group view

**Parameters** *ratio*: Maximum ratio of broadcast traffic to the total transmission capability of an Ethernet port, in the range of 1 to 100. The smaller the ratio, the less broadcast traffic is allowed to pass through the port.

**pps** *max-pps*: Specifies the maximum broadcast packet number per second for an Ethernet port, in pps, representing packets per second. The value range of *max-pps* varies with port types.

**Description** Use the **broadcast-suppression** command to configure the broadcast storm suppression ratio for one or multiple ports.

Use the **undo broadcast-suppression** command to restore the default broadcast storm suppression ratio.

By default, all broadcast traffic is allowed to pass through an Ethernet port, that is, broadcast traffic is not suppressed.

If you execute this command in Ethernet port view, the configurations take effect only on the current port. If you execute this command in port-group view, the configurations take effect on all ports in the port group.

Note that when broadcast traffic exceeds the maximum value configured, the system will discard the extra packets so that the broadcast traffic ratio falls below the limit to ensure that the network functions properly.



*Do not use the **broadcast-suppression** command along with the **storm-constrain** command. Otherwise, the multicast storm suppression ratio configured may get invalid.*

**Examples** # Allow broadcast traffic equivalent to 20% of the total transmission capability of Ethernet 2/0/1 to pass and suppress the excessive broadcast packets.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] broadcast-suppression 20
```

# On all the ports of the manual port group named **group1**, allow broadcast traffic equivalent to 20% of the total transmission capability of each port to pass and suppress excessive broadcast packets.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member ethernet 2/0/1
[Sysname-port-group manual group1] group-member ethernet 2/0/2
[Sysname-port-group manual group1] broadcast-suppression 20
```

---

## description

**Syntax** **description** *text*

**undo description**

**View** Ethernet port view

**Parameters** *text*: Description of an Ethernet port, a string of 1 to 80 characters.

**Description** Use the **description** command to configure the description of an Ethernet port.

Use the **undo description** command to remove the description.

By default, the description of an Ethernet port is the port name followed by the "interface" string, **Ethernet2/0/1 Interface** for example.

**Examples** # Configure the description of port Ethernet 2/0/1 as **lanswitch-interface**.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] description lanswitch-interface
```

---

## display brief interface

**Syntax** **display brief interface** [ *interface-type* [ *interface-number* ] ] [ [ { **begin** | **include** | **exclude** } *text* ]

**View** Any view

**Parameters** *interface-type*: Type of a specified port.

*interface-number*: Number of a specified port.

[ ]: Uses a regular expression to filter output information.

**begin**: Displays the line that matches the regular expression and all the subsequent lines. For detailed description on regular expression, refer to "Parameters" on page 1165.

**include:** Displays the lines that match the regular expression.

**exclude:** Displays the lines that do not match the regular expression.

*text:* Regular expression. a string of 1 to 256 characters. Note that this argument is case-sensitive.

**Description** Use the **display brief interface** command to display brief port information, including simple port name, link state, protocol link state, protocol type, and main IP address.

- If neither port type nor port number is specified, all port information will be displayed;
- If only port type is specified, then only information of this particular type of port will be displayed.
- If both port type and port number are specified, then only information of the specified port will be displayed.

**Related commands:** **interface.**

**Examples** # Display brief information of port(s).

```
<Sysname> display brief interface
The brief information of interface(s) under route mode:
Interface Link Protocol-link Protocol type Main IP
Loop0 UP UP(spoofing) LOOP 10.1.1.1
NULL0 UP UP(spoofing) NULL --
Tun0 DOWN DOWN TUNNEL --
Vlan1 DOWN DOWN ETHERNET 2.2.2.2
Vlan2 UP UP ETHERNET 1.1.1.1
```

```
The brief information of interface(s) under bridge mode:
Interface Link Speed Duplex Link-type PVID
Eth2/0/1 DOWN auto auto access 1
Eth2/0/2 UP 100M(a) full(a) access 1
Eth2/0/3 DOWN auto auto access 1
Eth2/0/4 DOWN auto auto access 1
Eth2/0/5 DOWN auto auto access 1
Eth2/0/6 DOWN auto auto access 1
Eth2/0/7 DOWN auto auto access 1
```

(The remain output information is omitted.)

# Display brief port information that contains the string **UP**.

```
<Sysname> display brief interface | include UP
The brief route information of interface(s) under route mode:
Interface Link Protocol-link Protocol type Main IP
Loop0 UP UP(spoofing) LOOP 10.1.1.1
NULL0 UP UP(spoofing) NULL --
Vlan2 UP UP ETHERNET 1.1.1.1

The brief information of interface(s) under bridge mode:
Interface Link Speed Duplex Link-type PVID
Eth2/0/2 UP 100M(a) full(a) access 1
```

**Table 4** Field descriptions of the display brief interface command.

Field	Description
The brief information of interface(s) under route mode	Brief information of port(s) in route mode
Interface	Port name
Link	Port physical link state, which can be up or down
Protocol-link	Port protocol link state, which can be up or down
Protocol type	Port protocol type
Main IP	Main IP
The brief information of interface(s) under bridge mode	Brief information of port(s) in bridge mode
Speed	Port rate, in bps
Duplex	Duplex mode, which can be half (half duplex), full (full duplex), or auto (auto-negotiation).
PVID	Default VLAN ID

**Table 5** Acronyms for different types of ports

Port name	Acronyms
Ethernet	Eth
GigabitEthernet	GE
Ten-GigabitEthernet	XGE

---

## display interface

**Syntax** **display interface** [ *interface-type* [ *interface-number* ] ]

**View** Any view

**Parameters** *interface-type*: Type of a specified port.

*interface-number*: Number of a specified port.

**Description** Use the **display interface** command to display the current state of a specified port and related information.

- If neither port type nor port number is specified, all port information will be displayed;
- If only port type is specified, then only information of this particular type of port will be displayed.
- If both port type and port number are specified, then only information of the specified port will be displayed.

**Related commands:** **interface**.

**Examples** # Display the current state of port Ethernet 2/0/1 and related information.



```

<Sysname> display interface ethernet 2/0/1
Ethernet2/0/1 current state: DOWN
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e200-2200
Description: Ethernet2/0/1 Interface
Loopback is not set
Media type is twisted pair, Port hardware type is 100_BASE_TX
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 1536
Broadcast MAX-ratio: 100%
Unicast MAX-ratio: 100%
Multicast MAX-ratio: 100%
PVID: 1
Mdi type: auto
Link delay is 0(sec)
Port link-type: access
 Tagged VLAN ID : none
 Untagged VLAN ID : 1
Port priority: 0
Last 300 seconds input: 0 packets/sec 0 bytes/sec -%
Last 300 seconds output: 0 packets/sec 0 bytes/sec -%
Input (total): 0 packets, 0 bytes
 0 broadcasts, 0 multicasts
Input (normal): 0 packets, - bytes
 0 broadcasts, 0 multicasts
Input: 0 input errors, 0 runts, 0 giants, 0 throttles
 0 CRC, 0 frame, - overruns, 0 aborts
 - ignored, - parity errors
Output (total): 0 packets, 0 bytes
 0 broadcasts, 0 multicasts, 0 pauses
Output (normal): 0 packets, - bytes
 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
 0 aborts, 0 deferred, 0 collisions, 0 late collisions
 0 lost carrier, - no carrier

```

**Table 6** Field descriptions of the display interface command (in bridge mode)

Field	Description
Ethernet2/0/1 current state	Current physical link state of the Ethernet port
IP Packet Frame Type	Frame type of the Ethernet port
Hardware address	Hardware address
Description	Description of the port
Loopback is not set	Loopback is not configured
Unknown-speed mode	Unknown-speed mode, in which mode speed is negotiated between the current host and the peer
unknown-duplex mode	unknown-duplex mode, in which mode speed is negotiated between the current host and the peer
Link speed type is auto negotiation	Link speed type is auto negotiation
link duplex type is auto negotiation	Link duplex type is auto negotiation
Flow-control is not enabled	Flow-control is not enabled
The Maximum Frame Length	The maximum frame length allowed on a port
Broadcast MAX-ratio	Broadcast storm suppression ratio (the maximum ratio of allowed number of broadcast packets to overall traffic through a port)

**Table 6** Field descriptions of the display interface command (in bridge mode)

Field	Description
Unicast MAX-ratio	Unicast storm suppression ratio (the maximum ratio of allowed number of unknown unicast packets to overall traffic through a port)
Multicast MAX-ratio	Multicast storm suppression ratio (the maximum ratio of allowed number of multicast packets to overall traffic through a port)
PVID	Default VLAN ID
Mdi type	Cable type
Link delay	Suppression time of physical-link-state changes on an Ethernet Port.
Port link-type	Port link type, which could be access, trunk, and hybrid.
Tagged VLAN ID	Identify the VLANs that need Tag markers
Untagged VLAN ID	Identify the VLANs that do not need Tag markers
Last 300 seconds input	Average input rate over the last 300 seconds,; among which: <ul style="list-style-type: none"> <li>■ <b>packets/sec</b> indicates the average input rate in terms of the average number of the packets received per second.</li> <li>■ <b>bytes/sec</b> indicates the average input rate in terms of the average number of bytes received per second.</li> <li>■ <b>x%</b> indicates the percentage of this average input rate to the total bandwidth, where "-" indicates that the rate is greater than the maximum value that can be displayed.</li> </ul>
Last 300 seconds output	Average output rate over the last 300 seconds, among which: <ul style="list-style-type: none"> <li>■ <b>packets/sec</b> indicates the average output rate in terms of the average number of the packets output per second.</li> <li>■ <b>bytes/sec</b> indicates the average output rate in terms of the average number of bytes output per second.</li> <li>■ <b>x%</b> indicates the percentage of this average output rate to the total bandwidth, where "-" indicates that the rate is greater than the maximum value that can be displayed.</li> </ul>
Input (total):	Error statistics on the port inbound and outbound packets, underscore indicates that the corresponding entry is invalid
Input (normal):	
Input:	
Output (total):	
Output (normal):	
Output:	

---

## display loopback-detection

**Syntax** `display loopback-detection`

**View** Any view

**Parameters** None

**Description** Use the **display loopback-detection** command to display loopback detection information on a port

If loopback detection is already enabled, this command will also display the detection interval and information on the ports currently detected with a loopback.

**Examples** # Display loopback detection information on a port.

```
<Sysname> display loopback-detection
Loopback-detection is running
Detection interval time is 30 seconds
No port is detected with loopback
```

**Table 7** Field descriptions of the display loopback-detection command.

Field	Description
Loopback-detection is running	Loopback-detection is running
Detection interval time is 30 seconds	Detection interval is 30 seconds
No port is detected with loopback	No port is currently being detected with a loopback

---

## display port-group manual

**Syntax** **display port-group manual** [**all** | **name** *port-group-name* ]

**View** Any view

**Parameters** **all**: Specifies all the manual port groups.

**name** *port-group-name*: Specifies the name of a manual port group, a string of 1 to 32 characters.

**Description** Use the **display port-group manual** command to display the information about a manual port group or all the manual port groups.

- If you provide the *port-group-name* argument, this command displays the details for a specified manual port group, including its name and the Ethernet ports included.
- If you provide the **all** keyword, this command displays the details for all manual port groups, including their names and the Ethernet ports included.
- Absence of parameters indicates that the names of all port groups will be displayed.

**Examples** # Display the names of all the port groups.

```
<Sysname> display port-group manual
The following manual port group exist(s):
 group1 group2
```

# Display details of all the manual port groups.

```
<Sysname> display port-group manual all
Member of group1:
 Ethernet2/0/4 Ethernet2/0/6

Member of group2:
 None
```

**Table 8** Field descriptions of the display port-group manual command

Field	Description
The following manual port group exist(s)	List of the existing port groups
Member of group	Member of the manual port group

## display storm-constrain

**Syntax** **display storm-constrain** [ **broadcast** | **multicast** ] [ **interface** *interface-type interface-number* ]

**View** Any view

**Parameters** **broadcast**: Displays the information about storm constrain for broadcast packets.

**multicast**: Displays the information about storm constrain for multicast packets.

**interface** *interface-type interface-number*: Specifies a port by its number and type. The storm constrain information about the port will be displayed.

**Description** Use the **display storm-constrain** command to display the information about storm constrain.

If you provide no argument or keyword, this command displays the information about storm constrain for all types of packets on all the ports.

**Examples** # Display the information about storm constrain for all types of packets on all the ports.

```
<Sysname> display storm-constrain
Flow Statistic Interval: 10(second)
PortName StormType LowerLimit UpperLimit Ctr-mode Status Trap Log Swi-num

Eth2/0/1 broadcast 50 200 N/A normal on on 0
```

**Table 9** Field descriptions of the display storm-constrain command

Field	Description
Flow Statistic Interval	Interval for generating storm constrain statistics
PortName	Simplified port index
StormType	Type of the packets for which storm constrain function is enabled, which can be broadcast (for broadcast packets), multicast (for multicast packets)
LowerLimit	Lower threshold (in pps)
UpperLimit	Upper threshold (in pps)
Ctr-mode	Action to be taken when the upper threshold is reached, which can be block, shutdown, and N/A.

**Table 9** Field descriptions of the display storm-constrain command

Field	Description
Status	Port state, which can be normal (indicating the port operates properly), control (indicating the port is blocked or shut down).
Trap	State of trap messages sending. "on" indicates trap message sending is enabled; "off" indicates trap message sending is disabled.
Log	State of log sending. "on" indicates log sending is enabled; "off" indicates log sending is disabled.
Swi-num	Number of the forwarding state switching. This field is numbered modulo 65,536.

---

## duplex

**Syntax** **duplex** { **auto** | **full** | **half** }

**undo duplex**

**View** Ethernet port view

**Parameters** **auto**: Indicates that the port is in an auto-negotiation state.

**full**: Indicates that the port is in a full-duplex state.

**half**: Indicates that the port is in a half-duplex state.

**Description** Use the **duplex** command to configure the duplex mode for an Ethernet port.

Use the **undo duplex** command to restore the duplex mode for an Ethernet port to the default.

By default, the duplex mode for an Ethernet port is auto.

**Related commands:** **speed**.



*You are recommended to configure the same rate and duplex mode for two interconnected ports to avoid packet loss.*

**Examples** # Configure the port Ethernet 2/0/1 to work in full-duplex mode.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] duplex full
```

---

## flow-control

**Syntax** **flow-control**

**undo flow-control**

**View** Ethernet port view

**Parameters** None

**Description** Use the **flow-control** command to enable flow control on an Ethernet port.  
Use the **undo flow-control** command to disable flow control on an Ethernet port.  
By default, flow control on an Ethernet port is disabled.



*The flow control function takes effect on the local Ethernet port only when it is enabled on both the local and peer devices.*

**Examples** # Enable flow control on port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] flow-control
```

## flow-interval

**Syntax** **flow-interval** *interval*

**undo flow-interval**

**View** Ethernet port view

**Parameters** *interval*: Interval for collecting port statistics, in the range 5 to 300 (in seconds). Note that this argument must be a multiple of 5. The system default is 300 seconds.

**Description** Use the **flow-interval** command to set the interval for collecting port statistics.  
Use the **undo flow-interval** command to restore the default.

**Examples** # Set the interval for collecting statistics to 100 seconds on Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] flow-interval 100
```

## group-member

**Syntax** **group-member** *interface-list*

**undo group-member** *interface-list*

**View** Port group view

**Parameters** *interface-list*: Ethernet port list, in the form of *interface-type interface-number* [ **to interface-type interface-number** ] &<1-10>, where &<1-10> indicates that you can specify up to 10 port or port ranges

**Description** Use the **group-member** command to add an Ethernet port to a specified manual port group.

Use the **undo group-member** command to remove a specified Ethernet port from a manual port group.

By default, a manual port group is empty, that is, there is no Ethernet port in it.

**Examples** # Add port Ethernet 2/0/1 to the manual port group named **group 1**.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member ethernet 2/0/1
```

## interface

**Syntax** **interface** *interface-type interface-number*

**View** System view

**Parameters** *interface-type interface-number*: Port type and port number.

**Description** Use the **interface** command to enter the related port view.

**Examples** # Enter Ethernet 2/0/1 port view.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1]
```

## jumboframe enable

**Syntax** **jumboframe enable** [ *value* ]

**undo jumboframe enable**

**View** Ethernet port view, port group view

**Parameters** *value*: Maximum frame length allowed on an Ethernet port. This argument ranges from 1536 to 9216 (in bytes) and defaults to 1536.

**Description** Use the **jumboframe enable** command to enable the forwarding of jumbo frames and set the maximum frame length allowed on an Ethernet port.

Use the **undo jumboframe enable** command to set the maximum frame length allowed on an Ethernet port to 1518 bytes.

By default, the maximum frame length allowed on an Ethernet port is 1536 bytes.

You can configure in Ethernet port view or port-group view to allow jumbo frames with specified length to pass through Ethernet ports.

- Execution of this command under Ethernet port view will only apply the configuration to the current Ethernet port.
- Execution of this command under port group view will apply the configurations to all the ports in the port group.



*If you execute the **jumboframe enable** command repeatedly, the latest configuration takes effect.*

**Examples** # Enable jumbo frames under 1560 bytes to pass through Ethernet port 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] jumboframe enable 1560
```

# Enable jumbo frames to pass through all the Ethernet ports in the manual port group named **group1**.

```
[Sysname-Ethernet2/0/1] quit
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member ethernet 2/0/2
[Sysname-port-group manual group1] group-member ethernet 2/0/3
[Sysname-port-group manual group1] jumboframe enable
```

---

## link-delay

**Syntax** **link-delay** *delay-time*

**undo link-delay**

**View** Ethernet port view

**Parameters** *delay-time*: Up/down suppression time for the physical connection of an Ethernet port (in seconds). The value ranges from 0 to 30. The system default is 0.

**Description** Use the **link-delay** command to configure the suppression time of physical-link-state changes on an Ethernet Port.

Use the **undo link-delay** command to restore the default suppression time.

The default suppression time of physical-link-state changes on an Ethernet port is 0 seconds, indicating that if the port state changes, the port reports the change to the system immediately.



**Examples** # Set the up/down suppression time of the physical connection of an Ethernet port to 8 seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] link-delay 8
```

---

## loopback

**Syntax** **loopback** { **external** | **internal** }

**View** Ethernet port view

**Parameters** **external**: Enables external loopback test on an Ethernet port.

**internal**: Enables internal loopback test on an Ethernet port.

**Description** Use the **loopback** command to enable Ethernet port loopback test.

By default, Ethernet port loopback test is disabled.



- *Ethernet port loopback test should be enabled while testing certain functionalities, such as during the initial identification of any network failure.*
- *While enabled, Ethernet port loopback test will work in a full-duplex mode. The port will return to its original state upon completion of the loopback testing.*

**Examples** # Enable internal loopback test on Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] loopback internal
Loop internal succeeded!
```

---

## loopback-detection control enable

**Syntax** **loopback-detection control enable**

**undo loopback-detection control enable**

**View** Ethernet port view

**Parameters** None

**Description** Use the **loopback-detection control enable** command to enable loopback detection for a Trunk port or Hybrid port.

Use the **undo loopback-detection control enable** command to restore the default.

By default, loopback detection for a Trunk port or Hybrid port is disabled.

- When the loopback detection is enabled, if a port has been detected with loopback, it will be shutdown. A Trap message will be sent to the terminal and the corresponding MAC address forwarding entries will be deleted.
- When the loopback detection is disabled, if a port has been detected with loopback, a Trap message will be sent to the terminal. The port is still working properly.

By default, loopback detection for Trunk port and Hybrid port is disabled.

Note that this command is inapplicable to an Access port as its loopback detection is enabled by default.

**Examples** # Enable loopback detection for trunk port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type trunk
[Sysname-Ethernet2/0/1] loopback-detection enable
[Sysname-Ethernet2/0/1] loopback-detection control enable
```

---

## loopback-detection enable

**Syntax** **loopback-detection enable**

**undo loopback-detection enable**

**View** System view, Ethernet port view

**Parameters** None

**Description** Use the **loopback-detection enable** command to enable loopback detection globally or on a specified port.

Use the **undo loopback-detection enable** command to disable loopback detection globally or on a specified port.

By default, loopback detection is disabled for an Access, Trunk, or Hybrid port.

- If an Access port has been detected with loopback, it will be shutdown. A Trap message will be sent to the terminal and the corresponding MAC address If a Trunk port or Hybrid port has been detected with loopback, a Trunk message will be sent to the terminal. They will be shutdown if the loopback testing function is enabled on them. In addition, a Trap message will be sent to the terminal and the corresponding MAC address forwarding entries will be deleted.

**Related commands:** **loopback-detection control enable.**

**CAUTION:**

- Loopback detection on a given port is enabled only after the `loopback-detection enable` command has been issued in both system view and the port view of the port.
- Loopback detection on all ports will be disabled after the issuing of the `undo loopback-detection enable` command under system view.

**Examples** # Enable loopback detection on port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] loopback-detection enable
```

## loopback-detection interval-time

**Syntax** `loopback-detection interval-time time`

`undo loopback-detection interval-time`

**View** System view

**Parameters** *time*: Time interval for performing port loopback detection, in the range 5 to 300 (in seconds).

**Description** Use the **loopback-detection interval-time** command to configure time interval for performing port loopback detection.

Use the **undo loopback-detection interval-time** command to restore the default time interval for port loopback detection, which is 30 seconds.

**Related commands:** `display loopback-detection`.

**Examples** # Set the time interval for performing port loopback detection to 10 seconds.

```
<Sysname> system-view
[Sysname] loopback-detection interval-time 10
```

## loopback-detection per-vlan enable

**Syntax** `loopback-detection per-vlan enable`

`undo loopback-detection per-vlan enable`

**View** Ethernet port view

**Parameters** None

**Description** Use the **loopback-detection per-vlan enable** command to enable loopback detection in all VLANs with Trunk ports or Hybrid ports.

Use the **undo loopback-detection per-vlan enable** command to enable loopback detection in the default VLAN with Trunk ports or Hybrid ports.

By default, loopback detection is only enabled in the default VLAN(s) with Trunk ports or Hybrid ports.

Note that the **loopback-detection per-vlan enable** command is not applicable to Access ports.

**Examples** # Enable loopback detection in all the VLANs to which the hybrid port Ethernet 2/0/1 belongs.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] loopback-detection enable
[Sysname-Ethernet2/0/1] port link-type trunk
[Sysname-Ethernet2/0/1] loopback-detection per-vlan enable
```

---

## mdi

**Syntax** **mdi** { **across** | **auto** | **normal** }

**undo mdi**

**View** Ethernet port view

**Parameters** **across**: Specifies cross-over cables for the Ethernet port.

**auto**: Configures the Ethernet port to sense the cable type automatically.

**normal**: Specifies straight-through cables for the Ethernet port.

**Description** Use the **mdi** command to configure the cable type that can be sensed by an Ethernet port.

Use the **undo mdi** command to restore the system default.

By default, an Ethernet port senses the type of the network cable connected to it automatically.

**Examples** # Configure the port Ethernet 2/0/1 to use cross over cable.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] mdi across
```

---

## multicast-suppression

**Syntax** `multicast-suppression { ratio | pps max-pps }`

`undo multicast-suppression`

**View** Ethernet port view, port group view

**Parameters** *ratio*: Maximum ratio of multicast traffic to the total transmission capability of an Ethernet port, in the range of 1 to 100. The smaller the ratio is, the less multicast traffic is allowed to pass through the port.

**pps** *max-pps*: Specifies the maximum number of multicast packets passing an Ethernet port per second, in pps, representing packets per second. The value range of *max-pps* varies with port types.

**Description** Use the **multicast-suppression** command to configure multicast storm suppression ratio on an port.

Use the **undo multicast-suppression** command to restore the default multicast suppression ratio.

By default, all multicast traffic is allowed to go through an Ethernet port, that is, multicast traffic is not suppressed.

If you execute this command in Ethernet port view, the configurations take effect only on the current port. If you execute this command in port-group view, the configurations take effect on all ports in the port group.

Note that when multicast traffic exceeds the maximum value configured, the system will discard the extra packets so that the multicast traffic ratio can drop below the limit to ensure that the network functions properly.



- *If a suppression ratio is set in global configuration mode or in port configuration mode, the suppression ratio which first satisfies the condition takes effect.*
- *If you set different suppression ratios in Ethernet port view or port-group view for multiple times, the latest configuration takes effect.*
- *Do not use the **multicast-suppression** command along with the **storm-constrain** command. Otherwise, the multicast storm suppression ratio configured may get invalid.*

**Examples** # Allow multicast traffic equivalent to 20% of the total transmission capability to pass through Ethernet 2/0/1 and suppress the excessive multicast packets.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] multicast-suppression 20
```

# On all the ports of the manual port group named **group1**, allow multicast traffic equivalent to 20% of the total transmission capability of each port to pass and suppress excessive multicast packets.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member ethernet 2/0/1
[Sysname-port-group manual group1] group-member ethernet 2/0/2
[Sysname-port-group manual group1] multicast-suppression 20
```

---

## port-group

**Syntax** **port-group** { **manual** *port-group-name* | **aggregation** *agg-id* }

**undo port-group manual** *port-group-name*

**View** System view

**Parameters** **manual** *port-group-name*: Name of a specified manual port group, a string of 1 to 32 characters.

**aggregation** *agg-id*: Number of the specified port aggregation group. The specified port aggregation group must already exist. You can use the **display link-aggregation summary** command to display brief information of all existing port aggregation groups.

**Description** Use the **port-group manual** command to create a manual port group and enter manual port group view.

Use the **port-group aggregation** command to enter aggregation group view.

Use the **undo port-group manual** command to remove a manual port group.

By default, no manual port group is created.

**Examples** # Create a manual port group named **group1**.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1]
```

---

## reset counters interface

**Syntax** **reset counters interface** [ *interface-type* [ *interface-number* ] ]

**View** User view

**Parameters** *interface-type*: Port type.

*interface-number*: Port number.

- Description** Use the **reset counters interface** command to reset statistics for a specified port.
- To sample network traffic within a period of time for a port, you need to reset the original port statistics.
- If neither port type nor port number is specified, all port information will be reset;
  - If only port type is specified, then only information of this particular type of ports will be reset.
  - If both port type and port number are specified, then only information of the specified port will be reset.
- Examples** # Clear the statistics on Ethernet 2/0/1.
- ```
<Sysname> reset counters interface ethernet 2/0/1
```

shutdown

Syntax **shutdown**
undo shutdown

View Ethernet port view

Parameters None

Description Use the **shutdown** command to shut down an Ethernet port.

Use the **undo shutdown** command to turn on Ethernet port.

In certain circumstances, modification to the port parameters does not immediately take effect, and therefore, you need to shut down the relative port to make the modification work.

Examples # Shut down the port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] shutdown
```

Bring up the port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] undo shutdown
```

speed

Syntax **speed { 10 | 100 | 1000 | auto }**

undo speed**View** Ethernet port view

Parameters **10**: Specifies the port rate as 10 Mbps.
100: Specifies the port rate as 100 Mbps.
1000: Specifies the port rate as 1,000 Mbps.
auto: Specifies to determine the port rate through auto-negotiation.

Description Use the **speed** command to configure Ethernet port data rate.
 Use the **undo speed** command to restore Ethernet port data rate.
 By default, Ethernet port data rate is automatically negotiated between peer Ethernet ports.
 Note that the **speed 1000** command is only applicable to Gigabit Ethernet ports.

Related commands: **duplex.**

You are recommended to configure the same rate and duplex mode for two interconnected ports to avoid packet loss.

Examples # Configure the port rate as 100 Mbps for port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] speed 100
```

storm-constrain

Syntax **storm-constrain { broadcast | multicast } pps max-pps-values min-pps-values**
undo storm-constrain { all | broadcast | multicast }

View Ethernet port view

Parameters **all**: Disables the storm constrain function for all types of packets (that is, multicast packets, and broadcast packets).
broadcast: Enables/Disables the storm constrain function for broadcast packets.
multicast: Enables/Disables the storm constrain function for multicast packets.
pps: Specifies the thresholds to be configured are measured in pps.
max-pps-values: Upper threshold to be set, in pps, representing packets per second. The value range of max-pps varies with port types.

min-pps-values: Lower threshold to be set, in the range 1 to *max-pps-values* (in pps).

Description Use the **storm-constrain** command to enable the storm constrain function for specific type of packets and set the upper and lower thresholds.

Use the **undo storm-constrain** command to disable the storm constrain function for specific type of packets.

By default, the storm constrain function is not enabled.



- Do not use the **storm-constrain** command along with the **multicast-suppression** command, or the **broadcast-suppression** command. Otherwise, traffics may be suppressed in an unpredictable way.
- An upper threshold cannot be less than the corresponding lower threshold. Besides, do not configure the two thresholds to the same value.

Examples # Enable the storm constrain function for broadcast packets on Ethernet 2/0/1, setting the upper and lower threshold to 200 pps and 150 pps.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] storm-constrain broadcast pps 200 150
```

storm-constrain control

Syntax **storm-constrain control { block | shutdown }**

undo storm-constrain control

View Ethernet port view

Parameters **block**: Blocks the traffic of a specific type on a port when the traffic detected exceeds the upper threshold.

shutdown: Shuts down a port when a type of traffic exceeds the corresponding upper threshold. A port shut down by the storm constrain function stops forwarding all types of packets (that is, multicast packets, and broadcast packets).

Description Use the **storm-constrain control** command to set the action to be taken when a type of traffic exceeds the corresponding upper threshold.

Use the **undo storm-constrain control** command to restore the default.

By default, no action is taken when a type of traffic exceeds the corresponding threshold.

Examples # Configure to block port Ethernet 2/0/1 when a type of traffic reaching it exceeds the corresponding upper threshold.

```

<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] storm-constrain control block

```

storm-constrain enable log

Syntax **storm-constrain enable log**
undo storm-constrain enable log

View Ethernet port view

Parameters None

Description Use the **storm-constrain enable log** command to enable log sending. With log sending enabled, the system sends log when traffic reaching a port exceeds the corresponding threshold or the traffic drops down below the lower threshold after exceeding the upper threshold.

Use the **undo storm-constrain enable log** command to disable log sending.

By default, log sending is enabled.

Examples # Disable log sending for Ethernet 2/0/1.

```

<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] undo storm-constrain enable log

```

storm-constrain enable trap

Syntax **storm-constrain enable trap**
undo storm-constrain enable trap

View Ethernet port view

Parameters None

Description Use the **storm-constrain enable trap** command to enable trap message sending. With trap message sending enabled, the system sends trap messages when traffic reaching a port exceeds the corresponding threshold or the traffic drops down below the lower threshold after exceeding the upper threshold.

Use the **undo storm-constrain enable trap** command to disable trap message sending.

By default, trap message sending is enabled.

Examples # Disable trap message sending on Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] undo storm-constrain enable trap
```

storm-constrain interval

Syntax **storm-constrain interval** *seconds*

undo storm-constrain interval

View System view

Parameters *Seconds*: Interval for generating traffic statistics, in the range 1 to 300 (in seconds).

Description Use the **storm-constrain interval** command to set the interval for generating traffic statistics.

Use the **undo storm-constrain interval** command to restore the default.

By default, the interval for generating traffic statistics is 10 seconds.



- *The interval set by the **storm-constrain interval** command is specifically for the storm constrain function. It is different from that set by the **flow-interval** command.*
- *For network stability consideration, configure the interval for generating traffic statistics to a value that is not shorter than the default.*

Examples # Set the interval for generating traffic statistics to 60 seconds.

```
<Sysname> system-view
[Sysname] storm-constrain interval 60
```

unicast-suppression

Syntax **unicast-suppression** { *ratio* | **pps** *max-pps* }

undo unicast-suppression

View Ethernet port view, port group view

Parameters *ratio*: Maximum ratio of unicast traffic to the total transmission capability of an Ethernet port, in the range of 1 to 100. The smaller the ratio is, the less unicast traffic is allowed through the port.

pps *max-pps*: Specifies the maximum number of unknown unicast packets passing through an Ethernet port per second, in pps, representing packets per second. The value range of *max-pps* varies with port types

Description Use the **unicast-suppression** command to configure a unicast storm suppression ratio.

Use the **undo unicast-suppression** command to restore the default unicast suppression ratio.

By default, all unicast traffic is allowed to go through an Ethernet port, that is, unicast traffic is not suppressed.

If you execute this command in Ethernet port view, the configurations take effect only on the current port. If you execute this command in port-group view, the configurations take effect on all ports in the port group

Note that when unicast traffic exceeds the maximum value configured, the system will discard the extra packets so that the unknown unicast traffic ratio can drop below the limit to ensure that the network functions properly.



If you set the suppression ratio repeatedly, the latest one takes effect.

Examples # Allow unicast traffic equivalent to 20% of the total transmission capability of the port to pass through Ethernet 2/0/1 and suppress the excessive unknown unicast packets.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] unicast-suppression 20
```

On all ports of the manual port group "group1", allow unknown unicast traffic equivalent to 20% of the total transmission capability of each port to pass and suppress excessive unknown unicast packets.

```
[Sysname-Ethernet2/0/1] quit
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member ethernet 2/0/2
[Sysname-port-group manual group1] group-member ethernet 2/0/3
[Sysname-port-group manual group1] unicast-suppression 20
```

4

PORT ISOLATION CONFIGURATION COMMANDS

display port-isolate group

Syntax `display port-isolate group`

View Any view

Parameters None

Description Use the **display port-isolate group** command to display the information about the system default isolation group **group1**.

Examples # Display the information about the system default isolation group.

```
<Sysname> display port-isolate group
Port-isolate group information:
Uplink port support: NO
Group ID: 2
    Ethernet2/0/4          Ethernet2/0/5
```

Table 10 Field descriptions of the display port-isolate group command

| Field | Description |
|--------------------------------|--|
| Port-isolate group information | Display information of a port-isolation group |
| Uplink port support | Whether support uplink port |
| Group ID | Isolation group number |
| Ethernet2/0/4 Ethernet2/0/5 | Ordinary ports (non-uplink ports) in a isolation group |

port-isolate enable

Syntax `port-isolate enable`
`undo port-isolate enable`

View Ethernet port view, port group view

Parameters None

Description Use the **port-isolate enable** command to add a port to the isolation group as ordinary port only.

Use the **undo port-isolate enable** command to remove the port from the isolation group.

Note that the **port-isolate enable** command adds a port to the system default isolation group **group1**.

Configured in Ethernet port view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Examples # Add port Ethernet 2/0/1 to the isolation group.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port-isolate enable
```

Add all the ports in port group **aa** to the isolation group.

```
[Sysname-Ethernet2/0/1] quit
[Sysname] port-group manual aa
[Sysname-port-group-manual-aa] group-member ethernet 2/0/2
[Sysname-port-group-manual-aa] group-member ethernet 2/0/3
[Sysname-port-group-manual-aa] group-member ethernet 2/0/4
[Sysname-port-group-manual-aa] port-isolate enable
```

5

MAC ADDRESS TABLE CONFIGURATION COMMANDS

display mac-address

Syntax `display mac-address blackhole [vlan vlan-id] [count]`

`display mac-address [mac-address [vlan vlan-id]] [dynamic | static]
[interface interface-type interface-number] [vlan vlan-id] [count]]`

View Any view

Parameters **blackhole**: Displays blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match blackhole MAC address entries are dropped.

vlan *vlan-id*: Displays MAC address entries of the specified VLAN, which is in the range 1 to 4094.

count: Displays the total number of MAC addresses in the MAC address table.

mac-address: Displays MAC address entries in a specified MAC address, in the format of H-H-H.

dynamic: Displays dynamic MAC address entries. Aging time is set for these entries.

static: Displays static MAC address entries. Similar to blackhole MAC address entries, these entries do not age but you can add or remove them.

interface *interface-type interface-number*: Displays MAC address learning status of the specified port. *interface-type interface-number* specifies a port by its type and number.

Description Use the **display mac-address** command to display information about the MAC address table.

Related commands: **mac-address, mac-address, mac-address timer.**

Examples # Display the MAC address table entry for MAC address 00e0-fc01-0101.

```
<Sysname> display mac-address 00e0-fc01-0101
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
00e0-fc01-0101  1          Config static  Ethernet2/0/2      NOAGED
```

```
--- 1 mac address(es) found ---
```

Table 11 Field descriptions of the display mac-address command

| Field | Description |
|---------------|--|
| MAC ADDR | MAC address |
| VLAN ID | ID of the VLAN to which the MAC address belongs |
| STATE | State of a MAC address, which could be Config static, Config dynamic, Learned and Blackhole |
| PORT INDEX | Port number (Displayed as N/A for a blackhole MAC address) |
| AGING TIME(s) | <p>Aging time, which could be:</p> <ul style="list-style-type: none"> ■ AGING, indicates that the entry is aging. ■ NOAGED, indicates that the entry does not age. |

display mac-address aging-time

Syntax **display mac-address aging-time**

View Any view

Parameters None

Description Use the **display mac-address aging-time** command to display the aging time of dynamic entries in the MAC address table.

Related commands: **mac-address, mac-address, mac-address timer, display mac-address.**

Examples # Display the aging time of dynamic entries in the MAC address table.

```
<Sysname> display mac-address aging-time
Mac address aging time: 300s
```

The above information indicates that the aging time of dynamic entries in the MAC address table is 300 seconds.

display mac-address mac-learning

Syntax **display mac-address mac-learning** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies a port by its type and number. Displays MAC address learning status of the specified port.

Description Use the **display mac-address mac-learning** command to display MAC address learning status of the specified or all Ethernet ports.

Examples # Display MAC address learning status of port Ethernet 2/0/3.


```
<Sysname> display mac-address mac-learning ethernet 2/0/3
Mac address learning status of the switch: enable
```

| PortName | Learning Status |
|---------------|-----------------|
| Ethernet2/0/3 | enable |

Table 12 Field descriptions of display mac-address mac-learning

| Field | Description |
|---|---|
| Mac-address learning status of the switch | Global MAC address learning status, enabled or disabled |
| PortName | Port name |
| Learning Status | MAC address learning status for a port, enabled or disabled |

mac-address

Syntax **mac-address** { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*
undo mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

View Ethernet port view

Parameters **dynamic**: Dynamic MAC address entries. Aging time is set for these entries.

static: Static MAC address entries. Similar to blackhole MAC address entries, these entries do not age but you can add or remove them.

mac-address: Specifies a MAC address in the format of H-H-H.

vlan *vlan-id*: Specifies the VLAN to which the Ethernet port belongs., where *vlan-id* is the specified VLAN ID, in the range 1 to 4094.

Description Use the **mac-address** command to add or modify a MAC address entry on a specified Ethernet port.

Use the **undo mac-address** command to remove a MAC address entry on the Ethernet port.

Note that:

- As your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic MAC address table entries however will be lost whether you save the configuration or not.
- You cannot configure a static or dynamic MAC address entry on an aggregation port.

Related commands: **display mac-address.**

Examples # Add a static entry for MAC address 00e0-fc01-0101 on port Ethernet 2/0/1 which belongs to VLAN 2.

```

<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] mac-address static 00e0-fc01-0101 vlan 2

```

mac-address

Syntax **mac-address blackhole** *mac-address* **vlan** *vlan-id*

mac-address { **dynamic** | **static** } *mac-address* **interface** *interface-type*
interface-number **vlan** *vlan-id*

undo mac-address [{ **dynamic** | **static** } *mac-address* **interface** *interface-type*
interface-number **vlan** *vlan-id*]

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] *mac-address* **interface** *interface-type*
interface-number **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type*
interface-number

View System view

Parameters **blackhole**: Blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match blackhole MAC address entries are dropped.

mac-address: Specifies a MAC address in the format of H-H-H.

vlan *vlan-id*: Specifies the VLAN to which the Ethernet port belongs., where *vlan-id* is the specified VLAN ID, in the range 1 to 4094.

dynamic: Dynamic MAC address entries. Aging time is set for these entries.

static: Static MAC address entries. Similar to blackhole MAC address entries, these entries do not age but you can add or remove them.

interface *interface-type* *interface-number*: Outbound port, with *interface-type* *interface-number* representing the port type and number.

Description Use the **mac-address** command to add or modify a MAC address entry.

Use the **undo mac-address** [{ **blackhole** | **dynamic** | **static** } *mac-address* **interface** *interface-type* *interface-number* **vlan** *vlan-id*] command to remove one or all MAC address entries.

Use the **undo mac-address** [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id* command to remove a MAC address entry, MAC address entries of a specified type, or all MAC address entries for a VLAN.

Use the **undo mac-address [blackhole | dynamic | static] interface interface-type interface-number** command to remove a MAC address entry, MAC address entries of a specified type, or all MAC address entries for an Ethernet port.

Use the **undo mac-address [blackhole | dynamic | static] [mac-address] interface interface-type interface-number vlan vlan-id** command to remove a MAC address entry or all MAC address entries for an Ethernet port.

Note that you can change a dynamic entry to a static or blackhole entry but not vice versa.

As your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic entries however will be lost whether you save the configuration or not.

Related commands: **display mac-address.**

Examples # Add a static entry for MAC address 00e0-fc01-0101. All frames destined to this MAC address are sent out of port Ethernet 2/0/1 which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address static 00e0-fc01-0101 interface ethernet 2/0/1
vlan 2
```

mac-address mac-learning disable

Syntax **mac-address mac-learning disable**

undo mac-address mac-learning disable

View System view, Ethernet port view, port group view

Parameters None

Description Use the **mac-address mac-learning disable** command to disable MAC address learning globally, on one or a group of Ethernet ports depending on the view you entered.

Use the **undo mac-address mac-learning disable** command to enable MAC address learning globally, on one or a group of Ethernet ports depending on the view you entered.

By default, MAC address learning is enabled globally and on all Ethernet ports.

Note that:

- You may need to disable MAC address learning sometimes to prevent the MAC address table from being saturated, for example, when your device is being attacked by a great deal of packets with different source MAC addresses. This somewhat affects update of the MAC address table.

- As disabling MAC address learning may result in broadcast storms, you need to enable broadcast storm suppression after you disable MAC address learning on a port.

Related commands: **display mac-address mac-learning.**



When global MAC address learning is disabled, the learned MAC addresses remain valid until they age out.

Examples # Disable global MAC address learning.

```
<Sysname> system-view
[Sysname] mac-address mac-learning disable
```

Disable MAC address learning on port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] mac-address mac-learning disable
```

mac-address max-mac-count

Syntax **mac-address max-mac-count** *count*

undo mac-address max-mac-count

View Ethernet port view, port group view

Parameters *count*: Maximum number of MAC addresses that can be learned on a port, in the range 0 to 4096. When the argument takes 0, the port is not allowed to learn MAC addresses.

Description Use the **mac-address max-mac-count** *count* command to configure the maximum number of MAC addresses that can be learned on an Ethernet port.

Use the **undo mac-address max-mac-count** command to remove the restriction on the maximum number of MAC addresses that can be learned on an Ethernet port.

By default, no maximum number of MAC addresses that can be learned on a port is configured.

Executed in port view, this command takes effect on the current port; executed in port group view, this command takes effect on all ports in the port group.

Related commands: **mac-address, mac-address, mac-address timer.**

Examples # Set the maximum number of MAC addresses that can be learned on port Ethernet 2/0/1 to 600.

```

<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] mac-address max-mac-count 600

```

mac-address timer

Syntax `mac-address timer { aging seconds | no-aging }`

`undo mac-address timer aging`

View System view

Parameters **aging** *seconds*: Sets an aging timer in seconds for dynamic MAC address entries, in the range 10 to 1000000.

no-aging: Sets dynamic MAC address entries not to age.

Description Use the **mac-address timer** command to configure the aging timer for dynamic MAC address entries.

Use the **undo mac-address timer** command to restore the default.

By default the default aging timer is 300 seconds.

Set the aging timer appropriately: a long aging interval may cause the MAC address table to retain outdated entries and fail to accommodate latest network changes; a short interval may result in removal of valid entries and hence unnecessary broadcasts which may affect device performance.

Examples # Set the aging timer for dynamic MAC address entries to 500 seconds.

```

<Sysname> system-view
[Sysname] mac-address timer aging 500

```


6

VLAN CONFIGURATION COMMANDS

description

Syntax **description** *text*
undo description

View VLAN view/VLAN interface view

Parameters *text*: String that describes the current VLAN or VLAN interface (Space can be included), case sensitive.

- For VLAN, this is a string of 1 to 32 characters.
- For VLAN interface, this is a string of 1 to 80 characters.

Description Use the **description** command to configure the descriptive string of the current VLAN or VLAN interface.

Use the **undo description** command to restore the default.

By default, the descriptive string for a VLAN is the VLAN ID, for example, "VLAN 0001"; for a VLAN interface is name of the current VLAN interface, for example, "Vlan-interface 1 Interface"

Examples # Assign a descriptive string **RESEARCH** for VLAN 1.

```
<Sysname> system-view  
[Sysname] vlan 1  
[Sysname-vlan1] description RESEARCH
```

Assign a descriptive string **VLAN-INTERFACE-2** for VLAN interface 2

```
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] quit  
[Sysname] interface vlan-interface 2  
[Sysname-Vlan-interface2] description VLAN-INTERFACE-2
```

display interface Vlan-interface

Syntax **display interface Vlan-interface** [*vlan-interface-id*]

View Any view

Parameters *vlan-interface-id*: VLAN interface ID.

Description Use the **display interface Vlan-interface** command to display the relevant information of a VLAN interface.

Execution of the command with the parameter included will display the information of a specified VLAN interface; otherwise, information on all created VLAN interfaces will be displayed.

Related commands: **interface Vlan-interface.**

Examples # Display the information of VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
Description: Vlan-interface2 Interface
The Maximum Transmit Unit is 1500
Internet Address is 192.168.0.72/24 Primary
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-fc00-6505
IPv6 Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-fc00-6505
```

Table 13 Field descriptions of the display interface Vlan-interface command

| Field | Description |
|-------------------------------|---|
| Vlan-interface2 current state | The physical state of a VLAN interface |
| Line protocol current state | The link layer protocol state of a VLAN interface |
| Description | The description of a VLAN interface |
| The Maximum Transmit Unit | The MTU of a VLAN interface |
| Internet protocol processing: | IP processing ability |
| IP Packet Frame Type | IPv4 outgoing frame format |
| Hardware address | MAC address corresponding to a VLAN interface |
| IPv6 Packet Frame Type | IPv6 outgoing frame format |

display vlan

Syntax **display vlan** [*vlan-id1* [**to** *vlan-id2*]] | **all** | **dynamic** | **reserved** | **static**]

View Any view

Parameters *vlan-id1*: Displays the information of a VLAN specified by VLAN ID in the range of 1 to 4,094.

vlan-id1 to vlan-id2: Displays the information of a range of VLANs specified by a VLAN ID range.

all: Displays all current VLAN information except for the reserved VLAN.

dynamic: Displays the information of dynamic VLANs

reserved: Displays information of the reserved VLANs. Protocol modules determine reserved VLANs according to function implementation, and reserved VLANs serve protocol modules. Reserved VLANs cannot be modified.

static: Displays static VLAN information.

Description Use the **display vlan** command to display VLAN information.

Related commands: **vlan**.

Examples # Display VLAN 2 information.

```
<Sysname> display vlan 2
VLAN ID: 2
VLAN Type: static
Route interface: not configured
Description: VLAN 0002
Tagged Ports: none
Untagged Ports:
    Ethernet2/0/1          Ethernet2/0/3          Ethernet2/0/4
```

Display VLAN 3 information.

```
<Sysname> display vlan 3
VLAN ID: 3
VLAN Type: static
Route Interface: configured
IP Address: 1.1.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Tagged Ports: none
Untagged Ports: none
```

Table 14 Field descriptions of the display vlan command

| Field | Description |
|-----------------|---|
| VLAN ID | VLAN ID |
| VLAN Type | VLAN type (static or dynamic) |
| Route interface | Whether the VLAN interface is configured for the VLAN: not configured or configured |
| Description | VLAN descriptive string |
| IP Address | IP address of the VLAN interface (not display if the VLAN interface has no IP address configured) |
| Subnet Mask | Subnet mask of the IP address (not display if the VLAN interface has no IP address configured) |
| Tagged Ports | Tagged ports |
| Untagged Ports | Untagged ports |

interface Vlan-interface

Syntax **interface Vlan-interface** *vlan-interface-id*

undo interface Vlan-interface *vlan-interface-id*

View System view

Parameters *vlan-interface-id*: VLAN interface ID, in the range of 1 to 4,094.

Description Use the **interface Vlan-interface** command to enter the specified VLAN interface view. Use the **undo interface Vlan-interface** command to delete the specified VLAN interface. The VLAN interface must be created first before entering its view

Before creating a VLAN interface, make sure the corresponding VLAN has been created; otherwise, the VLAN interface cannot be created.

Related commands: **display interface Vlan-interface.**

Examples # Create VLAN interface 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

ip address

Syntax **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]
undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View VLAN interface view

Parameters *ip-address*: IP address of a VLAN interface, in dotted decimal format.

mask: Subnet mask that corresponds to the IP address of a VLAN interface, in dotted decimal format.

mask-length: Length of a sub-net mask, indicated by the number of "1"s. This argument ranges from 0 to 32.

sub: Indicates the address is a sub-IP address of the VLAN interface.

Description Use the **ip address** command to specify the IP address and subnet mask for a VLAN interface.

Use the **undo ip address** command to remove the IP address and sub-net mask for a VLAN interface.

By default, no IP address is configured.

Normally, a VLAN interface has one IP address. To enable a device to connect to multiple subnets through a VLAN, you can assign multiple IP addresses to a VLAN interface, among which one is the primary IP address and the rest are secondary IP

addresses. On an S7900E Ethernet switch, you can assign up to five IP addresses to a VLAN interface. As for the primary and secondary IP addresses of a VLAN interface, note that:

- A newly configured main IP address will replace the original one, if there is one.
- Using the **undo ip address** command without any parameter indicates that all IP addresses will be deleted from the VLAN interface.
- Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to delete the main IP address.
- Use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command to delete a sub-interface.
- Note that before deletion of the main IP address you must first delete the sub-IP address.

Examples # Specify the IP address as 1.1.0.1, the sub-net mask as 255.255.255.0 for the VLAN interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 1.1.0.1 255.255.255.0
```

shutdown

Syntax **shutdown**

undo shutdown

View VLAN interface view

Parameters None

Description Use the **shutdown** command to shut down a VLAN interface.

Use the **undo shutdown** command to bring up a VLAN interface.

By default, the VLAN interface is down if all ports in the VLAN are down, as long as one port in the VLAN is up, the VLAN interface will be up

You can use the **undo shutdown** command to bring up a VLAN interface after configurations of the related parameter and protocol. When there is a fault in a VLAN interface, you can use the **shutdown** command to shut down the interface and then bring it up using the **undo shutdown** command. In this way, the interface will resume Shutting down/bringing up a VLAN interface does not affect any Ethernet ports in the VLAN. The state of an Ethernet port does not change with the VLAN interface state.

Examples # Shut down the VLAN interface and then bring it up.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

vlan

Syntax `vlan { vlan-id1 [to vlan-id2] | all }`

`undo vlan { vlan-id1 [to vlan-id2] | all }`

View System view

Parameters *vlan-id*: VLAN ID, in the range 1 to 4094.

vlan-id1 to vlan-id2: Specifies a VLAN range. VLAN ID is in the range 1 to 4094.

all: Specifies all the VLANs except the reserved VLANs.

Description Use the **vlan** *vlan-id* command to create specified VLAN(s).

If a specified VLAN exists, the command places you into its view.

Use the **undo vlan** command to delete specified VLAN(s).



- *As the default VLAN, VLAN 1 cannot be created, or removed.*
- *You cannot create/remove reserved VLANs that are reserved for specific function implementation.*
- *Dynamic VLANs cannot be removed using the **undo vlan** command.*
- *A VLAN configured with QoS policies cannot be removed.*
- *If an isolate-user-vlan or a secondary VLAN is associated to another VLAN using the **isolate-user-vlan** command, the VLAN can not be removed unless the association is removed.*
- *If a VLAN is configured as a remote mirroring VLAN, it cannot be removed using the **undo vlan** command unless its mirroring VLAN configuration is removed first.*

Related commands: **display vlan.**

Examples # Enter VLAN 2 view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2]
```

Create VLAN 4 through VLAN 100.

```
<Sysname> system-view
[Sysname] vlan 4 to 100
Please wait..... Done.
```

7

PORT-BASED VLAN CONFIGURATION COMMANDS

port

Syntax **port** *interface-list*
undo port *interface-list*

View VLAN interface view

Parameters **interface** *interface-list*: Ethernet interface list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> means that you can specify up to 10 port ranges.

Description Use the **port** command to add one Access port or a group of Access ports to a VLAN. Use the **undo port** command to remove one Access port or a group of Access ports from a VLAN.

Note:

- This command is only applicable to Access ports.
- All ports have their default link type configured as Access, however, users can manually configure the port type. For more information, refer to **port link-type**.

Related commands: **display vlan**.

Examples # Add Ethernet 2/0/1 through Ethernet 2/0/3 to VLAN 2.

```
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] port ethernet 2/0/1 to ethernet 2/0/3
```

port access vlan

Syntax **port access vlan** *vlan-id*
undo port access vlan

View Ethernet port view, port group view

Parameters *vlan-id*: VLAN ID, in the range 1 to 4094.

Description Use the **port access vlan** command to add the current Access port to a specified VLAN.

Use the **undo port access vlan** command to add the current Access port to the default VLAN.

Execution of the above command under Ethernet port view will apply the configurations to the current port only whereas under port group view will apply the configurations to all the ports in the port group.

By default, all the Access ports belong to VLAN 1.

Before adding an Access port to a VLAN, make sure the VLAN already exists.

Examples # Add Ethernet 2/0/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port access vlan 3
```

port hybrid pvid vlan

Syntax **port hybrid pvid vlan** *vlan-id*
undo port hybrid pvid

View Ethernet port view, port group view

Parameters *vlan-id*: VLAN ID, in the range 1 to 4094.

Description Use the **port hybrid pvid vlan** command to configure the default VLAN ID of the Hybrid port.

Use the **undo port hybrid pvid** command to restore the default, VLAN 1.

Execution of the **undo vlan** command on a Hybrid port to remove the default VLAN does not affect the default VLAN configuration. That is to say, the non-existent VLAN can still be the default VLAN.

Execution of the above commands under Ethernet port view will apply to the current port only whereas under port group view will apply to all ports in the port group view.

The default VLAN ID of local Hybrid port must be consistent with that of the peer; otherwise, packets cannot be forwarded properly.

Related commands: **port link-type**.

Examples # Configure the default VLAN ID for the Hybrid port Ethernet 2/0/1 to be 100.

```

<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type hybrid
[Sysname-Ethernet2/0/1] port hybrid pvid vlan 100

```

port hybrid vlan

Syntax **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

View Ethernet port view, port group view

Parameters *vlan-id-list*: The range of VLANs that the Hybrid ports will be added to, *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where *vlan-id* ranges from 1 to 4,094 and &<1-10> indicates that the you can specify up to 10 times.

tagged: Specifies to tag the packets of the specified VLAN (s).

untagged: Specifies not to tag the specified VLAN(s).

Description Use the **port hybrid vlan** command to add the current Hybrid port to the specified VLAN(s).

Use the **undo port hybrid vlan** command to remove the current Hybrid port from the specified VLAN(s).

The Hybrid port can allow multiple VLANs to pass. Repetitive execution of the **port hybrid vlan** command will yield a set VLANs, to which the Hybrid port belongs.

Execution of the above commands in Ethernet port view will apply to the current port only whereas under port group view will apply to all ports in the port group.

Related commands: **port link-type**.

Examples # Add the Hybrid port Ethernet 2/0/1 to VLAN 2, VLAN 4, and the range of VLANs from VLAN 50 to VLAN 100. Tag all packets of these VLANs.

```

<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type hybrid
[Sysname-Ethernet2/0/1] port hybrid vlan 2 4 50 to 100 tagged

```

Add Hybrid ports of port group 2 to VLAN 2. Packets are untagged.

```

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] port-group manual 2
[Sysname-port-group-manual-2] group-member ethernet 2/0/1 to ethernet 2/0/6
[Sysname-port-group-manual-2] port link-type hybrid
[Sysname-port-group-manual-2] port hybrid vlan 2 untagged

```

```
Configuring Ethernet2/0/1... Done.
Configuring Ethernet2/0/2... Done.
Configuring Ethernet2/0/3... Done.
Configuring Ethernet2/0/4... Done.
Configuring Ethernet2/0/5... Done.
Configuring Ethernet2/0/6... Done.
```

port link-type

Syntax `port link-type { access | hybrid | trunk }`

`undo port link-type`

View Ethernet port view, port group view

Parameters **access**: Configures the link type of a port as Access.

hybrid: Configures the link type of a port as Hybrid.

trunk: Configures the link type of a port as Trunk.

Description Use the **port link-type** command to configure the link type of a port.

Use the **undo port link-type** command to restore the default link type of a port, which is Access by default.

Execution of the above commands in Ethernet port view will apply to the current port only whereas under port group view will apply to all ports in the port group view.

By default, a port is an Access port.



The Trunk and Hybrid ports cannot be converted to each other directly. You can convert either to the Access port, and then to the other type. For example, convert a Trunk port to an Access port, and then to a Hybrid port.

Examples # Configure Ethernet 2/0/1 to be a Trunk port.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type trunk
```

Configure all the ports in the manual port group group1 as Hybrid ports.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member ethernet 2/0/1
[Sysname-port-group manual group1] group-member ethernet 2/0/2
[Sysname-port-group manual group1] port link-type hybrid
```

port trunk permit vlan

Syntax **port trunk permit vlan** { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

View Ethernet port view, port group view

Parameters *vlan-id-list*: The range of VLANs that the Hybrid ports will be added to, in the format of *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where *vlan-id* ranges from 1 to 4,094 and &<1-10> indicates that you can specify up to 10 parameters.

all: Adds the Trunk port to all VLANs.

Description Use the **port trunk permit vlan** command to add a Trunk port to a specified VLAN, a selection of VLANs, or all VLANs.

Use the **undo port trunk permit vlan** command to remove the Trunk port from a specified VLAN, a selection of VLANs, or all VLANs.

The Trunk port can allow multiple VLANs to pass. Repetitive execution of the **port trunk permit vlan** command will yield a set of *vlan-id-list*, to which the Trunk port belongs.

Execution of the above commands in Ethernet port view will apply to the current port only whereas under port group view will apply to all ports in the port group view.

Related commands: **port link-type**.

Examples # Add the Trunk port Ethernet 2/0/1 to VLAN 2, VLAN 4, and the range of VLANs from VLAN 50 to VLAN 100.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type trunk
[Sysname-Ethernet2/0/1] port trunk permit vlan 2 4 50 to 100
Please wait..... Done.
```

port trunk pvid vlan

Syntax **port trunk pvid vlan** *vlan-id*

undo port trunk pvid

View Ethernet port view, port group view

Parameters *vlan-id*: VLAN ID, in the range 1 to 4094

Description Use the **port trunk pvid vlan** command to configure the default VLAN ID for the Trunk port.

Use the **undo port trunk pvid** command to restore the default.

By default, the default VLAN on a Trunk port is VLAN 1.

Execution of the **undo vlan** command on a Trunk port to remove a default VLAN does not affect the default VLAN configurations. That is to say, a non-existent VLAN can still be the default VLAN.

Execution of the above commands in Ethernet port view will apply to the current port only whereas under port group view will apply to all ports in the port group view.

You must configure the same default VLAN ID for the Trunk port of both the local device and remote device. Otherwise, the packets cannot be transmitted correctly.

Related commands: **port link-type**.

Examples # Configure the default VLAN ID for the Trunk port Ethernet 2/0/1 as 100.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type trunk
[Sysname-Ethernet2/0/1] port trunk pvid vlan 100
```

8

PROTOCOL-BASED VLAN CONFIGURATION COMMANDS

display protocol-vlan interface

Syntax **display protocol-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

View Any view

Parameters *interface-type interface-number1*: Specifies an port by its type and number.
interface-type interface-number1 to interface-type interface-number2: Specifies an port range.
all: Displays protocol information and protocol indexes of all ports.

Description Use the **display protocol-vlan interface** command to display protocol based VLAN information on the specified port(s).

Examples # Display protocol based VLAN information on Ethernet 2/0/1.
[Sysname] display protocol-vlan interface ethernet 2/0/1
Interface: Ethernet2/0/1
VLAN ID Protocol Index Protocol Type
=====

| | | |
|---|---|----------------|
| 2 | 0 | ipv4 |
| 2 | 3 | ipx ethernetii |

Table 15 Field descriptions of the display protocol-vlan interface command

| Field | Description |
|----------------|--|
| Interface | Port of which you want to view the information |
| VLAN ID | VLAN ID |
| Protocol Index | Protocol Index |
| Protocol Type | Protocol Type |

display protocol-vlan vlan

Syntax **display protocol-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }

View Any view

Parameters *vlan-id*: VLAN ID, in the range 1 to 4094.

to: Specifies VLAN range, the value after this parameter must be greater than or equal to that before it.

all: All VLANs.

Description Use the **display protocol-vlan vlan** command to display the protocol information and protocol index configured on the specified VLAN(s).

Related commands: **display vlan.**

Examples # Display the protocol information and protocol index configured on all protocol-based-VLANs.

```
<Sysname> display protocol-vlan vlan all
VLAN ID:2
  Protocol Index      Protocol Type
=====
          0          ipv4
          3          ipx ethernetii
VLAN ID:3
  Protocol Index      Protocol Type
=====
          0          ipv4
          1          ipx snap
```

Refer to Table 13 for description on the output fields.

port hybrid protocol-vlan

Syntax **port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

undo port hybrid protocol-vlan { **vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** } | **all** }

View Ethernet port view, port group view

Parameters **vlan** *vlan-id*: Specifies a VLAN ID, in the range 1 to 4094.

protocol-index: Beginning protocol index, in the range 0 to 15. Note that the beginning protocol index is automatically numbered according to the order in which protocols are associated with VLANs if not manually specified. You can use the **display protocol-vlan vlan all** command to display the protocol index.

to *protocol-end*: Specifies the end protocol index, in the range 0 to 15. The *protocol-end* argument must be greater than or equal to the beginning protocol index.

all: All protocols.

Description Use the **port hybrid protocol-vlan vlan** command to associate a port with a protocol-based VLAN.

Use the **undo port hybrid protocol-vlan** command to delete the association between the port and the protocol-based VLAN.

Execution of the above commands in Ethernet port view will apply the configurations to the current port only whereas under port group view will apply the configurations to all ports in the port group.

Note that only the Hybrid port supports the above feature at the moment. Before issuing this command, ensure that the port has been added to the VLAN to be associated with and that the VLAN has been assigned with a protocol.



CAUTION: *At present, the AppleTalk-based protocol template cannot be associated with a port on an S7900E Ethernet switch*

Related commands: **display protocol-vlan interface.**

Examples # Associate the Hybrid port Ethernet 2/0/1, with protocol 0 in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-Vlan2] protocol-vlan at
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type hybrid
[Sysname-Ethernet2/0/1] port hybrid vlan 2 untagged
Please wait... Done
[Sysname-Ethernet2/0/1] port hybrid protocol-vlan vlan 2 0
```

protocol-vlan

Syntax **protocol-vlan** [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii** **etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap** **etype** *etype-id* }

undo protocol-vlan { *protocol-index* [**to** *protocol-end*] | **all** }

View VLAN view

Parameters **at**: Specifies the AppleTalk based VLAN.

ipv4: Specifies the IPv4 based VLAN.

ipv6: Specifies the IPv6 based VLAN.

ipx: Specifies the IPX based VLAN. The keywords **ethernetii**, **llc**, **raw**, and **snap** are encapsulation formats.

mode: Configures self-defined protocol template for the VLAN, which could also have four encapsulation formats, namely, **ethernetii**, **llc**, **raw**, and **snap**.

ethernetii etype etype-id: Specifies to match Ethernet II encapsulation format and the corresponding protocol type values. The *etype-id* argument is the Ethernet

type of inbound packets, in the range 0x0600 to 0xffff (excluding 0x0800, 0x809b, 0x8137, and 0x86dd).

llc: Specifies the encapsulation format for Ethernet packets to be **llc**.

dsap *dsap-id*: Specifies the destination service access point, in the rang 00 to ff.

ssap *ssap-id*: Specifies the source service access point, in the rang 00 to ff.

snap etype *etype-id*: Specifies to match SNAP encapsulation format and the corresponding protocol type values. The *etype-id* argument is the Ethernet type of inbound packets, in the range 0x0600 to 0xffff (excluding **ipx snap** under the **snap** encapsulation format).

protocol-index: Beginning protocol index, in the range 0 to 15. The system will automatically assign an index if this parameter is not specified.

to *protocol-end*: Specifies the end protocol index, which ranges from 0 to 15 and must be greater than or equal to the *protocol-index* argument.

all: Specifies all the protocol indexes.



CAUTION:

- *Ensure that the dsap-id and ssap-id arguments are not configured as 0xe0 that corresponds with **ipx llc** at the same time, or as 0xff that corresponds with **ipx raw** at the same time. When either of the dsap-id and ssap-id arguments is configured, the system assigns **aa** to the other argument.*
- *Ensure that the **etype** keyword is not configured as 0x0800, 0x8137, 0x809b, or 0x86dd, as which are identical to protocol templates of IPv4, IPX, AppleTalk, and IPv6 respectively.*

Description Use the **protocol-vlan** command to configure the VLAN as a protocol based VLAN and the protocol template.

Use the **undo protocol-vlan** command to remove the configured protocol template.

Related commands: **display protocol-vlan vlan.**



To make sure that data can be transmitted properly, do not configure a VLAN as a protocol-based VLAN and voice VLAN at the same time.

Examples # Specify VLAN 3 as the IPv4 based VLAN to make the VLAN transmit IPv4 packets.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] protocol-vlan ipv4
```



CAUTION: *Due to the close relationship between IPv4 and ARP, it is recommended to bind the two protocols to the same VLAN and associate the binding to related ports to guarantee normal communication.*

Configure ARP protocol template for VLAN3 (ARP code is 0x0806) to make the VLAN transmit ARP packets.

- To use Ethernet encapsulation, use the command:

```
[Sysname-vlan3] protocol-vlan mode ethernetii etype 0806
```

- To use 802.3 encapsulation, use the command:

```
[Sysname-vlan3] protocol-vlan mode snap etype 0806
```


9

IP-SUBNET-BASED VLAN CONFIGURATION COMMANDS

display ip-subnet-vlan interface

Syntax **display ip-subnet-vlan interface** { *interface-type interface number1* [**to** *interface-type interface-number2*] | **all** }

View Any view

Parameters *interface-type interface-number1*: Specifies a port by its type and number.

Interface-type interface-number1 to Interface-type interface-number2: Specifies multiple ports.

all: Displays the IP-subnet-based VLAN information about all the ports with IP-subnet-based VLAN configured.

Description Use the **display ip-subnet-vlan interface** command to display the IP-subnet-based VLAN information and IP subnet ID on a specified port.

Examples # Display the IP-subnet-based VLAN information and IP subnet index on Ethernet 2/0/1.

```
<Sysname> display ip-subnet-vlan interface ethernet 2/0/1
Interface: Ethernet2/0/1
  VLAN ID   Subnet-Index   IP ADDRESS           NET MASK
  =====
      3             0           192.168.1.0         255.255.255.0
```

Table 16 Field descriptions of the display ip-subnet-vlan interface command

| Field | Description |
|--------------|---|
| Interface | Interface of which you want to view the information |
| VLAN ID | VLAN ID |
| Subnet-Index | Index of the subnet |
| IP ADDRESS | IP address of the subnet (can be either an IP address or network address) |
| NET MASK | Mask of IP subnet |

display ip-subnet-vlan vlan

Syntax **display ip-subnet-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }

View Any view

Parameters *vlan-id*: VLAN ID, in the range 1 to 4094.

to: Specifies a VLAN ID range, the argument to the right of this keyword must be greater than or equal to that to the left of this keyword.

all: Specifies all the VLANs.

Description Use the **display ip-subnet-vlan vlan** command to display the IP subnet information and IP subnet index on the specified VLAN(s).

Related commands: **display vlan**.

Examples # Display the IP subnet information of all VLANs.

```
<Sysname> display ip-subnet-vlan vlan all
VLAN ID: 3
Subnet Index      IP Address      Subnet Mask
=====
          0      192.168.1.0    255.255.255.0
```

Table 17 Field descriptions of the display ip-subnet-vlan vlan command

| Field | Description |
|--------------|--|
| VLAN ID | VLAN ID |
| Subnet Index | Subnet Index |
| IP Address | IP address of the subnet (can be an IP address or a network address) |
| Subnet Mask | Mask of the IP subnet |

ip-subnet-vlan

Syntax **ip-subnet-vlan** [*ip-subnet-index*] **ip** *ip-address* [*mask*]

undo ip-subnet-vlan { *ip-subnet-index* [**to** *ip-subnet-end*] | **all** }

View VLAN view

Parameters *ip-subnet-index*: IP subnet Index, in the range of 0 to 11. This value can be configured by users, or automatically numbered by system based on the order in which the IP subnet or IP address is associated with the VLAN.

ip *ip-address* [*mask*]: Specifies the source IP address or network address based on which the subnet-based VLANs are classified, in dotted decimal notation. The *mask* argument is the subnet mask of the source IP address or network address, in dotted decimal notation with a default value of 255.255.255.0.

to: Specifies an IP subnet Index range.

ip-subnet-end: The last index value of the IP subnet, in the range of 0 to 11, must be greater than or equal to the *ip-subnet-index* value.

all: Removes all the associations between the VLAN and the specified IP subnets or IP addresses.

Description Use the **ip-subnet-vlan** command to associate the current VLAN with a specified IP subnet or IP address.

Use the **undo ip-subnet-vlan** command to delete the association.

Note that the IP subnet or IP address cannot be a multicast network segment or a multicast address.

Related commands: **display ip-subnet-vlan vlan.**

Examples # Configure VLAN 3 to be an IP-subnet-based VLAN. Associate it with the 192.168.1.0/24 network segment.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
```

port hybrid ip-subnet-vlan vlan

Syntax **port hybrid ip-subnet-vlan vlan** *vlan-id*
undo port hybrid ip-subnet-vlan { **vlan** *vlan-id* | **all** }

View Ethernet port view, port group view

Parameters *vlan-id*: VLAN ID, in the range of 1 to 4,094.

all: All VLANs.

Description Use the **port hybrid ip-subnet-vlan vlan** command to associate the current Ethernet port with an IP-subnet-based VLAN.

Use the **undo port hybrid ip-subnet-vlan vlan** command to remove the association between the current Ethernet port and an IP-subnet-based VLAN.

Execution of the above commands in Ethernet port view will apply the configurations to the current port only whereas under port group view will apply the configurations to all ports in the port group.

Note that only the Hybrid port supports the above feature at the moment. Before issuing this command, ensure that the port has been added to the IP-subnet-based VLAN to be associated with. Otherwise, the port cannot be associated with the VLAN.

Related commands: **display ip-subnet-vlan interface.**

Examples # Associate Ethernet 2/0/1 with VLAN 3 (assuming that VLAN 3 is an IP-subnet-based VLAN).

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
```

```
[Sysname-vlan3] quit
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type hybrid
[Sysname-Ethernet2/0/1] port hybrid vlan 3 untagged
Please wait... Done.
[Sysname-Ethernet2/0/1] port hybrid ip-subnet-vlan vlan 3
```

10

ISOLATE-USER-VLAN CONFIGURATION COMMANDS

display isolate-user-vlan

Syntax `display isolate-user-vlan [isolate-user-vlan-id]`

View Any view

Parameters *isolate-user-vlan-id*: VLAN ID of an isolate-user-VLAN, in the range 1 to 4094.

Description Use the **display isolate-user-vlan** command to display the mapping between an isolate-user-vlan and the secondary VLAN(s).

Related commands: **isolate-user-vlan, isolate-user-vlan enable.**

Examples # Display the mapping between an isolate-user-vlan and secondary VLANs.

```
<Sysname> display isolate-user-vlan
Isolate-user-VLAN VLAN ID : 2
Secondary VLAN ID : 3 4

VLAN ID: 2
VLAN Type: static
Isolate-user-VLAN type : isolate-user-VLAN
Route Interface: configured
IP Address: 1.1.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0002
Broadcast MAX-ratio: 100%
Tagged Ports: none
Untagged Ports:
    Ethernet2/0/2          Ethernet2/0/3          Ethernet2/0/4
VLAN ID: 3
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: configured
IP Address: 2.2.2.2
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Broadcast MAX-ratio: 100%
Tagged Ports: none
Untagged Ports:
    Ethernet2/0/2          Ethernet2/0/3

VLAN ID: 4
VLAN Type: static
```

```

Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0004
Broadcast MAX-ratio: 100%
Tagged Ports: none
Untagged Ports:
    Ethernet2/0/2                Ethernet2/0/4

```

Table 18 Field descriptions of the display isolate-user-vlan command

| Field | Description |
|---------------------------|---|
| Isolate-user-VLAN VLAN ID | Isolate-user-VLAN ID |
| Secondary VLAN ID | Secondary VLAN ID |
| VLAN ID | VLAN ID |
| VLAN Type | VLAN Type, either static or dynamic VLAN |
| Isolate-user-VLAN type | Current VLAN type, either Isolate-user-VLAN or secondary VLAN |
| Route Interface | Whether VLAN interface is configured or not |
| IP Address | IP address of VLAN interface. If VLAN interface is not configured, this field will not be displayed. |
| Subnet Mask | Subnet Mask of the VLAN interface. If VLAN interface is not configured, this field will not be displayed. |
| Description | VLAN description |
| Tagged Ports | Indicating the ports that need to have VLAN tag |
| Untagged Ports | Indicating the ports that need not to have VLAN tag |

isolate-user-vlan

Syntax `isolate-user-vlan isolate-user-vlan-id secondary secondary-vlan-id-list`

`undo isolate-user-vlan isolate-user-vlan-id [secondary secondary-vlan-id-list]`

View System view

Parameters `isolate-user-vlan-id`: VLAN ID of an isolate-user-vlan, in the range 1 to 4094.

secondary secondary-vlan-id-list: Specifies a list of secondary VLAN IDs. You need to provide the `secondary-vlan-id` argument in the form of { `secondary-vlan-id1 [to secondary-vlan-id2]` }<1-10>, where `secondary-vlan-id1` and `secondary-vlan-id2` are VLAN IDs in the range 1 to 4094 and <1-10> means that you can provide up to ten secondary VLAN IDs/secondary VLAN ID ranges.

Description Use the **isolate-user-vlan** command to create the mapping between an isolate-user-vlan and the secondary VLAN(s).

Use the **undo isolate-user-vlan** command to delete the mapping between an isolate-user-vlan and the secondary VLANs.

By default, there is no mapping between the isolate-user-vlan and the secondary VLANs.

Note that:

- To use the **isolate-user-vlan** command, the isolate-user-vlan and the secondary VLAN must have at least a port, which allows the isolate-user-vlan or the secondary VLAN to pass. The default VLAN of the port must be the isolate-user-vlan or the secondary VLAN. Otherwise, the command can not be used.
- Use of the **undo isolate-user-vlan** command without the **secondary secondary-vlan-id** parameter will delete the mapping between the specified isolate-user-vlan and all secondary VLANs, while use of the command with the parameter will only delete the mapping between the specified isolate-user-vlan and the specified secondary VLANs.



After the mapping between the isolate-user-vlan and the secondary VLANs is created, no port can be added to or deleted from either the isolate-user-vlan or the secondary VLAN(s). Only after the mapping relation is deleted are the above operations possible.

Related commands: **display isolate-user-vlan.**

Examples # Associate the isolate-user-VLAN 2 to the secondary VLANs VLAN 3 and VLAN 4.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] isolate-user-vlan enable
[Sysname-vlan2] port ethernet 2/0/2
[Sysname-vlan2] vlan 3
[Sysname-vlan3] port ethernet 2/0/3
[Sysname-vlan3] vlan 4
[Sysname-vlan4] port ethernet 2/0/4
[Sysname-vlan4] quit
[Sysname] isolate-user-vlan 2 secondary 3 to 4
```

isolate-user-vlan enable

Syntax **isolate-user-vlan enable**

undo isolate-user-vlan enable

View VLAN view

Parameters None

Description Use the **isolate-user-vlan enable** command to configure the current VLAN as an isolate-user-VLAN.

Use the **isolate-user-vlan enable** command to remove the isolate-user-VLAN configuration for a specified VLAN.

By default, no VLAN is an isolate-user-VLAN.

An isolate-user-VLAN may include multiple ports, including those that are connected to upstream devices.

Related commands: **display isolate-user-vlan.**

Examples # Configure VLAN 5 to be an isolate-user-VLAN.

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] isolate-user-vlan enable
```


11

VOICE VLAN CONFIGURATION COMMANDS

display voice vlan oui

Syntax `display voice vlan oui`

View Any view

Parameters None

Description Use the **display voice vlan oui** command to display the organizationally unique identifier (OUI) address(es), the OUI address mask, and the descriptive string currently supported by system.

Related commands: `voice vlan`, `voice vlan enable`.



As the first 24 bits of a MAC address (in binary format), an OUI address is a globally unique identifier assigned to a vendor by IEEE.

Examples # Display the OUI address of a voice VLAN.

```
<Sysname> display voice vlan oui
Oui Address      Mask              Description
0001-e300-0000   ffff-ff00-0000   Siemens phone
0003-6b00-0000   ffff-ff00-0000   Cisco phone
0004-0d00-0000   ffff-ff00-0000   Avaya phone
0060-b900-0000   ffff-ff00-0000   Philips/NEC phone
00d0-1e00-0000   ffff-ff00-0000   Pingtel phone
00e0-7500-0000   ffff-ff00-0000   Polycom phone
00e0-bb00-0000   ffff-ff00-0000   3com phone
```

Table 19 Field descriptions of the display voice vlan oui command

| Field | Description |
|-------------|---|
| Oui Address | OUI addresses that are allowed to pass |
| Mask | Mask of the OUI addresses that are allowed to pass |
| Description | Description of the OUI addresses that are allowed to pass |

display voice vlan state

Syntax `display voice vlan state`

View Any view

Parameters None

Description Use the **display voice vlan state** command to display the voice VLAN configuration.

Related commands: **voice vlan enable**.

Examples # Display the voice VLAN configurations.

```
<Sysname> display voice vlan state
Voice VLAN status: ENABLE
Voice VLAN ID: 2
Voice VLAN security mode: Security
Voice VLAN aging time: 1440 minutes
Voice VLAN enabled port and its mode:
PORT                MODE
-----
Ethernet2/0/2       MANUAL
Ethernet2/0/3       MANUAL
Ethernet2/0/4       MANUAL
Ethernet2/0/5       AUTO
```

Table 20 Field descriptions of the display voice vlan state command

| Field | Description |
|--|---|
| Voice VLAN status | The current voice VLAN status, that is, whether it is enabled or disabled. |
| Voice VLAN ID | ID of a voice VLAN |
| Voice VLAN security mode | Security mode of a voice VLAN |
| Voice VLAN aging time | Aging time of a voice VLAN |
| Current voice vlan enabled port and its mode | The port that is currently enabled with the voice VLAN feature and its working mode |
| PORT | port ID |
| MODE | Voice VLAN working mode: manual or automatic. |

voice vlan

Syntax **voice vlan** *vlan-id* **enable**

undo voice vlan enable

View System view

Parameters *vlan-id*: ID of the VLAN to be enabled with the voice VLAN feature, in the range 2 to 4094.

Description Use the **voice vlan** command to enable the voice VLAN feature globally.

Use the **undo voice vlan enable** command to disable the voice VLAN feature globally.

- At one particular moment, only one VLAN of a certain device can have the voice VLAN feature enabled.
- Ensure that a VLAN exists before enabling its voice VLAN feature and that it is not VLAN 1. Otherwise, the configurations will fail.
- If a VLAN to be deleted has the voice VLAN feature enabled, you need to disable the voice VLAN feature first before deleting the VLAN.

Related commands: **display voice vlan state.**

Examples # Enable the voice VLAN feature on VLAN 2 (assuming that VLAN 2 already exists).

```
<Sysname> system-view
[Sysname] voice vlan 2 enable
```

voice vlan aging

Syntax **voice vlan aging** *minutes*
undo voice vlan aging

View System view

Parameters *minutes*: Aging time of a voice VLAN, in the range 5 to 43,200 (in minutes). This value is 1,440 by default.

Description Use the **voice vlan aging** command to configure the aging time of a voice VLAN.

Use the **undo voice vlan aging** command to restore the aging time of a voice VLAN.

Under automatic mode, the system will decide whether to add a port to a voice VLAN based on the source MAC address contained in its inbound voice packets. After adding a port to the voice VLAN, the system will start the aging timer at the same time. If within the aging time, no voice packets is received from the port, it will be removed from the voice VLAN when the aging time expires.

Related commands: **display voice vlan state.**

Examples # Configure the aging time of the voice VLAN as 100 minutes.

```
<Sysname> system-view
[Sysname] voice vlan aging 100
```

voice vlan enable

Syntax **voice vlan enable**
undo voice vlan enable

| | |
|--------------------|---|
| View | Ethernet port view |
| Parameters | None |
| Description | <p>Use the voice vlan enable command to enable the voice VLAN feature on an Ethernet port.</p> <p>Use the undo voice vlan enable command to disable the voice VLAN feature on an Ethernet port.</p> <p>No voice VLAN is enabled on a port by default.</p> <ul style="list-style-type: none"> ■ Under automatic mode, only The Trunk or Hybrid port can be configured with the voice VLAN feature. The Access port cannot be configured with this feature. ■ Before enabling the voice VLAN feature on a port, ensure that its is enabled globally first ■ Only after the voice VLAN feature is enabled under both system view and Ethernet port view will it functions properly. |
| Examples | <p># Enable the voice VLAN feature on the port Ethernet 2/0/1.</p> <pre><Sysname> system-view [Sysname] voice vlan 2 enable [Sysname] interface ethernet 2/0/1 [Sysname-Ethernet2/0/1] voice vlan enable</pre> |

voice vlan mac-address

| | |
|-------------------|---|
| Syntax | <p>voice vlan mac-address <i>mac-addr</i> mask <i>oui-mask</i> [description <i>text</i>]</p> <p>undo voice vlan mac-address <i>oui</i></p> |
| View | System view |
| Parameters | <p><i>mac-addr</i>: MAC address, in the format of H-H-H, such as 1234-1234-1234.</p> <p>mask <i>oui-mask</i>: Specifies the valid length of the OUI address, represented in mask, in the format of H-H-H, from left to right are consecutive fs and 0s, for example, ffff-f000-0000.</p> <p>description <i>text</i>: Specifies a string that describes the OUI address. The string is of 1 to 30 characters and is case sensitive.</p> <p><i>oui</i>: Deletes an OUI address that is in the format H-H-H, such as 1234-1200-0000, which is the logic AND result of <i>mac-addr</i> and <i>oui-mask</i>. Using the display voice vlan oui command can display OUI address information. The OUI address cannot be a broadcast, multicast or address of all 0s or all fs.</p> |

Description Use the **voice vlan mac-address** command to make a specified OUI address identified by the voice VLAN.

Use the **undo voice vlan mac-address** command to remove an OUI address from being identified by the voice VLAN.

A maximum of 16 OUI addresses can be supported by the system.

By default, default OUI addresses, which can be removed or then added, as illustrated in the following table.

Table 21 Default OUI addresses

| Number | OUI | Description |
|--------|----------------|-------------------|
| 1 | 0001-e300-0000 | Siemens phone |
| 2 | 0003-6b00-0000 | Cisco phone |
| 3 | 0004-0d00-0000 | Avaya phone |
| 4 | 0060-b900-0000 | Philips/NEC phone |
| 5 | 00d0-1e00-0000 | Pingtel phone |
| 6 | 00e0-7500-0000 | Polycom phone |
| 7 | 00e0-bb00-0000 | 3com phone |

Related commands: **display voice vlan oui.**

Examples # Configure the OUI address as 1234-1234-1234, the mask as ffff-ff00-0000, and the descriptive string as phone A, that is, voice packets from Phone A with source MAC address being 1234-1234-1234 can pass through the voice VLAN.

```
<Sysname> system-view
[Sysname] voice vlan mac-address 1234-1234-1234 mask ffff-ff00-0000
description PhoneA
```

Display OUI address information.

```
<Sysname> display voice vlan oui
```

```
Oui Address      Mask             Description
0001-e300-0000   ffff-ff00-0000   Siemens phone
0003-6b00-0000   ffff-ff00-0000   Cisco phone
0004-0d00-0000   ffff-ff00-0000   Avaya phone
0060-b900-0000   ffff-ff00-0000   Philips/NEC phone
00d0-1e00-0000   ffff-ff00-0000   Pingtel phone
00e0-7500-0000   ffff-ff00-0000   Polycom phone
00e0-bb00-0000   ffff-ff00-0000   3com phone
1234-1200-0000   ffff-ff00-0000   PhoneA
```


Disable voice packets of Phone A from passing through the voice VLAN.

```
<Sysname> system-view
[Sysname] undo voice vlan mac-address 1234-1200-0000
```

voice vlan mode auto

| | |
|--------------------|---|
| Syntax | voice vlan mode auto
undo voice vlan mode auto |
| View | Ethernet port view |
| Parameters | None |
| Description | <p>Use the voice vlan mode auto command to configure the voice VLAN working mode on a port to be automatic.</p> <p>Use the undo voice vlan mode auto command to configure the voice VLAN working mode on a port to be manual.</p> <p>By default, the voice VLAN working mode is automatic.</p> <p>The voice VLAN working mode of a port is independent of those of other ports.</p> <p>Note that: if the interface is enabled with voice VLAN in manual mode, you need to add the port to the voice VLAN manually to validate the voice VLAN.</p> |
| Examples | <pre># Configure the voice VLAN working mode on Ethernet 2/0/1 as manual.
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] undo voice vlan mode auto</pre> |

voice vlan security enable

| | |
|---|--|
| Syntax | voice vlan security enable
undo voice vlan security enable |
| View | System view |
| Parameters | None |
| Description | <p>Use the voice vlan security enable command to enable the security mode for voice VLAN.</p> <p>Use the undo voice vlan security enable command to disable the security mode for voice VLAN.</p> <p>By default, the security mode of voice VLAN is enabled.</p> |
|  | <i>The voice vlan security enable and undo voice vlan security enable commands take effect only after the voice VLAN feature is enabled globally.</i> |

Examples # Disable the security mode of the voice VLAN.
<Sysname> system-view
[Sysname] undo voice vlan security enable

12

QINQ CONFIGURATION COMMANDS

classifier behavior

Syntax **classifier** *classifier-name* **behavior** *behavior-name*
undo classifier *classifier-name*

View Policy view

Parameters *classifier-name*: Name of a class, a string of 1 to 31 characters.
behavior-name: Name of a traffic behavior, a string of 1 to 31 characters.

Description Use the **classifier behavior** command to associate a traffic behavior with a class.
Use the **undo classifier** command to remove the association.
Note that each class can be associated with only one traffic behavior.

Related commands: **qos policy**.



In a QoS policy with multiple class-to-traffic-behavior associations, if the action of creating an outer VLAN tag is configured in a traffic behavior, we recommend you not to configure any other action in this traffic behavior. Otherwise, the QoS policy may not function as expected after it is applied.

Examples # Associate the behavior **test** with the class **database** in the policy **user1**.

```
<Sysname> system-view  
[Sysname] qos policy user1  
[Sysname-qospolicy-user1] classifier database behavior test
```

if-match customer-vlan-id

Syntax **if-match customer-vlan-id** *vlan-id-list*
undo if-match customer-vlan-id *vlan-id-list*

View Class view

- Parameters** *vlan-id-list*: Customer VLAN IDs. You can specify up to eight VLAN IDs for the argument in the form of *vlan-id* **to** *vlan-id* or multiple discontinuous space-separated VLAN IDs. A VLAN ID ranges from 1 to 4094.
- Description** Use the **if-match customer-vlan-id** command to use the specified customer VLAN ID(s) as the match criterion.
- Use the **undo if-match customer-vlan-id** command to remove the match criterion.
- Example** # Create class **class1** and classify frames of customer VLAN 9 through 100 to class 1.
- ```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-vlan-id 9 to 100
```

## nest top-most vlan-id

- Syntax** **nest top-most vlan-id** *vlan-id*
- undo nest**
- View** Traffic behavior view
- Parameters** *vlan-id*: VLAN ID, in the range of 1 to 4094.
- Description** Use the **nest top-most vlan-id** command to configure the action of creating an outer VLAN tag for the traffic behavior.
- Use the **undo nest** command to remove the action.
- Related commands:** **qos policy**, **traffic behavior**.
- Examples** # Configure the action of creating outer VLAN tag 100 for the traffic behavior **database**.
- ```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] nest top-most vlan-id 100
```

qinq enable

- Syntax** **qinq enable**
- undo qinq enable**
- View** Ethernet port view, port group view

Parameters None

Description Use the **qinq enable** command to enable basic QinQ for the current Ethernet port.

Use the **undo qinq enable** command to disable basic QinQ for the current Ethernet port.

By default, basic QinQ is disabled for Ethernet port.

After basic QinQ is enabled on the port, frames on this port will be tagged with a new VLAN tag, the VLAN ID in which is the default VLAN ID of the port.

Configured in Ethernet port view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Examples # Enable basic QinQ on port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] qinq enable
```

Enable basic QinQ on all the ports in port group 1.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode manual
[Sysname] interface ethernet 2/0/2
[Sysname-Ethernet2/0/2] port link-aggregation group 1
[Sysname-Ethernet2/0/2] interface ethernet 2/0/3
[Sysname-Ethernet2/0/3] port link-aggregation group 1
[Sysname-Ethernet2/0/3] quit
[Sysname] port-group aggregation 1
[Sysname-port-group-aggregation-1] qinq enable
```

qinq ethernet-type customer-tag

Syntax **qinq ethernet-type customer-tag** *hex-value*

undo qinq ethernet-type customer-tag

View System view

Parameters *hex-value*: Hexadecimal protocol type ID, in the range of 0x0001 to 0xFFFF, but you cannot set it to any of the protocol type values listed in Table 22.

Table 22 Common protocol type values

| Protocol type | Value |
|---------------|--------|
| ARP | 0x0806 |
| PUP | 0x0200 |
| RARP | 0x8035 |

Table 22 Common protocol type values

| Protocol type | Value |
|---------------|----------------------|
| IP | 0x0800 |
| IPv6 | 0x86DD |
| PPPoE | 0x8863/0x8864 |
| MPLS | 0x8847/0x8848 |
| IPX/SPX | 0x8137 |
| IS-IS | 0x8000 |
| LACP | 0x8809 |
| 802.1x | 0x888E |
| Cluster | 0x88A7 |
| Reserved | 0xFFFD/0xFFFE/0xFFFF |

Description Use the **qinq ethernet-type customer-tag** command to configure the TPID value of the customer network VLAN tags.

Use the **undo qinq ethernet-type customer-tag** command to restore the system default.

By default, the TPID value of the customer network VLAN tags is 0x8100.

Examples # Set the TPID value of the customer network VLAN tags to 0x9100.

```
<Sysname> system-view
[Sysname] qinq ethernet-type customer-tag 9100
```

qinq ethernet-type service-tag

Syntax **qinq ethernet-type service-tag** *hex-value*

undo qinq ethernet-type service-tag

View Ethernet port view, port group view

Parameters *hex-value*: Hexadecimal protocol type ID, in the range of 0x0001 to 0xFFFF except the protocol type values listed in Table 22.

Description Use the **qinq ethernet-type service-tag** command to configure the TPID value of the service provider network VLAN tags.

Use the **undo qinq ethernet-type service-tag** command to restore the default.

By default, the TPID value of the service provider network VLAN tags is 0x8100.

Examples # Set the TPID value of the service provider network VLAN tags to 0x9100 for Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet2/0/1
[Sysname-Ethernet2/0/1] qinq ethernet-type service-tag 9100
```

qos apply policy

Syntax **qos apply policy** *policy-name* **inbound**

undo qos apply policy inbound

View Ethernet port view, port group view

Parameters **inbound**: Applies the specified policy to the traffic received on the current port(s).

policy-name: Policy name, a string of 1 to 31 characters.

Description Use the **qos apply policy** command to apply a policy on a port or a port group.

Use the **undo qos apply policy** command to remove the policy applied on a port or a port group.

In selective QinQ implementation on SC/SA/EA series modules, a QoS policy can be applied only to incoming traffic. Therefore, the **qos apply policy** command can be applied only on ports receiving traffic from the customer network.



SC modules include 0231A931 modules, SA modules include LSQ13C16915SA modules, and EA modules include only 0231A92P modules. For complete information about module types, refer to the accompanied installation manual.

Examples # Apply the policy **test** in the inbound direction of Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] qos apply policy test inbound
```

qos policy

Syntax **qos policy** *policy-name*

undo qos policy *policy-name*

View System view

Parameters *policy-name*: Policy name, a string of 1 to 31 characters.

Description Use the **qos policy** command to create a policy. This command also leads you to policy view.

Use the **undo qos policy** command to remove a policy.

To remove a policy that has been applied on a port, remove it from the port first.

Related commands: **classifier behavior, qos apply policy.**

Examples # Create the policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

traffic behavior

Syntax **traffic behavior** *behavior-name*
undo traffic behavior *behavior-name*

View System view

Parameters *behavior-name*: Behavior name, a string of 1 to 31 characters.

Description Use the **traffic behavior** command to create a traffic behavior. This command also leads you to traffic behavior view.

Use the **undo traffic classifier** command to remove a traffic behavior.

Related commands: **qos policy, classifier behavior, qos apply policy.**

Examples # Create a traffic behavior **behavior1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

traffic classifier

Syntax **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]
undo traffic classifier *classifier-name*

View System view

Parameters **and**: Specifies the relationship between the match criteria in the specified class as logical AND. That is, a packet belongs to the class only when it matches all the match criteria defined in the class.

or: Specifies the relationship between the match criteria in the class as logical OR. That is, a packet belongs to the class if it matches a match criterion defined in the class.

classifier-name: Class name, a string of 1 to 31 characters.

Description Use the **traffic classifier** command to create a class. This command also leads you to class view.

Use the **undo traffic classifier** command to remove a class.

By default, a packet belongs to the class only when it matches all match criteria defined in the class.

Examples # Create the class **class1**.

```
<Sysname> system-view  
[Sysname] traffic classifier class1  
[Sysname-classifier-class1]
```


13

BPDU TUNNELING CONFIGURATION COMMANDS

bpdu-tunnel dot1q stp

Syntax **bpdu-tunnel dot1q stp**
undo bpdu-tunnel dot1q stp

View Ethernet port view, port group view

Parameters None

Description Use the **bpdu-tunnel dot1q stp** command to enable BPDU tunneling for STP on the current port or ports.

Use the **undo bpdu-tunnel dot1q stp** command to disable BPDU tunneling for STP on the port or ports.

By default, the BPDU tunneling for STP is disabled.

Configured in Ethernet port view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Before you can enable BPDU tunneling for STP on a port, you need to enable BPDU tunneling and disable STP on the port.

Relative command: **bpdu-tunnel dot1q enable**.

Examples # Enable BPDU tunneling for STP on Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] stp disable
[Sysname-Ethernet2/0/1] bpdu-tunnel dot1q stp
```

Enable BPDU tunneling for STP on all the ports of port group 1.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode manual
[Sysname] interface ethernet 2/0/2
[Sysname-Ethernet2/0/2] port link-aggregation group 1
[Sysname-Ethernet2/0/2] interface ethernet 2/0/3
[Sysname-Ethernet2/0/3] port link-aggregation group 1
[Sysname-Ethernet2/0/3] quit
[Sysname] port-group aggregation 1
```

```
[Sysname-port-group-aggregation-1] stp disable
[Sysname-port-group-aggregation-1] bpdu-tunnel dot1q stp
```

bpdu-tunnel dot1q enable

Syntax **bpdu-tunnel dot1q enable**

undo bpdu-tunnel dot1q enable

View System view, Ethernet port view, port group view

Parameters None

Description Use the **bpdu-tunnel dot1q enable** command to enable BPDU tunneling.

Use the **undo bpdu-tunnel dot1q enable** command to disable BPDU tunneling.

Configured in system view, the command enables or disables BPDU tunneling globally; configured in Ethernet port view, the setting is effective on the current port only; configured in port group view, the command enables or disables BPDU tunneling on all ports in the port group.

By default, BPDU tunneling is enabled globally but disabled for all ports.

Note: BPDU tunneling must be enabled globally before the BPDU tunnel configuration for a port can take effect.

Examples # Enable BPDU tunneling globally.

```
<Sysname> system-view
[Sysname] bpdu-tunnel dot1q enable
```

Enable BPDU tunneling on the Ethernet 2/0/1 port.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] bpdu-tunnel dot1q enable
```

Enable BPDU tunneling on all the ports in port group 1.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode manual
[Sysname] interface ethernet 2/0/2
[Sysname-Ethernet2/0/2] port link-aggregation group 1
[Sysname-Ethernet2/0/2] interface ethernet 2/0/3
[Sysname-Ethernet2/0/3] port link-aggregation group 1
[Sysname-Ethernet2/0/3] quit
[Sysname] port-group aggregation 1
[Sysname-port-group-aggregation-1] bpdu-tunnel dot1q enable
```

bpdu-tunnel tunnel-dmac

Syntax **bpdu-tunnel tunnel-dmac** *mac-address*

undo bpdu-tunnel tunnel-dmac

View System view

Parameters *mac-address*: Destination multicast MAC address for BPDU Tunnel frames, in the format of H-H-H. The allowed values are 0100-0CCD-CDD0, 0100-0CCD-CDD1, 0100-0CCD-CDD2, and 010F-E200-0003.

Description Use the **bpdu-tunnel tunnel-dmac** command to configure the destination multicast MAC address for BPDU Tunnel frames.

Use the **undo bpdu-tunnel tunnel-dmac** command to restore the default value.

By default, the destination multicast MAC address for BPDU Tunnel frames is 0x010F-E200-0003.

Examples # Set the destination multicast MAC address for BPDU Tunnel frames to 0100-0CCD-CDD0.

```
<Sysname> system-view  
[Sysname] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```


14

MSTP CONFIGURATION COMMANDS

active region-configuration

Syntax `active region-configuration`

View MST region view

Parameters None

Description Use the **active region-configuration** command to activate your MST region configuration.

When you carry out this command, MSTP will replace the currently running MST region-related parameters with the parameters you have just configured, and will perform spanning tree calculation again.

Related commands: **instance, region-name, revision-level, vlan-mapping modulo, check region-configuration.**

Examples # Activate MST region configuration manually.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] active region-configuration
```

check region-configuration

Syntax `check region-configuration`

View MST region view

Parameters None

Description Use the **check region-configuration** command to view all the configuration information of the MST region, including the region name, VLAN-to-instance mapping and revision level settings.

As specified in the MSTP protocol, the configurations of MST regions must be right, especially the VLAN-to-MSTI mapping table. MSTP-enabled switches are in the same region only when they have the same format selector (a 802.1s-defined

protocol selector, which is 0 by default and cannot be configured), region name, VLAN-to-MSTI mapping table, and revision level. A switch cannot be in the expected region if any of the four MST region-related parameters mentioned above are not consistent with those of another switch in the region.

The 3Com series support only the MST region name, VLAN-to-MSTI mapping table, and revision level. Switches with the settings of these parameters being the same are assigned to the same MST region.

Related commands: **instance, region-name, revision-level, vlan-mapping modulo, active region-configuration.**

Examples # View all the configuration information of the MST region.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
Admin Configuration
  Format selector :0
  Region name    :00b010000001
  Revision level  :0

  Instance      Vlans Mapped
    0           1 to 9, 11 to 4094
    16          10
```

Table 23 Field descriptions of the check region-configuration command

| Field | Description |
|-----------------------|---|
| Format selector | Configuration format selector of the MST region |
| Region name | MST region name |
| Revision level | Revision level of the MST region |
| Instance Vlans Mapped | VLAN-to-instance mappings in the MST region |

display stp

Syntax **display stp** [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]

View Any view

Parameters **instance** *instance-id*: Displays the spanning tree information of a particular spanning tree instance. The effective range of *instance-id* is 0 to 31, with 0 representing the common internal spanning tree (CIST).

interface *interface-list*: Displays the spanning tree information on one or multiple ports. You can provide up to 10 port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number to interface-type end-interface-number*, where the end port number must be greater than the start port number.

slot *slot-number*: Displays the spanning tree information of the module on the specified slot.

brief: Displays brief information.

Description Use the **display stp** command to view the MSTP status information and statistics information.

Based on the MSTP status information and statistics information, you can analyze and maintain the network topology or check whether MSTP is working normally.

Note that:

- If you do not specify any spanning tree instance ID or port list, this command will display the MSTP information on all ports. The displayed information is sequenced by spanning tree instance ID and by port name in each spanning tree instance.
- If you specify a spanning tree instance ID, this command will display the MSTP information on all ports in that spanning tree instance. The displayed information is sequenced by port name.
- If you specify a port list, this command will display the MSTP information on the specified ports. The displayed information is sequenced by spanning tree instance ID, and by port name in each spanning tree instance.
- If you specify both a spanning tree instance ID and a port list, this command will display the MSTP information on the specified ports in the specified spanning tree instance.

The MSTP status information includes:

- CIST global parameters: Protocol work mode, device priority in the CIST instance (Priority), MAC address, hello time, max age, forward delay, maximum hops, common root of the CIST, external path cost from the device to the CIST common root, regional root, the internal path cost from the device to the regional root, CIST root port of the device, and status of the BPDU guard function (enabled or disabled).
- CIST port parameters: Port status, role, priority, path cost, designated bridge, designated port, edge port/non-edge port, whether connecting to a point-to-point link, maximum transmission rate (transmit limit), status of the root guard function (enabled or disabled), BPDU format, boundary port/non-boundary port, hello time, max age, forward delay, message age, remaining hops, whether a port in an aggregation group, and whether rapid state transition enabled (designated ports).
- MSTI global parameters: MSTI instance ID, bridge priority of the instance, regional root, internal path cost, MSTI root port, and master bridge.
- MSTI port parameters: Port status, role, priority, path cost, designated bridge, designated port, remaining hops, whether a port in an aggregation group, and whether rapid state transition enabled (for designated ports).

The statistics information includes:

- The number of TCN BPDUs, configuration BPDUs, RST BPDUs and MST BPDUs sent from each port
- The number of TCN BPDUs, configuration BPDUs, RST BPDUs, MST BPDUs and wrong BPDUs received on each port
- The number of BPDUs discarded on each port

Related commands: `reset stp`.

Examples # Display the state information about MSTI 0 on GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> display stp instance 0 interface GigabitEthernet 2/0/1 to
GigabitEthernet 2/0/4 brief
MSTID      Port                               Role  STP State  Protection
0          GigabitEthernet2/0/1              DESI  FORWARDING NONE
0          GigabitEthernet2/0/2              DESI  FORWARDING NONE
0          GigabitEthernet2/0/3              DESI  FORWARDING NONE
0          GigabitEthernet2/0/4*            DESI  FORWARDING NONE
(*) means port in aggregation group
```

Table 24 Field descriptions of the display stp command

| Field | Description |
|-------------------------------------|---|
| MSTID | spanning tree instance ID in the MST region |
| Port | Port name, corresponding to each spanning tree instance |
| Role | Port role |
| STP State | MSTP status on the port, including forwarding, discarding, and learning |
| Protection | Protection type on the port, including root guard, loop guard, and BPDU guard |
| (*) means port in aggregation group | * indicates a port in an aggregation group |

display stp abnormal-port

Syntax `display stp abnormal-port`

View Any view

Parameters None

Description Use the `display stp abnormal-port` command to view the information about abnormally blocked ports.

Any of the following reasons may cause a port to be abnormally blocked:

- Root guard action
- Loop guard action
- MSTP BPDU format compatibility protection action

Examples # View information about abnormally blocked ports.

```
<Sysname> display stp abnormal-port
MSTID   Blocked Port                               Reason
1       GigabitEthernet2/0/1                       ROOT-Protected
2       GigabitEthernet2/0/2                       LOOP-Protected
2       GigabitEthernet2/0/3                       Formatcompatibility-Protected
```

Table 25 Field descriptions of the display stp abnormal-port command

| Field | Description |
|--------------|---|
| MSTID | spanning tree instance ID |
| Blocked Port | Name of blocked port, which corresponds to the related spanning tree instance |
| Reason | Reason that caused abnormal blocking of the port. <ul style="list-style-type: none"> ■ ROOT-Protected: root guard action ■ LOOP-Protected: loop guard action ■ Formatcompatibility-Protected: MSTP BPDU format compatibility protection action |

display stp down-port

Syntax **display stp down-port**

View Any view

Parameters None

Description Use the **display stp down-port** command to view the information about ports blocked by STP protection actions.

These actions include:

- BPDU attack guard action
- MSTP BPDU format compatibility protection action

Examples # View the information about ports blocked by STP protection actions.

```
<Sysname> display stp down-port
Down Port                               Reason
GigabitEthernet2/0/1                   BPDU-Protected
GigabitEthernet2/0/2                   Formatfrequency-Protected
```

Table 26 Field descriptions of the display stp abnormal-port command

| Field | Description |
|-----------|--|
| Down Port | Name of blocked port |
| Reason | Reason that caused the port to be blocked. <ul style="list-style-type: none"> ■ BPDU-Protected: BPDU attack guard action ■ Formatfrequency-Protected: MSTP BPDU format compatibility protection action |

display stp history

Syntax **display stp** [**instance** *instance-id*] **history** [**slot** *slot-number*]

View Any view

Parameters **instance** *instance-id*: Displays the historic port role calculation information of a particular spanning tree instance. The effective range of *instance-id* is 0 to 31, with 0 representing the common internal spanning tree (CIST).

slot *slot-number*: Displays the historic port role calculation information of the module on the specified slot.

Description Use the **display stp history** command to view the historic port role calculation information of the specified spanning tree instance or all spanning tree instances.

Note that:

- If you do not specify a spanning tree instance ID, this command will display the historic port role calculation information of all spanning tree instances. The displayed information is sequenced by instance ID, and in the timing of port role calculation in each instance.
- If you specify a spanning tree instance ID, this command will display the historic port role calculation information of only this specified spanning instance, in the timing of port role calculation.

Examples # View the historic port role calculation information of the module on slot 1 in MSTP instance 2.

```
<Sysname> display stp instance 2 history slot 1
----- STP slot 1 history trace -----
----- Instance 2 -----
Port GigabitEthernet2/0/1
  Role change   : ROOT->DESI (Aged)
  Time          : 2006/08/08 00:22:56
  Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1

Port GigabitEthernet2/0/2
  Role change   : ALTER->ROOT
  Time          : 2006/08/08 00:22:56
  Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

Table 27 Field descriptions of the display stp history command

| Field | Description |
|---------------|--|
| Port | Port name |
| Role change | A role change of the port ("Age" means that the change was caused by expiry of a configuration BPDU) |
| Time | Time of port role calculation |
| Port priority | Port priority |

display stp region-configuration

Syntax **display stp region-configuration**

View Any view

Parameters None

Description Use the **display stp region-configuration** command to view the currently effective configuration information of the MST region, including the region name, revision level, and user-configured VLAN-to-instance mappings.

Related commands: **stp region-configuration.**

Examples # View the currently effective MST region configuration information.

```
<Sysname> display stp region-configuration
Oper Configuration
  Format selector :0
  Region name    :hello
  Revision level :0

  Instance  Vlans Mapped
    0       21 to 4094
    1       1 to 10
    2       11 to 20
```

Table 28 Field descriptions of the display stp region-configuration command

| Field | Description |
|-----------------------|---|
| Format selector | MSTP-defined format selector |
| Region name | MST region name |
| Revision level | Revision level of the MST region |
| Instance Vlans Mapped | VLAN-to-instance mappings in the MST region |

display stp root

Syntax **display stp root**

View Any view

Parameters None

Description Use the **display stp root** command to view the root bridge information of all MSTP instances.

Examples # View the root bridge information of all MSTP instances.

```
<Sysname> display stp root
MSTID      Root Bridge ID      ExtPathCost  IntPathCost      Root Port
0          0.0013.1923.da80    0            0
```

Table 29 Field descriptions of the display stp root command

| Field | Description |
|----------------|--|
| MSTID | spanning tree instance ID |
| Root Bridge ID | Root bridge ID |
| ExtPathCost | External path cost |
| IntPathCost | Internal path cost |
| Root Port | Root port name (displayed only if a port of the current device is the root port of multiple instances) |

display stp tc

Syntax `display stp [instance instance-id] tc [slot slot-number]`

View Any view

Parameters **instance** *instance-id*: Displays the statistics of TC BPDUs (also known as TCN BPDUs) received and sent by all ports in a particular spanning tree instance. The effective range of *instance-id* is 0 to 31, with 0 representing the common internal spanning tree (CIST).

slot *slot-number*: Displays the statistics of TC BPDUs received and sent by all ports on a particular module spanning tree instance.

Description Use the **display stp tc** command to view the statistics of TC BPDUs received and sent.

Note that:

- If you do not specify a spanning tree instance ID, this command will display the statistics of TC BPDUs received and sent by all ports in all spanning trees. The displayed information is sequenced by instance ID and by port name in each spanning tree instance.
- If you specify a spanning tree instance ID, this command will display the statistics of TC BPDUs received and sent by all ports in the specified spanning tree instance, in port name order.

Examples # View the statistics of TC BPDUs received and sent by all ports on the module on slot 1 in MSTP instance 0.

```
<Sysname> display stp instance 0 tc slot 1
----- STP slot 1 TC or TCN count -----
MSTID      Port                      Receive      Send
0          GigabitEthernet2/0/1      6            4
0          GigabitEthernet2/0/2      0            2
```

Table 30 Field descriptions of the display stp tc command

| Field | Description |
|---------|--|
| MSTID | MSTP instance ID in the MST region |
| Port | Port name |
| Receive | Number of TC BPDUs received on each port |
| Send | Number of TC BPDUs received by each port |

instance

Syntax **instance** *instance-id* **vlan** *vlan-list*

undo instance *instance-id* [**vlan** *vlan-list*]

View MST region view

Parameters *instance-id*: spanning tree instance ID, ranging from 0 to 31, with 0 representing the CIST.

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description Use the **instance** command to map the specified VLAN(s) to the specified spanning tree instance.

Use the **undo instance** command to remap the specified VLAN(s) or all VLANs to the CIST (spanning tree instance 0).

By default, all VLANs are mapped to the CIST.

Notice that:

- If you specify no VLAN in the **undo instance** command, all VLANs mapped to the specified spanning tree instance will be remapped to the CIST.
- You cannot map the same VLAN to different spanning tree instances. If you map a VLAN that has been mapped to an instance to a new instance, the old mapping will be automatically removed.

Related commands: **region-name**, **revision-level**, **vlan-mapping modulo**, **check region-configuration**, **active region-configuration**.

Examples # Map VLAN 2 to spanning tree instance 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
```

region-name**Syntax** **region-name** *name***undo region-name****View** MST region view**Parameters** *name*: Name of the MST region, a string of 1 to 32 characters.**Description** Use the **region-name** command to configure the MST region name of your device.Use the **undo region-name** command to restore the default MST region name.

By default, the MST region name of a device is its MAC address.

The MST region name, the VLAN-to-instance mapping table and the MSTP revision level of a device jointly determine the MST region the device belongs to.

Related commands: **instance, revision-level, vlan-mapping modulo, check region-configuration, active region-configuration.****Examples** # Set the MST region name of the device to "hello".

```

<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name hello

```

reset stp**Syntax** **reset stp** [**interface** *interface-list*]**View** User view**Parameters** **interface** *interface-list*: Clears the spanning tree statistics information on one or multiple ports. You can provide up to 10 port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number to interface-type end-interface-number*, where the end port number must be greater than the start port number.**Description** Use the **reset stp** command to clear the MSTP statistics information.

The MSTP statistics information includes the numbers of TCN BPDUs, configuration BPDUs, RST BPDUs and MST BPDUs sent/received through the specified port(s) (STP BPDUs and TCN BPDUs are counted only for the CIST).

Note that this command clears the spanning tree-related statistics information on the specified port(s) if you specify the *interface-list* argument; otherwise, this command clears the spanning tree-related statistics on all ports.

Related commands: **display stp.**

Examples # Clear the spanning tree-related statistics information on ports GigabitEthernet 2/0/1 through GigabitEthernet 2/0/3.
 <Sysname> reset stp interface GigabitEthernet 2/0/1 to GigabitEthernet 2/0/3

revision-level

Syntax **revision-level** *level*
undo revision-level

View MST region view

Parameters *level*: MSTP revision level, in the range of 0 to 65535. The system default is 0.

Description Use the **region-level** command to configure the MSTP revision level of your device.

Use the **undo region-level** command to restore the default MSTP revision level.

The MSTP revision level, the MST region name and the VLAN-to-instance mapping table of a device jointly determine the MST region the device belongs to.

Related commands: **region-name, instance, vlan-mapping modulo, check region-configuration, active region-configuration.**

Examples # Set the MSTP revision level of the MST region to 5.
 <Sysname> system-view
 [Sysname] stp region-configuration
 [Sysname-mst-region] revision-level 5

stp

Syntax **stp** { **enable** | **disable** }
undo stp

View System view, Ethernet interface view, port group view

Parameters **enable**: Enables the MSTP feature.

disable: Disables the MSTP feature.

Description Use the **stp** command to enable or disable the MSTP feature globally or on the port(s).

Use the **undo stp** command to restore the default MSTP status.

By default, MSTP is globally disabled.

MSTP is disabled on ports by default and automatically enabled on all ports when it is enabled globally on the device.

Note that:

- To control MSTP flexibly, you can disable the MSTP feature for certain ports so that they will not take part in spanning tree calculation and thus to save the device's CPU resources.
- After you enable MSTP, the device determines whether to work in STP-compatible mode, in RSTP mode or in MSTP mode according to your MSTP work mode setting. After MSTP is disabled, the device becomes a transparent bridge.
- After being enabled, MSTP dynamically maintains spanning tree status of the corresponding VLANs based on the received configuration BPDUs. After being disabled, it stops maintaining the spanning tree status.
- Configured in system view, the setting is effective for the device globally; configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Related commands: **stp mode.**

Examples # Enable the MSTP feature globally.

```
<Sysname> system-view
[Sysname] stp enable
```

Disable MSTP on port GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp disable
```

stp bpdu-protection

Syntax **stp bpdu-protection**

undo stp bpdu-protection

View System view

Parameters None

Description Use the **stp bpdu-protection** command to enable the BPDU guard function for the device.

Use the **undo stp bpdu-protection** command to disable the BPDU guard function for the device.

By default, the BPDU guard function is disabled.

Examples # Enable the BPDU guard function for the device.

```
<Sysname> system-view
[Sysname] stp bpdu-protection
```

stp bridge-diameter

Syntax **stp bridge-diameter** *bridge-number*

undo stp bridge-diameter

View System view

Parameters *bridge-number*: Specifies the switched network diameter, in the range of 2 to 7.

Description Use the **stp bridge-diameter** command to specify the network diameter, namely the maximum number of stations between any two terminal devices on the switched network.

Use the **undo stp bridge-diameter** command to restore the default network diameter setting.

By default, the network diameter of the switched network is 7.

An appropriate setting of hello time, forward delay and max age can speed up network convergence. The values of these timers are related to the network size. You can set these three timers indirectly by setting the network diameter. Based on the network diameter you configured, MSTP automatically sets an optimal hello time, forward delay, and max age for the device. With the network diameter set to 7 (the default), the three timer are also set to their defaults.

Note that this configuration is effective for the CIST and root bridge only, and not for MSTIs.

Related commands: **stp timer forward-delay**, **stp timer hello**, **stp timer max-age**.

Examples # Set the network diameter of the switched network to 5.

```
<Sysname> system-view
[Sysname] stp bridge-diameter 5
```

stp compliance

Syntax `stp compliance { auto | dot1s | legacy }`

`undo stp compliance`

View Ethernet interface view, port group view

Parameters **auto**: Configures the port(s) to recognize the MSTP BPDU format automatically and accordingly determine the format of MSTP BPDUs to send.

dot1s: Configures the port(s) to receive and send only standard-format (802.1s-compliant) MSTP BPDUs.

legacy: Configures the port(s) to receive and send only compatible-format MSTP BPDUs.

Description Use the **stp compliance** command to configure the mode the port(s) will use to recognize and send MSTP BPDUs.

Use the **undo stp compliance** command to restore the system default.

The default mode is **auto**, namely all ports recognize the BPDU format automatically.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.
- If the mode is set to **auto** on a port, the port automatically recognizes and resolves the received compatible-format BPDUs or 802.1s-compliant BPDUs, and sends, when needed, compatible-format or 802.1s-compliant BPDUs.
- If the mode is set to **legacy** or **dot1s**, on a port, the port can only receive and send BPDUs of the specified format. If the port is configured not to detect the packet format automatically while it works in the MSTP mode, and if it receives a packet in the format other than as configured, that port will become a designated port, and the port will remain in the discarding state to prevent the occurrence of a loop.

Examples # Configure GigabitEthernet 2/0/1 to receive and send only standard-format (802.1s) MSTP packets.

```
<Sysname>system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp compliance dot1s
```

Restore the default mode for port GigabitEthernet 2/0/1 to recognize and send MSTP BPDUs.

```
<Sysname>system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] undo stp compliance
```

stp config-digest-snooping

Syntax **stp config-digest-snooping**

undo stp config-digest-snooping

View System view, Ethernet interface view, port group view

Parameters None

Description Use the **stp config-digest-snooping** command to enable Digest Snooping.

Use the **undo stp config-digest-snooping** command to disable Digest Snooping.

The feature is disabled by default.

Notice that:

- You need to enable this feature both globally and on ports connected to other vendors' devices to make it take effect. It is recommended to enable the feature on all associated ports first and then globally, making all configured ports take effect at the same time to minimize the impact, and disable the feature globally to disable it on all associated ports.
- It is not recommended to enable Digest Snooping on the MST region edge port to avoid loops.

Examples # Enable Digest Snooping globally.

```
<Sysname> system-view
[Sysname] stp config-digest-snooping
```

Enable Digest Snooping on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp config-digest-snooping
```

stp cost

Syntax **stp [instance *instance-id*] cost *cost***

undo stp [instance *instance-id*] cost

View Ethernet interface view, port group view

Parameters **instance** *instance-id*: Sets the path cost of the port(s) in a particular spanning tree instance. The effective range of *instance-id* is 0 to 31, with 0 representing the CIST.

cost: Path cost of the port, the effective range of which depends on the path cost calculation standard adopted.

Description Use the **stp cost** command to set the path cost of the port(s) in the specified spanning tree instance or all spanning tree instances.

Use the **undo stp cost** command to restore the system default.

By default, the device automatically calculates the path costs of ports in each spanning tree instance based on the corresponding standard.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

If you set *instance-id* to 0, you are setting the path cost of the port in the CIST. The path cost setting of a port can affect the role selection of the port. Setting different path costs for the same port in different spanning tree instances allows different VLAN traffic flows to be forwarded along different physical links, thus to enable per-VLAN load balancing. When the path cost of a port is changed, MSTP will re-compute the role of the port and initiate a state transition.

If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples # Set the path cost of port GigabitEthernet 2/0/1 in spanning tree instance 2 to 200.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp instance 2 cost 200
```

stp edged-port

Syntax **stp edged-port** { **enable** | **disable** }

undo stp edged-port

View Ethernet interface view, port group view

Parameters **enable**: Configures the current port to be an edge port.

disable: Configures the current port to be a non-edge port.

Description Use the **stp edged-port enable** command to configure the port(s) to be an edge port or edge ports.

Use the **stp edged-port disable** or **undo stp edged-port enable** command to configure the port(s) to be a non-edge port or non-edge ports.

All Ethernet ports are non-edge ports by default.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.
- If a port directly connects to a user terminal rather than another device or a shared LAN segment, this port is regarded as an edge port. When the network topology changes, an edge port will not cause a temporary loop. Therefore, configuring a port as an edge port can enable the port to transition to the forwarding state rapidly. We recommend that you configure an Ethernet port directly connecting to a user terminal as an edge port before to enable it to transition to the forwarding state rapidly.
- Normally, configuration BPDUs from other devices cannot reach an edge port because it does not connect to any other device. Before the BPDU guard function is enabled, if a port receives a configuration BPDU, the port is working actually as a non-edge port even if you have configured it as an edge port.

Examples # Configure GigabitEthernet 2/0/1 as a non-edge port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp edged-port disable
```

stp loop-protection

Syntax **stp loop-protection**
undo stp loop-protection

View Ethernet interface view, port group view

Parameters None

Description Use the **stp loop-protection** command to enable the loop guard function on the port(s).

Use the **undo stp loop-protection** command to restore the system default.

By default, the loop guard function is disabled.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Examples # Enable the loop guard function on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp loop-protection
```

stp max-hops

Syntax `stp max-hops hops`

undo stp max-hops

View System view

Parameters *hops*: Maximum hops, in the range of 1 to 40

Description Use the **stp max-hops** command to set the maximum number of hops of the MST region on the device.

Use the **undo stp max-hops** command to restore the maximum number of hops to the default setting.

By default, the maximum number of hops of an MST region is 20.

In the CIST and spanning tree instances, the maximum hops setting configured on the regional root bridge determines the maximum network diameter supported by this MST region. After a configuration BPDU leaves the root bridge, its hop count is decremented by 1 whenever it passes a device. When its hop count reaches 0, it will be discarded by the device that has received it. As a result, devices beyond the maximum hop count are unable to take part in spanning tree calculation, and thereby the size of the MST region is limited.

When the current device becomes the root bridge of the CIST or an MSTI, the maximum hops setting configured on the device becomes the network diameter of that spanning tree and restricts the size of that spanning tree in the current MST region.

Devices other than the root bridge in an MST region use the maximum hops setting on the root bridge.

Examples # Set the maximum number of hops of the MST region to 35.

```
<Sysname> system-view
[Sysname] stp max-hops 35
```

stp mcheck

Syntax `stp mcheck`

View System view, Ethernet interface view

Parameters None

Description Use the **stp mcheck** command to carry out the mCheck operation globally or on the current port.

In a switched network, if a port on the device running MSTP (or RSTP) connects to a device running STP, this port will automatically migrate to the STP-compatible mode. However, if the device running STP is removed, this will not be able to migrate automatically to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode. In this case, you can perform an mCheck operation to force the port to migrate to the MSTP (or RSTP) mode.

Note that the **stp mcheck** command is meaningful only when the device works in the MSTP (or RSTP) mode, not in the STP-compatible mode.

Related commands: **stp mode**.

Examples # Carry out mCheck on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp mcheck
```

stp mode

Syntax **stp mode { stp | rstp | mstp }**

undo stp mode

View System view

Parameters **stp**: Configures the MSTP-compliant device to work in STP-compatible mode.

rstp: Configures MSTP-compliant device to work in RSTP mode.

mstp: Configures MSTP-compliant device to work in MSTP mode.

Description Use the **stp mode** command to configure the MSTP work mode of the device.

Use the **undo stp mode** command to restore the MSTP work mode to the default setting.

By default, an MSTP-compliant device works in MSTP mode.

Related commands: **stp mcheck**, **stp**.


Examples # Configure the MSTP-compliant device to work in STP-compatible mode.

```
<Sysname> system-view
[Sysname] stp mode stp
```

stp no-agreement-check

| | |
|--------------------|---|
| Syntax | stp no-agreement-check
undo stp no-agreement-check |
| View | Ethernet interface view, port group view |
| Parameters | None |
| Description | Use the stp no-agreement-check command to enable No Agreement Check on the port(s).

Use the undo stp no-agreement-check command to disable No Agreement Check on the port(s).

By default, No Agreement Check is disabled. |
| |  <i>The No Agreement Check feature can take effect only on the root port.</i> |
| Examples | # Enable No Agreement Check on GigabitEthernet 2/0/1.

<pre><Sysname> system-view [Sysname] interface GigabitEthernet 2/0/1 [Sysname-GigabitEthernet2/0/1] stp no-agreement-check</pre> |

stp pathcost-standard

| | |
|--------------------|--|
| Syntax | stp pathcost-standard { dot1d-1998 dot1t legacy }
undo stp pathcost-standard |
| View | System view |
| Parameters | dot1d-1998: The device calculates the default path cost for ports based on IEEE 802.1D-1998.

dot1t: The device calculates the default path cost for ports based on IEEE 802.1t.

legacy: The device calculates the default path cost for ports based on a private standard. |
| Description | Use the stp pathcost-standard command to specify a standard for the device to use when calculating the default path cost of the link connected with the device.

Use the undo stp pathcost-standard command to restore the system default.

The default standard used by the device is legacy . |

Note that if you change the standard that the device uses in calculating the default path cost, the port path cost value set through the **stp cost** command will be out of effect.

Table 31 Link speed vs. path cost

| Link speed | Duplex state | 802.1D-1998 | IEEE 802.1t | Private standard |
|------------|-------------------------|-------------|-------------|------------------|
| 0 | - | 65535 | 200,000,000 | 200,000 |
| 10 Mbps | Single Port | 100 | 2,000,000 | 2,000 |
| | Aggregated Link 2 Ports | 100 | 1,000,000 | 1,800 |
| | Aggregated Link 3 Ports | 100 | 666,666 | 1,600 |
| | Aggregated Link 4 Ports | 100 | 500,000 | 1,400 |
| 100 Mbps | Single Port | 19 | 200,000 | 200 |
| | Aggregated Link 2 Ports | 19 | 100,000 | 180 |
| | Aggregated Link 3 Ports | 19 | 66,666 | 160 |
| | Aggregated Link 4 Ports | 19 | 50,000 | 140 |
| 1000 Mbps | Single Port | 4 | 20,000 | 20 |
| | Aggregated Link 2 Ports | 4 | 10,000 | 18 |
| | Aggregated Link 3 Ports | 4 | 6,666 | 16 |
| | Aggregated Link 4 Ports | 4 | 5,000 | 14 |
| 10 Gbps | Single Port | 2 | 2,000 | 2 |
| | Aggregated Link 2 Ports | 2 | 1,000 | 1 |
| | Aggregated Link 3 Ports | 2 | 666 | 1 |
| | Aggregated Link 4 Ports | 2 | 500 | 1 |

In the calculation of the path cost value of an aggregated link, 802.1D-1998 does not take into account the number of ports in the aggregated link. Whereas, 802.1T takes the number of ports in the aggregated link into account. The calculation formula is: Path Cost = 200,000,000/link speed (in 100 kbps), where link speed is the sum of the link speed values of the non-blocked ports in the aggregated link.

Examples # Configure the device to calculate the default path cost for ports based on IEEE 802.1D-1998.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
```

Configure the device to calculate the default path cost for ports based on IEEE 802.1t.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1t
```

stp point-to-point

Syntax **stp point-to-point** { **auto** | **force-false** | **force-true** }

undo stp point-to-point

- View** Ethernet interface view, port group view
- Parameters** **auto**: Specifies automatic detection of the link type.
- force-false**: Specifies the non-point-to-point link type.
- force-true**: Specifies the point-to-point link type.
- Description** Use the **stp point-to-point** command to specify whether the current port(s) connect(s) to a point-to-point link or point-to-point links.
- Use the **undo stp point-to-point** command to restore the system default.
- The default setting is **auto**; namely the MSTP-compliant device automatically detects whether an Ethernet port connects to a point-to-point link.
- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.
- Note that:
- When connecting to a non-point-to-point link, a port is incapable of rapid state transition.
 - If the current port is the master port of a link aggregation group or if it works in full duplex mode, the link to which the current port connects is a point-to-point link. We recommend that you use the default setting, namely let MSTP detect the link status automatically.
 - This setting is effective to the CIST and all spanning tree instances. If a port is configured as connecting to a point-to-point link or a non-point-to-point link, the setting takes effect for the port in all spanning tree instances. If the physical link to which the port connects is not a point-to-point link and you force it to be a point-to-point link by configuration, your configuration may incur a temporary loop.

Examples # Configure port GigabitEthernet 2/0/1 as connecting to a point-to-point link.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp point-to-point force-true
```

stp port-log

- Syntax** **stp port-log** { **all** | **instance** *instance-id* }
- undo stp port-log** { **all** | **instance** *instance-id* }
- View** System view
- Parameters** **all**: Enables output of port state transition information for all instances.

instance *instance-id*: Enables output of port state transition information for the specified spanning tree instance. The effective range of *instance-id* is 0 to 31, with 0 representing the CIST.

Description Use the **stp port-log** command to enable the output of port state transition information for the specified instance or all instances.

Use the **undo stp port-log** command to disable the output of port state transition information for the specified instance or all instances.

By default, the output of port state transition information is enabled.

Examples # Enable output of port state transition information for instance 2.

```
<Sysname> system-view
[Sysname] stp port-log instance 2
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PDISC: Instance 2's Gigabit
Ethernet2/0/1 has been set to discarding state!
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PFWD: Instance 2's GigabitE
thernet2/0/2 has been set to forwarding state!
```

// The information above shows that in instance 2, the state of GigabitEthernet 2/0/1 has changed to discarding and that of GigabitEthernet 2/0/2 has changed to forwarding.

stp port priority

Syntax **stp** [**instance** *instance-id*] **port priority** *priority*

undo stp [**instance** *instance-id*] **port priority**

View Ethernet interface view, port group view

Parameters **instance** *instance-id*: Sets the priority of the current port(s) in a particular spanning tree instance. The effective range of *instance-id* is 0 to 31, with 0 representing the CIST.

priority: Port priority, in the range of 0 to 240 at the step of 16 (0, 16, 32..., for example).

Description Use the **stp port priority** command to set the priority of the port(s).

Use the **undo stp port priority** command to restore the system default.

By default, the port priority is 128.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

If you set *instance-id* to 0, you are setting the priority of the port in the CIST. The priority of a port can affect the role selection of the port in the specified spanning tree instance.

Setting different priorities for the same port in different spanning tree instances allows different VLAN traffic flows to be forwarded along different physical links, thus to enable per-VLAN load balancing.

When the priority of a port is changed, MSTP will re-compute the role of the port and initiate a state transition.

If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples # Set the priority of port GigabitEthernet 2/0/1 in spanning tree instance 2 to 16.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp instance 2 port priority 16
```

stp priority

Syntax **stp** [**instance** *instance-id*] **priority** *priority*

undo stp [**instance** *instance-id*] **priority**

View System view

Parameters **instance** *instance-id*: Sets the priority of the device in a particular spanning tree instance. The effective range of *instance-id* is 0 to 31, with 0 representing the CIST.

priority: Port priority, in the range of 0 to 61440 at the step of 4096, namely you can set up to 16 priority values, such as 0, 4096, 8192..., on the device.

Description Use the **stp priority** command to set the priority of the device.

Use the **undo stp priority** command to restore the default device priority.

By default, the device priority is 32768.

The device priority is involved in spanning tree calculation. The device priority is set on a per-instance basis. An MSTP-compliant device can have different priorities in different spanning tree instances.

If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples # Set the device priority in spanning tree instance 1 to 4096.

```
<Sysname> system-view
[Sysname] stp instance 1 priority 4096
```

stp region-configuration

| | |
|--------------------|--|
| Syntax | stp region-configuration

undo stp region-configuration |
| View | System view |
| Parameters | None |
| Description | <p>Use the stp region-configuration command to enter MST region view.</p> <p>Use the undo stp region-configuration command to restore the default MST region configurations.</p> <p>By default, the default settings are used for all the three MST region parameters. Namely, the device's MST region name is the device's MAC address, all VLANs are mapped to the CIST, and the MSTP revision level is 0.</p> <p>After you enter MST region view, you can configure the parameters related to the MST region, including the region name, VLAN-to-instance mapping and revision level.</p> |
| Examples | <pre># Enter MST region view. <Sysname> system-view [Sysname] stp region-configuration [Sysname-mst-region]</pre> |

stp root primary

| | |
|--------------------|--|
| Syntax | stp [instance <i>instance-id</i>] root primary [bridge-diameter <i>bridge-number</i>]
[hello-time <i>centi-seconds</i>]

undo stp [instance <i>instance-id</i>] root |
| View | System view |
| Parameters | <p>instance <i>instance-id</i>: Configures the device as the root bridge in a particular spanning tree instance. The effect range of <i>instance-id</i> is 0 to 31, with 0 representing the CIST.</p> <p><i>bridge-number</i>: Network diameter of the spanning tree, in the range of 2 to 7 and defaulting to 7.</p> <p><i>centi-seconds</i>: Hello time (in centiseconds) of the spanning tree, in the range of 100 to 1,000.</p> |
| Description | Use the stp root primary command to configure the current device as the root bridge. |

Use the **undo stp root** command to restore the system default.

By default, a device is not a root bridge.

Note that:

- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.
- There is only one root bridge in effect in a spanning tree instance. If two or more devices have been designated to be root bridges of the same spanning tree instance, MSTP will select the device with the lowest MAC address as the root bridge.
- You can specify a root bridge for each spanning tree instance without caring about the device priority. After specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.
- When configuring a root bridge, you can use this command to specify the network diameter of the switched network, so that the MSTP-compliant device automatically calculates the three timers (hello time, forward delay and max age). As the calculated hello time value is not the optimal value, you can specify a hello time value by providing **hello-time** *centi-seconds* in the command, which will override the hello time value calculated by the device based on the network diameter. Generally, we recommend that you use the values of the other two timers calculated by the device based on the specified network diameter.
- The configured network diameter and hello time settings are effective only for spanning tree instance 0, namely the CIST. If you configure these two timers for any other instance, your configuration can succeed, but they will not actually work.

Examples # Define the current device as the root bridge of spanning tree instance 0 and set the network diameter to 4 and the hello time of the device to 500 centiseconds.

```
<Sysname> system-view
[Sysname] stp instance 0 root primary bridge-diameter 4 hello-time 500
```

stp root secondary

Syntax **stp** [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridge-number*] [**hello-time** *centi-seconds*]

undo stp [**instance** *instance-id*] **root**

View System view

Parameters **instance** *instance-id*: Configures the device as a secondary root bridge in a particular spanning tree instance. The effective range of *instance-id* is 0 to 31, with 0 representing the CIST.

bridge-number: Network diameter of the spanning tree, in the range of 2 to 7 and defaulting to 7.

centi-seconds: Hello time (in centiseconds) of the spanning tree, in the range of 100 to 1,000.

Description Use the **stp root secondary** command to configure the device as a secondary root bridge.

Use the **undo stp root** command to restore the system default.

By default, a device is not a secondary root bridge.

Note that:

- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.
- You can configure one or more secondary root bridges for each spanning tree instance. When the root bridge of an instance fails or is shut down, the secondary root bridge can take over the role of the instance of the specified spanning tree instance. If you specify more than one secondary root bridge, the secondary root bridge with the lowest MAC address will become the root bridge.
- When configuring a secondary root bridge, you can specify the network diameter of the switched network and the hello time for the secondary root bridge, so that the MSTP-compliant device automatically calculates the other two timers (forward delay and max age) of the root bridge.
- The configured network diameter and hello time settings are effective only for spanning tree instance 0, namely the CIST. If you configure these two timers for any other instance, your configuration can succeed, but they will not actually work.
- If you set *instance-id* to 0, you are specifying the current device as the secondary root bridge of the CIST.
- Upon specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.

Examples # Define the current device as the secondary root bridge of spanning tree instance 0 and set the network diameter to 5 and the hello time of the device to 300 centiseconds.

```
<Sysname> system-view
[Sysname] stp instance 0 root secondary bridge-diameter 5 hello-time 300
```

stp root-protection

Syntax **stp root-protection**
undo stp root-protection

View Ethernet interface view, port group view

| | |
|--------------------|--|
| Parameters | None |
| Description | <p>Use the stp root-protection command to enable the root guard function on the port(s).</p> <p>Use the undo stp root-protection command to disable the root guard function on the port(s).</p> <p>By default, the root guard function is disabled.</p> <p>Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.</p> |
| Examples | <pre># Enable the root guard function for port GigabitEthernet 2/0/1. <Sysname> system-view [Sysname] interface GigabitEthernet 2/0/1 [Sysname-GigabitEthernet2/0/1] stp root-protection</pre> |

stp tc-protection

| | |
|--------------------|--|
| Syntax | <p>stp tc-protection enable</p> <p>stp tc-protection disable</p> |
| View | System view |
| Parameters | None |
| Description | <p>Use the stp tc-protection enable command to enable the TC-BPDU attack guard function for the device.</p> <p>Use the stp tc-protection disable command to disable the TC-BPDU attack guard function for the device.</p> <p>By default, the TC-BPDU attack guard function is enabled.</p> |
| Examples | <pre># Enable the TC-BPDU attack guard function for the device. <Sysname> system-view [Sysname] stp tc-protection enable</pre> |

stp tc-protection threshold

| | |
|---------------|--|
| Syntax | <p>stp tc-protection threshold <i>number</i></p> <p>undo stp tc-protection threshold</p> |
| View | System view |

Parameters *number*: Maximum number of times the device deletes forwarding address entries within a certain period of time immediately after it receives TC-BPDUs, in the range of 1 to 255.

Description Use the **stp tc-protection threshold** command to configure the maximum number of times the device deletes forwarding address entries within 10 seconds immediately after it receives TC-BPDUs.

Use the **undo stp tc-protection threshold** command to restore the system default.

By default, the device deletes forwarding address entries a maximum of six times within a certain period of time immediately after it receives TC-BPDUs.

Examples # Set the maximum number of times the device deletes forwarding address entries within a certain period of time immediately after it receives TC-BPDUs to 10.

```
<Sysname> system-view
[Sysname] stp tc-protection threshold 10
```

stp timer forward-delay

Syntax **stp timer forward-delay** *centi-seconds*

undo stp timer forward-delay

View System view

Parameters *centi-seconds*: Forward delay in centiseconds, in the range of 400 to 3,000.

Description Use the **stp timer forward-delay** command to set the forward delay timer of the device.

Use the **undo stp timer forward-delay** command to restore the system default.

By default, the forward delay timer is set to 1,500 centiseconds.

In order to prevent temporary loops, a port must go through an intermediate state, the learning state, before it transitions from the discarding state to the forwarding state, and must wait a certain period of time before it transitions from one state to another to keep synchronized with the remote device during state transition. The forward delay timer set on the root bridge determines the time interval of state transition.

If the current device is the root bridge, the state transition interval of the device depends on the set forward delay value; for a secondary root bridge, its state transition interval is determined by the forward delay timer set on the root bridge.

The setting of the hello time, forward delay and max age timers must meet the following formulae:

- $2 \times (\text{forward delay} - 1 \text{ second}) \rightarrow \text{max age}$
- $\text{Max age} \rightarrow 2 \times (\text{hello Time} + 1 \text{ second})$

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, network instability will frequently occur. We recommend that you specify the network diameter of the switched network in the **stp root primary** command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer hello, stp timer max-age, stp bridge-diameter.**

Examples # Set the forward delay timer of the device to 2,000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer forward-delay 2000
```

stp timer hello

Syntax **stp timer hello** *centi-seconds*

undo stp timer hello

View System view

Parameters *centi-seconds*: Hello time (in centiseconds), in the range of 100 to 1,000.

Description Use the **stp timer hello** command to set the hello time of the device.

Use the **undo stp timer hello** command to restore the system default.

By default, the hello time is set to 200 centiseconds.

Hello time is the time interval at which MSTP-compliant devices send configuration BPDUs to maintain spanning tree stability. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree calculation process will be triggered due to timeout. The root bridge sends configuration BPDUs at the interval of the hello time set on the device, while secondary root bridges use the hello time set on the root bridge.

The setting of the hello time, forward delay and max age timers must meet the following formulae:

- $2 \times (\text{forward delay} - 1 \text{ second}) \rightarrow \text{max age}$
- $\text{Max age} \rightarrow 2 \times (\text{hello time} + 1 \text{ second})$

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, network instability will frequently occur. We recommend that you specify the network diameter of the switched network in the **stp root primary** command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer forward-delay, stp timer max-age, stp bridge-diameter.**

Examples # Set the hello time of the device to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer hello 400
```

stp timer max-age

Syntax **stp timer max-age** *centi-seconds*

undo stp timer max-age

View System view

Parameters *centi-seconds*: Max age (in centiseconds), in the range of 600 to 4,000.

Description Use the **stp timer max-age** command to set the max age timer of the device.

Use the **undo stp timer max-age** command to restore the system default.

By default, the max age is set to 2,000 centiseconds.

MSTP can detect link faults and automatically restore the forwarding state of the redundant link. In the CIST, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If a port receives a configuration BPDU that has expired, that spanning tree instance needs to be re-computed.

The max age timer is not meaningful for MSTIs. If the current device is the root bridge of the CIST, it determines whether a configuration BPDU has expired based on the configured max age timer; if the current device is not the root bridge of the CIST, it uses the max age timer set on the CIST root bridge.

The setting of the hello time, forward delay and max age timers must meet the following formulae:

- $2 \times (\text{forward delay} - 1 \text{ second}) \rightarrow \text{max age}$
- $\text{Max age} \rightarrow 2 \times (\text{hello time} + 1 \text{ second})$

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, network instability will frequently occur. We recommend that you specify the network diameter in the **stp root primary** command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer forward-delay, stp timer hello, stp bridge-diameter.**

Examples # Set the max age timer of the device to 1,000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer max-age 1000
```

stp timer-factor

Syntax **stp timer-factor** *number*

undo stp timer-factor

View System view

Parameters *number*: Timeout factor, in the range of 1 to 20.

Description Use the **stp timer-factor** command to configure the timeout time of the device by setting the timeout factor. Timeout time = timeout factor × 3 × hello time.

Use the **undo stp timer-factor** command to restore the default timeout factor.

By default, the timeout factor of the device is set to 3.

After the network topology is stabilized, each non-root-bridge device forwards configuration BPDUs to the surrounding devices at the interval of hello time to check whether any link is faulty. Typically, if a device does not receive a BPDU from the upstream device within nine times the hello time, it will assume that the upstream device has failed and start a new spanning tree calculation process.

In a very stable network, this kind of spanning tree calculation may occur because the upstream device is busy. In this case, you can avoid such unwanted spanning tree calculation by lengthening the timeout time (by setting the timeout factor to 4 or more). We recommend that you set the timeout factor to 5, or 6, or 7 for a stable network.

Examples # Set the timeout factor of the device to 7.

```
<Sysname> system-view  
[Sysname] stp timer-factor 7
```

stp transmit-limit

Syntax **stp transmit-limit** *packet-number*

undo stp transmit-limit

View Ethernet interface view, port group view

Parameters *packet-number*: Maximum number of MSTP packets that the port can send within each hello time, namely the maximum transmission rate of the port, in the range of 1 to 255.

Description Use the **stp transmit-limit** command to set the maximum transmission rate of the port(s).

Use the **undo stp transmit-limit** command to restore the system default.

By default, the maximum transmission rate of all ports of the device is 10.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

A larger maximum transmission rate value represents more MSTP packets that the port will send within each hello time, but this means that more device resources will be used. An appropriate maximum transmission rate setting can prevent MSTP from using an excessive bandwidth resource during network topology instability.

Examples # Set the maximum transmission rate of port GigabitEthernet 2/0/1 to 5.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp transmit-limit 5
```

vlan-mapping modulo

Syntax **vlan-mapping modulo** *modulo*

View MST region view

Parameters *modulo*: Modulo value, in the range of 1 to 31.

Description Use the **vlan-mapping modulo** command to map VLANs in the current MST region to spanning tree instances according to the specified modulo value.

By default, all VLANs are mapped to the CIST (instance 0).

You cannot map the same VLAN to different spanning tree instances. If you map a VLAN that has been mapped to an instance to a new instance, the old mapping will be automatically removed.



*By using the **vlan-mapping modulo** command, you can quickly specify a VLAN for each spanning tree instance. This command maps each VLAN to the spanning tree instance whose ID is $(VLAN\ ID - 1) \% modulo + 1$, where $(VLAN\ ID - 1) \% modulo$ is the modulo operation for $(VLAN\ ID - 1)$. If the modulo value is 16, for example, then VLAN 1 will be mapped to MSTI 1, VLAN 2 to MSTI 2, VLAN 16 to MSTI 16, VLAN 17 to MSTI 1, and so on.*

Related commands: **region-name, revision-level, check region-configuration, active region-configuration.**

Examples # Map VLANs to MSTIs as per modulo 16.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 16
```


15

LINK AGGREGATION CONFIGURATION COMMANDS

display lacp system-id

Syntax `display lacp system-id`

View Any view

Parameters None

Description Use the **display lacp system-id** command to display the local system ID (also called the actor system ID), which comprises the system LACP priority and the system MAC address.

Examples # Display the local system ID.

```
<Sysname> display lacp system-id
Actor System ID: 0x8000, 0000-fc00-0100
```

display link-aggregation interface

Syntax `display link-aggregation interface interface-type interface-number [to interface-type interface-number]`

View Any view

Parameters **interface** *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies a port range or a port if the **to** keyword and the second port are not specified.

Description Use the **display link-aggregation interface** command to display detailed information about link aggregation for the specified port or ports.

You may find that information about the remote system is replaced by 0 and no statistics about LACPDUs are provided for manual link aggregation groups. This is normal because this type of aggregation group has no knowledge of its partner and does not use LACP PDUs for maintaining link aggregation.

Examples # Display detailed information about link aggregation for port Ethernet 2/0/1 in a manual aggregation group.

```
<Sysname> display link-aggregation interface ethernet 2/0/1
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
```

```
Ethernet2/0/1:
  Selected AggID: 1
  Local:
    Port-Priority: 32768, Oper key: 1, Flag: {}
  Remote:
    System ID: 0x0, 0000-0000-0000
    Port Number: 0, Port-Priority: 0, Oper-key: 0, Flag: {}
```

Display detailed information about link aggregation for port Ethernet 2/0/2 in a static aggregation group.

```
<Sysname> display link-aggregation interface ethernet 2/0/2
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
```

```
Ethernet2/0/2:
  Selected AggID: 20
  Local:
    Port-Priority: 32768, Oper key: 2, Flag: {ACDEF}
  Remote:
    System ID: 0x8000, 000e-84a6-fb00
    Port Number: 2, Port-Priority: 32768 , Oper-key: 10, Flag: {ACDEF}
    Received LACP Packets: 8 packet(s), Illegal: 0 packet(s)
    Sent LACP Packets: 9 packet(s)
```

Table 32 Field descriptions of the display link-aggregation interface command

| Field | Description |
|----------------|--|
| Flags | <p>One-octet LACP state flags field. From the least to the most significant bit, they are represented by A through H as follows:</p> <ul style="list-style-type: none"> ■ A indicates whether LACP is enabled, 1 for enabled and 0 for disabled. ■ B indicates the timeout control value, 1 for short timeout, and 0 for long timeout. ■ C indicates whether the sending system considers this link to be aggregatable, 1 for true, and 0 for false. ■ D indicates whether the sending system considers that this link is synchronized, 1 for true, and 0 for false. ■ E indicates whether the sending end considers that collection of incoming frames is enabled on the link, 1 for true and 0 for false. ■ F indicates whether the sending system considers that distribution of outgoing frames is enabled on the link, 1 for true and 0 for false. ■ G indicates whether the receive state machine of the sending system is using default operational partner information, 1 for true and 0 for false. ■ H indicates whether the receive state machine of the sending system is in the expired state, 1 for true and 0 for false. <p>If a flag bit is set to 1, the corresponding English letter that otherwise is not output displays.</p> |
| Selected AggID | ID of the link aggregation group of which this port is a member |

Table 32 Field descriptions of the display link-aggregation interface command

| Field | Description |
|--|---|
| Local:
Port-Priority, Oper key,
Flag | Local port LACP priority, operational key, LACP state flag |
| Remote:
System ID, Port Number,
Port-Priority, Oper-key,
Flag | Remote system ID, port number, port LACP priority, operational key, and LACP state flag |
| Received LACP Packets,
Illegal, Sent LACP Packets | Statistics about received, invalid, and sent LACP packets |

display link-aggregation service-type

Syntax `display link-aggregation service-type [agg-id]`

View Any view

Parameters *agg-id*: ID of an existing service loop group.

Description Use the **display link-aggregation service-type** command to display information about the specified service loop groups.

If no aggregation group is specified, information about all service loop groups is displayed.

Examples # Display information about service loop group 1.

```
<Sysname> display link-aggregation service-type 1
Service-Loop      Service      Quote
Group ID          Type         Number
-----
1                  tunnel      0
```

Table 33 Field descriptions of the display link-aggregation service-type command

| Field | Description |
|-----------------------|---|
| Service-Loop Group ID | Service loop group ID |
| Service Type | Service type supported by the group |
| Quote Number | Reference count for the service loop group. Only after it decreases to zero can you remove the group. |

display link-aggregation summary

Syntax `display link-aggregation summary`

View Any view

Parameters None

Description Use the **display link-aggregation summary** command to display a summary for all link aggregation groups.

You may find that information about the remote system for a manual link aggregation group is either replaced by none or not displayed at all. This is normal because this type of aggregation group has no knowledge of its partner.

Examples # Display the link aggregation group summary.

```
<Sysname> display link-aggregation summary
Aggregation Group Type: S -- Static, M -- Manual
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor ID: 0x8000, 0000-fcfc-ff04
```

| AL ID | AL Type | Partner ID | Select Ports | Unselect Ports | Share Type | Master Port |
|-------|---------|-----------------------|--------------|----------------|------------|---------------|
| 10 | M | none | 1 | 0 | NonS | Ethernet2/0/2 |
| 20 | S | 0x8000,0000-fcfc-ff01 | 1 | 0 | NonS | Ethernet2/0/3 |

Table 34 Field descriptions of the display link-aggregation summary command

| Field | Description |
|------------------------|---|
| Aggregation Group Type | Aggregation group type. <ul style="list-style-type: none"> ■ S: static LACP aggregation ■ M: manual aggregation |
| Loadsharing Type | Load sharing type |
| Actor ID | Local system ID |
| AL ID | Link aggregation group ID |
| AL Type | Link aggregation type |
| Partner ID | Remote system ID |
| Select Ports | Number of selected ports |
| Unselect Ports | Number of unselected ports |
| Share Type | Load sharing type |
| Master Port | Master port |

display link-aggregation verbose

Syntax **display link-aggregation verbose** [*agg-id*]

View Any view

Parameters *agg-id*: ID of an existing link aggregation group.

Description Use the **display link-aggregation verbose** command to display detailed information about the specified or all link aggregation groups.

You may find that information about the remote system for a manual link aggregation group is either replaced by none or not displayed at all. This is normal because this type of aggregation group has no knowledge of its partner.

Examples # Display detailed information about all the link aggregation groups.

```

<Sysname> display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Flags: A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
      D -- Synchronization, E -- Collecting, F -- Distributing,
      G -- Defaulted, H -- Expired

Aggregation ID: 1, AggregationType: Manual, Loadsharing Type: Shar
Aggregation Description:
System ID: 0x8000, 0000-fc00-6504
Port Status: S -- Selected, U -- Unselected
Local:
  Port          Status  Priority  Oper-Key  Flag
  -----
  Eth2/0/23    S      32768    1         {}

Remote:
  Actor          Partner Priority  Oper-Key  SystemID          Flag
  -----
  Eth2/0/23     0      0        0         0x0000,0000-0000-0000 {}

```

Table 35 Field descriptions of the display link-aggregation verbose command

| Field | Description |
|---|---|
| Loadsharing Type | Load sharing type, either shar for load sharing or NonS for non-load sharing |
| Flags | <p>One-octet LACP flags field indicates the actor state variables for the port. From the least to the most significant bit, they are represented by A through H as follows:</p> <ul style="list-style-type: none"> ■ A indicates the enabling/disabling state of LACP, 1 for enabled and 0 for disabled ■ B indicates the timeout control value, 1 for short timeout, and 0 for long timeout ■ C indicates whether the sending system considers this link to be aggregatable, 1 for true, and 0 for false ■ D indicates whether the sending system considers that this link is synchronized, 1 for true, and 0 for false ■ E indicates whether the sending system considers that collection of incoming frames is enabled on the link, 1 for true and 0 for false ■ F indicates whether the sending system considers that distribution of outgoing frames is enabled on the link, 1 for true and 0 for false ■ G indicates whether the receive state machine of the sending system is using default operational partner information, 1 for true and 0 for false ■ H indicates whether the receive state machine of the sending system is in the expired state, 1 for true and 0 for false <p>If a flag bit is set to 1, the corresponding English letter that otherwise is not output displays.</p> |
| Aggregation ID | Link aggregation group ID |
| AggregationType | Link aggregation type: manual or static LACP. |
| Aggregation Description | Link aggregation group name |
| System ID | Local system ID |
| Port Status | Port state in a link aggregation group: selected or unselected |
| Local:
Port, Status, Priority,
Oper-key, Flag | Other information about the local end, including member ports, port state, port LACP priority, operational key, and flags |

Table 35 Field descriptions of the display link-aggregation verbose command

| Field | Description |
|--|---|
| Remote:
Actor, Partner, Priority,
Oper-key, SystemID, Flag | Detailed information about the remote end, including corresponding local port, port ID, port LACP priority, operational key, system ID, and flags |

lacp port-priority

Syntax **lacp port-priority** *port-priority*

undo lacp port-priority

View Ethernet port view

Parameters *port-priority*: Port LACP priority, in the range 0 to 65535.

Description Use the **lacp port-priority** command to assign an LACP priority to the port.
Use the **undo lacp port-priority** command to restore the default.
By default, port LACP priority is 32768.

Examples # Assign LACP priority 64 to a port.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] lacp port-priority 64
```

lacp system-priority

Syntax **lacp system-priority** *system-priority*

undo lacp system-priority

View System view

Parameters *system-priority*: System LACP priority, in the range 0 to 65535.

Description Use the **lacp system-priority** command to assign an LACP priority to the local system.
Use the **undo lacp system-priority** command to restore the default.
By default, system LACP priority is 32768.

Examples # Assign LACP priority 64 to the local system.

```
<Sysname> system-view
[Sysname] lacp system-priority 64
```

link-aggregation group description

Syntax `link-aggregation group agg-id description agg-name`

`undo link-aggregation group agg-id description`

View System view

Parameters *agg-id*: Link aggregation group ID.

agg-name: Link aggregation group name, a string of 1 to 32 characters.

Description Use the **link-aggregation group description** command to configure a name for the specified link aggregation group.

Use the **undo link-aggregation group description** command to remove the name of the specified link aggregation group.

Related commands: **display link-aggregation verbose.**

Examples # Name link aggregation group 22 as abc.

```
<Sysname> system-view
[Sysname] link-aggregation group 22 description abc
```

link-aggregation group mode

Syntax `link-aggregation group agg-id mode { manual | static }`

`undo link-aggregation group agg-id`

View System view

Parameters *agg-id*: Link aggregation group ID.

manual: Creates a manual link aggregation group.

static: Creates a static LACP link aggregation group.

Description Use the **link-aggregation group mode** command to create a link aggregation group.

Use the **undo link-aggregation group** command to remove a link aggregation group. If the group is functioning as a service loop group, this can result in the removal of the service loop group.

An aggregation group currently being referenced by other modules cannot be removed.

Related commands: `display link-aggregation summary`.

Examples # Create manual link aggregation group 22.

```
<Sysname> system-view
[Sysname] link-aggregation group 22 mode manual
```

link-aggregation group service-type

Syntax `link-aggregation group agg-id service-type tunnel`

`undo link-aggregation group agg-id service-type`

View System view

Parameters *agg-id*: Link aggregation group ID.

tunnel: Sets the service type to **tunnel**.

Description Use the **link-aggregation group service-type** command to configure a manual aggregation group as a service loop group that is of specific type.

Use the **undo link-aggregation group service-type** command to change a service loop group back to a common manual aggregation group.



*You can remove an existing service loop group using the **undo link-aggregation group** command. However, service loop groups currently referenced by modules cannot be removed.*

Examples # Configure link aggregation group 5 as a tunnel service loop group.

```
<Sysname> system-view
[Sysname] link-aggregation group 5 service-type tunnel
```

port link-aggregation group

Syntax `port link-aggregation group agg-id`

`undo port link-aggregation group`

View Ethernet port view

Parameters *agg-id*: Link aggregation group ID.

Description Use the **port link-aggregation group** command to add the Ethernet port to the specified link aggregation group (manual or static LACP) or service loop group.

Use the **undo port link-aggregation group** command to remove the Ethernet port from the specified aggregation group or service loop group.

Related commands: **display link-aggregation verbose.**

Examples # Add port Ethernet 2/0/1 to link aggregation group **22**.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-aggregation group 22
```

port-group aggregation

Syntax **port-group aggregation** *agg-id*

View System view

Parameters *agg-id*: Aggregation port group ID, same as the ID of its corresponding link aggregation group.

Description Use the **port-group aggregation** command to enter aggregation port group view.

Instead of being created administratively, an aggregation port group is created automatically upon creation of a link aggregation group and assigned the ID of the link aggregation group. In aggregation port group view, you can configure aggregation related settings such as STP, VLAN, QoS, GVRP, Q-in-Q, BPDU tunnel, and MAC address learning, but cannot add or remove member ports.

Examples # Enter aggregation port group view.

```
<Sysname> system-view
[Sysname] port-group aggregation 10
[Sysname-port-group-aggregation-10]
```

reset lacp statistics

Syntax **reset lacp statistics** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

View User view

Parameters **interface** *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies an interface range or an interface if the **to** keyword and the second interface are not specified.

Description Use the **reset lacp statistics** command to clear statistics about LACP on a specified port or ports.

Related commands: **display link-aggregation interface.**

Examples # Clear statistics about LACP on all ports.

```
<Sysname> reset lacp statistics
```


16

GARP/GVRP CONFIGURATION COMMANDS

display garp statistics

Syntax `display garp statistics [interface interface-list]`

View Any view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> means that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **display garp statistics** command to display GARP statistics of specified or all the ports.

Note that:

- If the **interface** *interface-list* keyword-argument combination is not specified, this command displays the GARP statistics of all the ports.
- If the **interface** *interface-list* keyword-argument combination is specified, this command displays the GARP statistics of the specified ports.

Examples # Display statistics about GARP for port Ethernet 2/0/1.

```
<Sysname> display garp statistics interface ethernet2/0/1
GARP statistics on port Ethernet2/0/1
```

```
Number of GVRP Frames Received      : 0
Number of GVRP Frames Transmitted   : 0
Number of Frames Discarded           : 0
```

display garp timer

Syntax `display garp timer [interface interface-list]`

View Any view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> means that you can specify up to 10 port ranges. A port range

defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **display garp timer** command to display GARP timer settings of specific ports.

Note that:

- If the **interface** *interface-list* keyword-argument combination is not specified, this command displays the GARP timer settings of all the ports.
- If the **interface** *interface-list* keyword-argument combination is specified, this command displays the GARP timer settings of the specified ports.

Related commands: **garp timer, garp timer leaveall.**

Examples # Display GARP timers on port Ethernet 2/0/1.

```
<Sysname> display garp timer interface ethernet 2/0/1
GARP timers on port Ethernet2/0/1

Garp Join Time           : 20 centiseconds
Garp Leave Time          : 60 centiseconds
Garp LeaveAll Time       : 1000 centiseconds
Garp Hold Time           : 10 centiseconds
```

garp timer

Syntax **garp timer** { **hold** | **join** | **leave** } *timer-value*

undo garp timer { **hold** | **join** | **leave** }

View Ethernet port view, port group view

Parameters **hold**: Sets the hold timer.

join: Sets the join timer.

leave: Sets the leave timer.

timer-value: Timer setting (in centiseconds), which must be a multiple of 5 centiseconds.

Description Use the **garp timer** command to set a GARP timer for an Ethernet port or all ports in a port group in compliance with the timer setting dependencies shown in Table 36.

Use the **undo garp timer** command to restore the default of a GARP timer. This may fail if the default does not satisfy the dependencies shown in Table 36.

By default, the hold timer, the join timer, and the leave timer are set to 10 centiseconds, 20 centiseconds, and 60 centiseconds.

Note that:

- In Ethernet port view, these two commands apply to the current port only; in port group view, these two commands apply to all the ports in the port group.
- When restoring the default GARP timers, you are recommended to do that on the timers in the order of hold, join, leave, and leaveall.
- When configuring GARP timers, note that their values are dependent on each other and must be a multiplier of five centiseconds. If the value range for a timer is not desired, you may change it by tuning the value of another timer as shown in the following table:

Table 36 Dependencies of GARP timers

| Timer | Lower limit | Upper limit |
|----------|--|---|
| Hold | 10 centiseconds | Not greater than half of the join timer setting |
| Join | Not less than two times the hold timer setting | Less than half of the leave timer setting |
| Leave | Greater than two times the join timer setting | Less than the leaveall timer setting |
| Leaveall | Greater than the leave timer setting | 32765 centiseconds |

Related commands: **display garp timer.**

Examples # Set the GARP join timer to 25 centiseconds, assuming that both the hold timer and the leave timer are using the default.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] garp timer join 25
```

garp timer leaveall

Syntax **garp timer leaveall** *timer-value*

undo garp timer leaveall

View System view

Parameters *timer-value*: Leaveall timer setting, in the range 65 to 32765 (in centiseconds), Note that the setting of the leaveall timer must be a multiple of 5 centiseconds and must be greater than the leave timer settings of all the ports.

Description Use the **garp timer leaveall** command to set the leaveall timer of GARP.

Use the **undo garp timer leaveall** command to restore the default. This may fail if the default is less than the setting of the current leave timer.

By default, the setting of the leaveall timer is 1000 centiseconds (that is, 10 seconds).

A leaveall timer starts upon the start of a GARP application entity. When this timer expires, the entity sends a LeaveAll message so that other entities can re-register its attribute information and starts another leaveall timer at the same time.

Each time a device on the network receives a LeaveAll message, it resets its leaveall timer. Therefore, a GARP application entity may send LeaveAll messages at the interval set by its leaveall timer or the leaveall timer on another device on the network, whichever is smaller.

Related commands: **display garp timer.**

Examples # Set the leaveall timer to 100 centiseconds, assuming that the leave timer is 60 centiseconds.

```
<Sysname> system-view
[Sysname] garp timer leaveall 100
```

reset garp statistics

Syntax **reset garp statistics** [**interface** *interface-list*]

View User view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> means that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **reset garp statistics** command to clear GARP statistics of specific or all the ports.

Note that:

- If the **interface** *interface-list* keyword-argument combination is not specified, this command clears the GARP statistics of all the ports.
- If the **interface** *interface-list* keyword-argument combination is specified, this command clears the GARP statistics of the specified ports.

Related commands: **display gvrp statistics.**

Examples # Clear statistics about GARP on all ports.

```
<Sysname> reset garp statistics
```

17

GVRP CONFIGURATION COMMANDS

display gvrp local-vlan interface

Syntax `display gvrp local-vlan interface interface-type interface-number`

View Any view

Parameters `interface-type interface-number`: Specifies an interface by its type and number.

Description Use the **display gvrp local-vlan interface** command to display the local VLAN information maintained by GVRP on a port.

Examples # Display the local VLAN information maintained by GVRP on Ethernet 2/0/1.

```
<Sysname> display gvrp local-vlan interface ethernet 2/0/1
Following VLANs exist in GVRP local database:
 1(default),2-500
```

```
// The information above shows that GVRP maintains the information about VLAN
1, VLAN 2 through VLAN 500, which Ethernet 2/0/1 belongs to.
```

display gvrp state

Syntax `display gvrp state interface interface-type interface-number vlan vlan-id`

View Any view

Parameters `interface interface-type interface-number`: Specifies an interface by its type and number.

`vlan vlan-id`: Specifies a VLAN ID, in the range 1 to 4094.

Description Use the **display gvrp state** command to display the current GVRP state.

Examples # Display the GVRP state of VLAN 1, which Ethernet 2/0/1 belongs to.

```
<Sysname> display gvrp state interface ethernet 2/0/1 vlan 1
GVRP state of VLAN 1 on port Ethernet2/0/1
```

```
Applicant state machine      : VP
Registrar state machine     : MTR
```

display gvrp statistics

Syntax `display gvrp statistics [interface interface-list]`

View Any view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> means that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **display gvrp statistics** command to display the GVRP statistics of specified or all trunk ports.

Note that if the **interface** *interface-list* is not provided, the GVRP statistics of all trunk ports will be displayed. Otherwise, only the GVRP statistics of all the specified trunk port will be displayed.

Examples # Display statistics about GVRP for trunk port Ethernet 2/0/1.

```
<Sysname> display gvrp statistics interface ethernet 2/0/1
```

```
GVRP statistics on port Ethernet2/0/1
```

```
GVRP Status           : Enabled
GVRP Running          : YES
GVRP Failed Registrations : 0
GVRP Last Pdu Origin   : 0000-0000-0000
GVRP Registration Type : Normal
```

Table 37 Field descriptions of the display gvrp statistics command

| Field | Description |
|---------------------------|--|
| GVRP Status | Indicates whether GVRP is enabled or disabled. |
| GVRP Running | Indicates whether GVRP is running. |
| GVRP Failed Registrations | Indicates the number of GVRP registration failures. |
| GVRP Last Pdu Origin | Indicates the source MAC address in the last GVRP PDU. |
| GVRP Registration Type | Indicates the GVRP registration type on the port. |

display gvrp status

Syntax `display gvrp status`

View Any view

Parameters None

Description Use the **display gvrp status** command to display the global enable/disable state of GVRP.

Examples # Display the global GVRP enable/disable state.

```
<Sysname> display gvrp status
```

```
GVRP is enabled
```

display gvrp vlan-operation interface

Syntax **display gvrp vlan-operation interface** *interface-type interface-number*

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display gvrp vlan-operation interface** command to display the information about dynamic VLAN operations performed on a port.

Examples # Display the information about dynamic VLAN operations performed on Ethernet 2/0/1.

```
<Sysname> display gvrp vlan-operation interface ethernet 2/0/1
Dynamic VLAN operations on port Ethernet2/0/1
Operations of creating VLAN           : 2-100
Operations of deleting VLAN          : none
Operations of adding VLAN to TRUNK    : 2-100
Operations of deleting VLAN from TRUNK : none
```

gvrp

Syntax **gvrp**
undo gvrp

View System view, Ethernet port view, port group view

Parameters None

Description Use the **gvrp** command to enable GVRP globally, on a port, or on all ports in a port group depending on the view you entered.

Use the **undo gvrp** command to disable GVRP globally, on a port, or on all ports in a port group depending on the view you entered.

By default, GVRP is disabled.

Execution of the above commands in system view, will apply the configurations globally, in Ethernet port view will apply the configurations to the current port, and in port group view will apply the configurations to all the ports in the port group.



- To enable GVRP on a port, you need to enable it globally.
- The port where you enable/disable GVRP must be a trunk port.
- BPDU Tunnel is incompatible with GVRP. Before enabling GVRP, disable BPDU Tunnel.
- Isolate-user-vlan is incompatible with global GVRP. Make sure that no Isolate-user-vlan has been created on the device before enabling GVRP.

Related commands: **display gvrp status.**

Examples # Enable GVRP globally.

```
<Sysname> system-view
[Sysname] gvrp
GVRP is enabled globally.
```

gvrp registration

Syntax **gvrp registration { fixed | forbidden | normal }**

undo gvrp registration

View Ethernet port view, port group view

Parameters **fixed**: Sets the registration type to **fixed**.
forbidden: Sets the registration type to **forbidden**.
normal: Sets the registration type to **normal**.

Description Use the **gvrp registration** command to configure the GVRP registration type on a port or all ports in a port group.

Use the **undo gvrp registration** command to restore the default.

The default GVRP registration type is **normal**.

Execution of the above commands in Ethernet port view will apply the configurations to the current port only whereas under port group view will apply the configurations to all the ports in the port group.

GVRP provides the following three registration types on a port:

- **Normal**. Port operating in this mode can dynamically register/deregister VLANs, and to propagate both dynamic and static VLAN information.
- **Fixed**. Port operating in this mode cannot dynamically register/deregister VLANs or propagate information about dynamic VLANs. However, they can propagate information about static VLANs. A trunk port of this type allows only manually configured VLANs to pass through even though it is configured to carry all VLANs.

- **Forbidden.** Port operating in this mode cannot dynamically register/deregister VLANs or propagate VLAN information except information about VLAN 1. A trunk port of this type allows only VLAN 1 to pass through even though it is configured to carry all VLANs.

Note that this command is only available to trunk ports.

Related commands: **display garp statistics.**

Examples # Set the GVRP registration type to **fixed** on port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type trunk
[Sysname-Ethernet2/0/1] gvrp registration fixed
```


18

IP ADDRESSING CONFIGURATION COMMANDS

display ip interface

Syntax `display ip interface [interface-type interface-number]`

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display ip interface** command to display information about a specified or all Layer 3 interfaces.

Examples # Display information about interface VLAN-interface 1.

```
<Sysname> display ip interface vlan-interface 1
Vlan-interface1 current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
ip fast-forwarding incoming packets state is Disable
ip fast-forwarding outgoing packets state is Disable
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
ARP packet input number:          0
  Request packet:                 0
  Reply packet:                   0
  Unknown packet:                 0
TTL invalid packet number:       0
ICMP packet input number:        0
  Echo reply:                     0
  Unreachable:                   0
  Source quench:                 0
  Routing redirect:              0
  Echo request:                  0
  Router advert:                 0
  Router solicit:                0
  Time exceed:                   0
  IP header bad:                 0
  Timestamp request:             0
  Timestamp reply:               0
  Information request:           0
  Information reply:             0
  Netmask request:               0
  Netmask reply:                 0
```

```
Unknown type: 0
DHCP packet deal mode: global
```

Table 38 Description on fields of the display ip interface command

| Field | Description |
|--|---|
| current state | Current physical state of an interface |
| Line protocol current state | Current state of the network layer protocol |
| Internet Address | IP address of an interface followed by: <ul style="list-style-type: none"> ■ Primary: Identifies a primary IP address, or ■ Sub: Identifies a secondary IP address. |
| Broadcast address | Broadcast address of the subnet attached to an interface |
| The Maximum Transmit Unit | Maximum transmission units on an interface |
| input packets: 0, bytes: 0, multicasts: 0 | Unicast packets, bytes, and multicast packets received on an interface |
| output packets: 0, bytes: 0, multicasts: 0 | Unicast packets, bytes, and multicast packets sent on an interface |
| ARP packet input number: 0 | Total number of ARP packets received on an interface, including |
| Request packet: 0 | <ul style="list-style-type: none"> ■ ARP request packets |
| Reply packet: 0 | <ul style="list-style-type: none"> ■ ARP reply packets |
| Unknown packet: 0 | <ul style="list-style-type: none"> ■ Unknown packets |
| TTL invalid packet number | Number of TTL-invalid packets received on an interface |
| ICMP packet input number: 0 | Total number of ICMP packets received on an interface, including the following packets: |
| Echo reply: 0 | <ul style="list-style-type: none"> ■ Echo reply packet |
| Unreachable: 0 | <ul style="list-style-type: none"> ■ Unreachable packets |
| Source quench: 0 | <ul style="list-style-type: none"> ■ Source quench packets |
| Routing redirect: 0 | <ul style="list-style-type: none"> ■ Routing redirect packets |
| Echo request: 0 | <ul style="list-style-type: none"> ■ Echo request packets |
| Router advert: 0 | <ul style="list-style-type: none"> ■ Router advertisement packets |
| Router solicit: 0 | <ul style="list-style-type: none"> ■ Router solicitation packets |
| Time exceed: 0 | <ul style="list-style-type: none"> ■ Time exceeded packets |
| IP header bad: 0 | <ul style="list-style-type: none"> ■ IP header bad packets |
| Timestamp request: 0 | <ul style="list-style-type: none"> ■ Timestamp request packets |
| Timestamp reply: 0 | <ul style="list-style-type: none"> ■ Timestamp reply packets |
| Information request: 0 | <ul style="list-style-type: none"> ■ Information request packets |
| Information reply: 0 | <ul style="list-style-type: none"> ■ Information reply packets |
| Netmask request: 0 | <ul style="list-style-type: none"> ■ Netmask request packets |
| Netmask reply: 0 | <ul style="list-style-type: none"> ■ Netmask reply packets |
| Unknown type: 0 | <ul style="list-style-type: none"> ■ Unknown type packets |
| DHCP packet deal mode | DHCP packet processing mode. This field appears on a DHCP-supporting device and can be one of the following values: <ul style="list-style-type: none"> ■ global: The DHCP server with the global address pool is enabled on the interface. ■ relay: The DHCP relay agent is enabled on the interface. |

display ip interface brief

Syntax **display ip interface brief** [interface-type [interface-number]]

View Any view

Parameters *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display ip interface brief** command to display brief information about a specified or all layer 3 interfaces.

Without the interface type and interface number specified, the information about all layer 3 interfaces is displayed; with only the interface type specified, the information about all layer 3 interfaces of the specified type is displayed; with both the interface type and interface number specified, only the information about the specified interface is displayed.

Related commands: **display ip interface.**

Examples # Display brief information about VLAN-interface 1.

```
<Sysname> display ip interface brief vlan-interface 1
*down: administratively down
(s): spoofing
Interface          Physical          Protocol          IP Address
Vlan-interface1   up                up                1.1.1.1
```

Table 39 Description on fields of the display ip interface brief command

| Field | Description |
|------------|---|
| *down | The interface is administratively shut down with the shutdown command. |
| (s) | Spoofing attribute of the interface. It indicates that an interface whose network layer protocol is displayed up may have no link present or the link is set up only on demand. |
| Interface | Interface name |
| Physical | Physical state of interface |
| Protocol | Network layer protocol state of interface |
| IP Address | IP address of interface (If no IP address is configured, "unassigned" is displayed.) |

ip address

Syntax **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View Interface view

Parameters *ip-address*: IP address of interface, in dotted decimal notation.

mask: Subnet mask in dotted decimal notation.

mask-length: Subnet mask length, the number of consecutive ones in the mask.

sub: Secondary IP address for the interface.

Description Use the **ip address** command to assign an IP address and mask to the interface.

Use the **undo ip address** command to remove all IP addresses.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to remove the primary IP address.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command to remove a secondary IP address.

By default, no IP address is assigned to any interface.

When assigning IP addresses to an interface, consider the following:

- You can assign only one primary IP address to an interface.
- The primary and secondary IP addresses can be located in the same network segment.
- Before removing the primary IP address, remove all secondary IP addresses.
- You can assign a secondary IP address only when the interface is not configured to obtain one through DHCP.

Related commands: **display ip interface.**

Examples # Assign VLAN-interface 1 a primary IP address and a secondary IP address, with subnet masks being 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
[Sysname-Vlan-interface1] ip address 202.38.160.1 255.255.255.0 sub
```

19

IP PERFORMANCE CONFIGURATION COMMANDS

display fib

Syntax `display fib [| { begin | include | exclude } string | acl acl-number | ip-prefix ip-prefix-name]`

View Any view

Parameters | { **begin** | **include** | **exclude** } *string*: Displays FIB information in the buffer related to the specified string according to a regular expression.

- The **begin** keyword specifies to display from the first FIB entry that contains the specified string.
- The **include** keyword specifies to display only the FIB entries that include the specified string.
- The **exclude** keyword specifies to display only the FIB entries that do not include the specified string.
- The *string* argument is a case-sensitive string, containing 1 to 256 characters.

acl *acl-number*: Displays FIB information matching a specified ACL numbered from 2000 to 2999.

ip-prefix *ip-prefix-name*: Displays FIB information matching a specified IP prefix list, a string of 1 to 19 characters.

Description Use the **display fib** command to display FIB forward information. If no parameters are specified, all FIB information will be displayed.

Examples # Display all FIB information.

```
<Sysname> display fib
FIB Table:
Total number of Routes : 4
Flag:
  U:Useable   G:Gateway   H:Host     B:Blackhole  D:Dynamic   S:Static
  R:Reject    L:Generated by ARP or ISIS

Destination/Mask  Nexthop      Flag      TimeStamp      Interface      Token
10.2.0.0/16       0.0.0.0      U         t[1150900568]  Vlan1         invalid
10.2.1.1/32       127.0.0.1    HU        t[1150900568]  InLoop0       invalid
127.0.0.0/8       127.0.0.1    U         t[1150623094]  InLoop0       invalid
127.0.0.1/32     127.0.0.1    HU        t[1150623094]  InLoop0       invalid
```

Table 40 Field descriptions of the display fib command

| Field | Description |
|------------------------|---|
| Total number of Routes | Total number of routes in the FIB table |
| Destination/Mask | Destination address/length of mask |
| Nexthop | Address of next hop |
| Flag | Flags of routes: <ul style="list-style-type: none"> ■ U"-Usable route ■ G"-Gateway route ■ H"-Host route ■ B"-Blackhole route ■ D"-Dynamic route ■ S"-Static route ■ R"-Refused route ■ L"-Route generated by ARP or ESIS |
| TimeStamp | Time stamp |
| Interface | Forward interface |
| Token | LSP index number |

Display FIB information passing ACL 2000

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] display fib acl 2000
Route entry matched by access-list 2000:
Summary counts: 2

Flag:
  U:Useable   G:Gateway   H:Host     B:Blackhole   D:Dynamic   S:Static
  R:Reject    L:Generated by ARP or ESIS

Destination/Mask  Nexthop    Flag      TimeStamp    Interface    Token
10.2.0.0/16      0.0.0.0    U         t[1150900568] Vlan1       invalid
10.2.1.1/32      127.0.0.1  HU        t[1150900568] InLoop0     invalid
```

Display all entries that contain the string 127 and start from the first one.

```
<Sysname> display fib | begin 127
Flag:
  U:Useable   G:Gateway   H:Host     B:Blackhole   D:Dynamic   S:Static
  R:Reject    L:Generated by ARP or ESIS

Destination/Mask  Nexthop    Flag      TimeStamp    Interface    Token
10.2.1.1/32      127.0.0.1  HU        t[1150900568] InLoop0     invalid
127.0.0.0/8      127.0.0.1  U         t[1150623094] InLoop0     invalid
127.0.0.1/32     127.0.0.1  HU        t[1150623094] InLoop0     invalid
```

Display FIB information passing the IP prefix list abc0

```
<Sysname> system-view
[Sysname] ip ip-prefix abc0 permit 10.2.0.0 16
[Sysname] display fib ip-prefix abc0
Route Entry matched by prefix-list abc0:
Summary count: 1

Flag:
```



```

U:Useable  G:Gateway  H:Host  B:Blackhole  D:Dynamic  S:Static
R:Reject   L:Generated by ARP or ESIS

Destination/Mask  Nexthop  Flag  TimeStamp  Interface  Token
10.2.0.0/16      0.0.0.0  U     t[1150900568]  Vlan1     invalid

```

display fib ip-address

Syntax **display fib** *ip-address1* [{ *mask1* | *mask-length1* } [*ip-address2* { *mask2* | *mask-length2* }] **longer**] | **longer**]

View Any view

Parameters *ip-address1*, *ip-address2*: Destination IP address, in dotted decimal notation. *ip-address1* and *ip-address2* together determine an address range for the FIB entries to be displayed.

mask1, *mask2*: IP address mask.

mask-length1, *mask-length2*: Length of IP address mask.

longer: Displays FIB entries that match the specified address/mask and have masks longer than or equal to the mask that a user enters. If no masks are specified, FIB entries that match the natural network address and have the masks longer than or equal to the natural mask will be displayed.

Description Use the **display fib** *ip-address* command to display FIB entries that match the specified destination IP address.

Examples # Display the FIB entries that match the natural network of 10.1.0.0 and have the masks longer than or equal to the natural mask.

```

<Sysname> display fib 10.1.0.0 longer
Route Entry Count: 2

Flag:
U:Useable  G:Gateway  H:Host  B:Blackhole  D:Dynamic  S:Static
R:Reject   L:Generated by ARP or ESIS

Destination/Mask  Nexthop  Flag  TimeStamp  Interface  Token
10.0.0.0/8        0.0.0.0  U     t[1141140133]  Vlan1     invalid
10.1.1.1/32       127.0.0.1  HU    t[1141140133]  InLoop0   invalid

```

For description about the above output, refer to Table 40.

display fib statistics

Syntax display fib statistics

View Any view

Parameters None

Description Use the **display fib statistics** command to display statistics about the FIB entries.

Examples # View statistics about the FIB entries.

```
<Sysname> display fib statistics
Route Entry Count          : 2
```

Table 41 Field descriptions of the display fib statistics command

| Field | Description |
|-------------------|-----------------------|
| Route Entry Count | Number of FIB entries |

display icmp statistics

Syntax **display icmp statistics** [**slot** *slot-number*]

View Any view

Parameters **slot** *slot-number*: Displays the ICMP statistics on a slot.

Description Use the **display icmp statistics** command to display ICMP statistics.

Related commands: **display ip interface**, **reset ip statistics**.

Examples # Display ICMP statistics.

```
<Sysname> display icmp statistics
Input: bad formats    0          bad checksum          0
      echo            5          destination unreachable 0
      source quench   0          redirects              0
      echo reply      10         parameter problem      0
      timestamp       0          information request     0
      mask requests   0          mask replies           0
      time exceeded   0
Output: echo          10         destination unreachable 0
      source quench   0          redirects              0
      echo reply      5          parameter problem      0
      timestamp       0          information reply       0
      mask requests   0          mask replies           0
      time exceeded   0
```

Table 42 Field descriptions of the display icmp statistics command

| Field | Description |
|-------------------------|--|
| bad formats | Number of input wrong format packets |
| bad checksum | Number of input wrong checksum packets |
| echo | Number of input/output echo packets |
| destination unreachable | Number of input/output destination unreachable packets |
| source quench | Number of input/output source quench packets |
| redirects | Number of input/output redirection packets |
| echo reply | Number of input/output replies |

Table 42 Field descriptions of the display icmp statistics command

| Field | Description |
|---------------------|--|
| parameter problem | Number of input/output parameter problem packets |
| timestamp | Number of input/output time stamp packets |
| information request | Number of input information request packets |
| mask requests | Number of input/output mask requests |
| mask replies | Number of input/output mask replies |
| information reply | Number of output information reply packets |
| time exceeded | Number of input/output expiration packets |

display ip socket

Syntax **display ip socket** [**socktype** *sock-type*] [*task-id* *socket-id*] [**slot** *slot-number*]

View Any view

Parameters **socktype** *sock-type*: Displays the socket information of this type. The sock type is in the range 1 to 3, corresponding to TCP, UDP and raw IP respectively.

task-id: Displays the socket information of this task. Task ID is in the range 1 to 100.

socket-id: Displays the information of the socket. Socket ID is in the range 0 to 3072.

slot-number: Displays the socket information of the slot.

Description Use the **display ip socket** command to display socket information.

Examples # Display all socket information.

```
<Sysname> display ip socket
SOCK_STREAM:
Task = VTYP(60), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPAALIVE SO_REUSEPORT SO_SENDDVNPID(3073) SO_SETKEEPAALIVE,
socket state = SS_PRIV SS_ASYNC

Task = HTTP(58), socketid = 1, Proto = 6,
LA = 0.0.0.0:80, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO

Task = VTYP(60), socketid = 3, Proto = 6,
LA = 192.168.0.152:23, FA = 192.168.0.208:1099,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 483, rb_cc = 0,
socket option = SO_KEEPAALIVE SO_OOBINLINE SO_REUSEPORT SO_SENDDVNPID(0) SO_SETKEEPAALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = AGNT(29), socketid = 1, Proto = 17,
LA = 0.0.0.0:161, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHKSUM SO_SENDDVNPID(3073),
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = ROUT(86), socketid = 3, Proto = 17,
LA = 0.0.0.0:520, FA = 0.0.0.0:0,
sndbuf = 1024, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
```

```

socket option = SO_BROADCAST SO_REUSEPORT SO_UDPChecksum SO_SETSRCADDR SO_SENDSVNPID(0),
socket state = SS_PRIV SS_ASYNC

Task = RDSO(75), socketid = 1, Proto = 17,
LA = 0.0.0.0:1024, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPChecksum,
socket state = SS_PRIV

Task = TRAP(71), socketid = 1, Proto = 17,
LA = 0.0.0.0:1025, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 0, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPChecksum,
socket state = SS_PRIV

Task = RDSO(75), socketid = 2, Proto = 17,
LA = 0.0.0.0:1812, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPChecksum,
socket state = SS_PRIV

SOCK_RAW:
Task = ROUT(86), socketid = 2, Proto = 65,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = ROUT(86), socketid = 1, Proto = 2,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = SO_SENDSVNPID(0) SO_RECVVNPID(0),
socket state = SS_PRIV SS_NBIO SS_ASYNC

```

Table 43 Field descriptions of the display ip socket command

| Field | Description |
|---------------|---|
| SOCK_STREAM | TCP socket |
| SOCK_DGRAM | UDP socket |
| SOCK_RAW | raw IP socket |
| Task | Task number |
| socketid | Socket ID |
| Proto | Protocol number of the socket |
| LA | Local address and local port number |
| FA | Remote address and remote port number |
| sndbuf | sending buffer size of the socket |
| rcvbuf | receiving buffer size of the socket |
| sb_cc | Current data size in the sending buffer (It is available only for TCP that can buffer data) |
| rb_cc | Data size currently in the receiving buffer |
| socket option | Socket option |
| socket state | Socket state |

display ip statistics

Syntax `display ip statistics [slot slot-number]`

View Any view

Parameters `slot slot-number`: Displays statistics of IP packets on the slot.

Description Use the **display ip statistics** command to display statistics of IP packets.

Related commands: `display ip interface`, `reset ip statistics`.

Examples # Display statistics of IP packets.

```
<Sysname> display ip statistics
  Input:  sum          92306          local          89167
         bad protocol  0           bad format     0
         bad checksum  0           bad options    0
  Output: forwarding  415         local          80746
         dropped       0           no route       0
         compress fails 0
  Fragment: input     0           output         0
         dropped       0
         fragmented    0           couldn't fragment 0
  Reassembling: sum   0           timeouts       0
```

Table 44 Field descriptions of the `display ip statistics` command

| Field | | Description |
|--------------|-------------------|---|
| Input: | sum | Total number of packets received |
| | local | Total number of packets with destination being local |
| | bad protocol | Total number of unknown protocol packets |
| | bad format | Total number of packets with incorrect format |
| | bad checksum | Total number of packets with incorrect checksum |
| Output: | bad options | Total number of packets with incorrect option |
| | forwarding | Total number of packets forwarded |
| | local | Total number of packets sent from the local |
| | dropped | Total number of packets discarded |
| | no route | Total number of packets for which no route is available |
| Fragment: | compress fails | Total number of packets failed to compress |
| | input | Total number of fragments received |
| | output | Total number of fragments sent |
| | dropped | Total number of fragments dropped |
| | fragmented | Total number of packets successfully fragmented |
| Reassembling | couldn't fragment | Total number of packets that failed to be fragmented |
| | sum | Total number of packets reassembled |
| | timeouts | Total number of reassembly timeout fragments |

display tcp statistics

Syntax `display tcp statistics`

View Any view

Parameters None

Description Use the `display tcp statistics` command to display statistics of TCP traffic.

Related commands: `display tcp status`, `reset tcp statistics`.

Examples # Display statistics of TCP traffic.

```
<Sysname> display tcp statistics
Received packets:
Total: 753
packets in sequence: 412 (11032 bytes)
window probe packets: 0, window update packets: 0
checksum error: 0, offset error: 0, short error: 0

duplicate packets: 4 (88 bytes), partially duplicate packets: 5 (7 bytes)
out-of-order packets: 0 (0 bytes)
packets of data after window: 0 (0 bytes)
packets received after close: 0

ACK packets: 481 (8776 bytes)
duplicate ACK packets: 7, too much ACK packets: 0

Sent packets:
Total: 665
urgent packets: 0
control packets: 5 (including 1 RST)
window probe packets: 0, window update packets: 2

data packets: 618 (8770 bytes) data packets retransmitted: 0 (0 bytes)
ACK-only packets: 40 (28 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections
disconnected : 0
Initiated connections: 0, accepted connections: 0, established connections:0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Table 45 Field descriptions of the `display tcp statistics` command

| Field | Description |
|-------------------|---|
| Received packets: | Total |
| | Total number of packets received |
| | packets in sequence |
| | Number of packets arriving in sequence |
| | window probe packets |
| | Number of window probe packets received |
| | window update packets |
| | Number of window update packets received |
| | checksum error |
| | Number of checksum error packets received |
| | offset error |
| | Number of offset error packets received |
| | short error |
| | Number of received packets with length being too small |
| | duplicate packets |
| | Number of completely duplicate packets received |
| | partially duplicate packets |
| | Number of partially duplicate packets received |
| | out-of-order packets |
| | Number of out-of-order packets received |
| | packets of data after window |
| | Number of packets outside the receiving window |
| | packets received after close |
| | Number of packets that arrived after connection is closed |
| | ACK packets |
| | Number of ACK packets received |
| | duplicate ACK packets |
| | Number of duplicate ACK packets received |
| | too much ACK packets |
| | Number of ACK packets for data unsend |

Table 45 Field descriptions of the display tcp statistics command

| Field | Description |
|--|--|
| Sent packets: Total | Total number of packets sent |
| urgent packets | Number of urgent packets sent |
| control packets | Number of control packets sent |
| window probe packets | Number of window probe packets sent; in the brackets are resent packets |
| window update packets | Number of window update packets sent |
| data packets | Number of data packets sent |
| data packets retransmitted | Number of data packets retransmitted |
| ACK-only packets | Number of ACK packets sent; in brackets are delayed ACK packets |
| Retransmitted timeout | Number of retransmission timer timeouts |
| connections dropped in retransmitted timeout | Number of connections broken due to retransmission timeouts |
| Keepalive timeout | Number of keepalive timer timeouts |
| keepalive probe | Number of keepalive probe packets sent |
| Keepalive timeout, so connections disconnected | Number of connections broken due to keepalive timer timeouts |
| Initiated connections | Number of connections initiated |
| accepted connections | Number of connections accepted |
| established connections | Number of connections established |
| Closed connections | Number of connections closed; in brackets are connections closed accidentally (before receiving SYN from the peer) and connections closed initiatively (after receiving SYN from the peer) |
| Packets dropped with MD5 authentication | Number of packets dropped with MD5 authentication |
| Packets permitted with MD5 authentication | Number of packets permitted with MD5 authentication |

display tcp status

Syntax `display tcp status`

View Any view

Parameters None

Description Use the **display tcp status** command to display status of all TCP connection for monitoring TCP connections.

Examples # Display status of all TCP connections

```
<Sysname> display tcp status
*: TCP MD5 Connection
TCPCB          Local Add:port    Foreign Add:port   State
03e37dc4       0.0.0.0:4001      0.0.0.0:0          Listening
04217174       100.0.0.204:23    100.0.0.253:65508  Established
```

Table 46 Field descriptions of the display tcp status command

| Field | Description |
|------------------|--|
| * | If the status information of a TCP connection contains *, the TCP adopts the MD5 algorithm for authentication. |
| TCPCB | TCP control block |
| Local Add:port | Local IP address and port number |
| Foreign Add:port | Remote IP address and port number |
| State | State of the TCP connection |

display udp statistics

Syntax `display udp statistics`

View Any view

Parameters None

Description Use the display udp statistics command to display statistics of UDP packets.

Related commands: `reset udp statistics`.

Examples # Display statistics of UDP packets.

```
<Sysname> display udp statistics
Received packets:
  Total: 0
  checksum error: 0
  shorter than header: 0, data length larger than packet: 0
  unicast(no socket on port): 0
  broadcast/multicast(no socket on port): 0
  not delivered, input socket full: 0
  input packets missing pcb cache: 0
Sent packets:
  Total: 0
```


Table 47 Field descriptions of the display udp statistics command

| Field | | Description |
|-------------------|--|--|
| Received packets: | Total | Total number of UDP packets received |
| | checksum error | Total number of packets with incorrect checksum |
| | shorter than header | Number of packets with data shorter than head |
| | data length larger than packet | Number of packets with data longer than packet |
| | unicast(no socket on port) | Number of unicast packets with no socket on port |
| | broadcast/multicast(no socket on port) | Number of broadcast/multicast packets without socket on port |
| | not delivered, input socket full | Number of packets not delivered to upper layer due to socket buffer being full |
| | input packets missing pcb cache | Number of packets without matching PCB cache |
| Sent packets: | Total | Total number of UDP packets sent |

ip forward-broadcast

Syntax `ip forward-broadcast [acl acl-number]`

`undo ip forward-broadcast`

View Interface view

Parameters `acl acl-number`: Number of an ACL from 2000 to 3999. From 2000 to 2999 are numbers for basic ACLs, and from 3000 to 3999 are numbers for advanced ACLs. Only directed broadcasts permitted by the ACL can be forwarded.

Description Use the **ip forward-broadcast** command to enable the interface to forward directed broadcasts.

Use the **undo ip forward-broadcast** command to disable an interface from forwarding directed broadcasts.

By default, an interface is disabled from forwarding directed broadcasts.

Examples # Allow VLAN-interface 2 to forward directed broadcasts permitted by ACL 2001.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast acl 2001
```

ip forward-broadcast

| | |
|--------------------|--|
| Syntax | ip forward-broadcast
undo ip forward-broadcast |
| View | System view |
| Parameters | None |
| Description | <p>Use the ip forward-broadcast command to enable the device to receive directed broadcasts.</p> <p>Use the undo ip forward-broadcast command to disable the device from receiving directed broadcasts.</p> <p>By default, the feature is disabled from receiving directed broadcasts.</p> |
| Examples | <pre># Enable the device to receive directed broadcasts. <Sysname> system-view [Sysname] ip forward-broadcast</pre> |

ip redirects enable

| | |
|--------------------|---|
| Syntax | ip redirects enable
undo ip redirects |
| View | System view |
| Parameters | None |
| Description | <p>Use the ip redirects enable command to enable sending ICMP redirection packets.</p> <p>Use the undo ip redirects command to disable sending ICMP redirection packets.</p> <p>This feature is enabled by default.</p> |
| Examples | <pre># Disable sending ICMP redirection packets. <Sysname> system-view [Sysname] undo ip redirects The function is disabled!</pre> |

ip ttl-expires enable

Syntax **ip ttl-expires enable**

undo ip ttl-expires

View System view

Parameters None

Description Use the **ip ttl-expires enable** command to enable the sending of ICMP timeout packets.

Use the **undo ip ttl-expires** command to disable sending ICMP timeout packets.

Sending ICMP timeout packets is enabled by default.

If the feature is disabled, the device will not send TTL timeout ICMP packets, but still send "reassembly timeout" ICMP packets.

Examples # Disable sending ICMP timeout packets.

```
<Sysname> system-view
[Sysname] undo ip ttl-expires
The function is disabled!
```

ip unreachable enable

Syntax **ip unreachable enable**

undo ip unreachable

View System view

Parameters None

Description Use the **ip unreachable enable** command to enable the sending of ICMP destination unreachable packets.

Use the **undo ip unreachable** command to disable sending ICMP destination unreachable packets.

Sending ICMP destination unreachable packets is enabled by default.

If the feature is disabled, the device will not send network unreachable and source route failure ICMP packets, but still send other destination unreachable ICMP packets.

Examples # Disable sending ICMP destination unreachable packets.

```

<Sysname> system-view
[Sysname] undo ip unreachable
The function is disabled!

```

reset ip statistics

Syntax `reset ip statistics [slot slot-number]`

View User view

Parameters `slot slot-number`: Clears IP packet statistics on the specified slot.

Description Use the **reset ip statistics** command to clear statistics of IP packets.

Related commands: **display ip interface, display ip statistics.**

Examples # Clear statistics of IP packets.
`<Sysname> reset ip statistics`

reset tcp statistics

Syntax `reset tcp statistics`

View User view

Parameters None

Description Use the **reset tcp statistics** command to clear statistics of TCP traffic.

Related commands: **display tcp statistics.**

Examples # Display statistics of TCP traffic.
`<Sysname> reset tcp statistics`

reset udp statistics

Syntax `reset udp statistics`

View User view

Parameters None

Description Use the **reset udp statistics** command to clear statistics of UDP traffic.

Examples # Display statistics of UDP traffic.
 <Sysname> reset udp statistics

tcp timer fin-timeout

Syntax **tcp timer fin-timeout** *time-value*
undo tcp timer fin-timeout

View System view

Parameters *time-value*: Length of the TCP finwait timer in seconds, ranging from 76 to 3,600.

Description Use the **tcp timer fin-timeout** command to configure the length of the TCP finwait timer.

Use the **undo tcp timer fin-timeout** command to restore the default.

By default, the length of the TCP finwait timer is 675 seconds.

Note that the actual length of the finwait timer is determined by the following formula:

Actual length of the finwait timer = (Configured length of the finwait timer - 75) + configured length of the synwait timer

Related commands: **tcp timer syn-timeout**, **tcp window**.

Examples # Set the length of the TCP finwait timer to 800 seconds.
 <Sysname> system-view
 [Sysname] tcp timer fin-timeout 800

tcp timer syn-timeout

Syntax **tcp timer syn-timeout** *time-value*
undo tcp timer syn-timeout

View System view

Parameters *time-value*: Length of the TCP synwait timer in seconds, ranging from 2 to 600.

Description Use the **tcp timer syn-timeout** command to configure the length of the TCP synwait timer.

Use the **undo tcp timer syn-timeout** command to restore the default.

By default, the length of the TCP synwait timer is 75 seconds.

Related commands: **tcp timer fin-timeout**, **tcp window**.

Examples # Set the length of the TCP synwait timer to 80 seconds.

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

tcp window

Syntax **tcp window** *window-size*

undo tcp window

View System view

Parameters *window-size*: Receiving/sending buffer size of TCP connection in KB, ranging from 1 to 32.

Description Use the **tcp window** command to configure the receiving/sending buffer size of TCP connection.

Use the **undo tcp window** command to restore the default.

The TCP receiving/sending buffer is 8 KB by default.

Related commands: **tcp timer fin-timeout**, **tcp timer syn-timeout**.

Examples # Configure the receiving/sending buffer of TCP connection as 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

20

IP SOURCE GUARD COMMANDS

display ip check source

Syntax **display ip check source** [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*]

View Any view

Parameters **interface** *interface-type interface-number*: Displays the dynamic bindings of the port specified by its type and number.

ip-address *ip-address*: Displays the dynamic bindings of an IP address.

mac-address *mac-address*: Displays the dynamic bindings of a MAC address (in the format of H-H-H).

Description Use the **display ip check source** command to display dynamic bindings.

With no options specified, the command displays the dynamic bindings of all ports.

Related commands: **ip check source**.

Examples # Display all dynamic bindings.

```
<Sysname> display ip check source
The following user address bindings have been configured:
MAC                IP                Vlan  Port                Status
0001-0203-0406    192.168.0.1      2     Ethernet2/0/1      DHCP-SNP
0001-0203-0407    192.168.0.2      2     Ethernet2/0/2      DHCP-SNP
-----2 binding entries queried, 2 listed-----
```

Table 48 Field descriptions of the display ip check source command

| Field | Description |
|--------|--|
| MAC | MAC address of the dynamic binding. N/A means that no MAC address is bound in the entry. |
| IP | IP address of the dynamic binding. N/A means that no IP address is bound in the entry. |
| Vlan | VLAN to which the obtained binding entry belongs. N/A means that no VLAN is bound in the entry. |
| Port | Port to which the dynamic binding entry is applied |
| Status | Type of dynamically obtaining the binding entry. DHCP-SNP means that the binding is dynamically obtained from DHCP snooping. |

Table 48 Field descriptions of the display ip check source command

| Field | Description |
|-------------------------------------|-----------------------------------|
| 2 binding entries queried, 2 listed | Counts of dynamic binding entries |

display user-bind

Syntax **display user-bind** [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*]

View Any view

Parameters **interface** *interface-type interface-number*: Displays the static bindings of the interface specified by its type and number.

ip-address *ip-address*: Displays the static bindings of an IP address.

mac-address *mac-address*: Displays the static bindings of a MAC address (in the format of H-H-H).

Description Use the **display user-bind** command to display static bindings.

With no options specified, the command displays static bindings of all interfaces.

Related commands: **user-bind**.

Examples # Display all static bindings.

```
<Sysname> display user-bind
The following user address bindings have been configured:
MAC                IP                Vlan    Port                Status
N/A                1.1.1.1          N/A     Ethernet2/0/6      Static
0002-0002-0002    1.1.1.1          N/A     Ethernet2/0/6      Static
-----2 binding entries queried, 2 listed-----
```

Table 49 Field descriptions of the display user-bind command

| Field | Description |
|-------------------------------------|--|
| MAC | MAC address of the binding. N/A means that no MAC address is bound in the entry. |
| IP | IP address of the binding. N/A means that no IP address is bound in the entry. |
| Vlan | Static binding entry does not support VLAN-port binding. |
| Port | Port of the binding |
| Status | Type of the binding. Static means that the binding is manually configured. |
| 2 binding entries queried, 2 listed | Counts of static binding entries |

ip check source

Syntax **ip check source** { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ip check source

View Ethernet port view

Parameters **ip-address**: Specifies to bind source IP addresses to the port.

mac-address: Specifies to bind source MAC addresses to the port.

Description Use the **ip check source** command to configure the dynamic binding function on a port.

Use the **undo ip check source** command to restore the default.

By default, the dynamic binding function is disabled.

Note that you cannot configure the dynamic binding function on a port that is in an aggregation group.

Related commands: **display ip check source.**

Examples # Configure dynamic binding function on port Ethernet 2/0/1 to filter packets based on both source IP address and MAC address.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] ip check source ip-address mac-address
```

user-bind

Syntax **user-bind** { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* }

undo user-bind { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* }

View Ethernet interface view

Parameters **ip-address** *ip-address*: Specifies the IP address for the static binding. The IP address can only be a Class A, Class B, or Class C address and can be neither 127.x.x.x nor 0.0.0.0.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format of H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address.

Description Use the **user-bind** command to configure a static binding.
Use the **undo user-bind** command to delete a static binding.

By default, no static binding exists on a port.

Note that:

- The system does not support repeatedly configuring a binding entry to one port. A binding entry can be configured to multiple ports.
- In a valid binding entry, the MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address, and the IP address can only be a Class A, Class B, or Class C address and can be neither 127.x.x.x nor 0.0.0.0.

Related commands: **display user-bind.**

Examples # Configure a static binding on port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] user-bind ip-address 192.168.0.1 mac-address
0001-0001-0001
```

21

ROUTING OVERVIEW COMMANDS



- The term “router” in this document refers to a Layer 3 switch running routing protocols.
- Currently, the 0231A92P module on S7900E Ethernet switches does not support IPv6 features.

display ip relay-route

Syntax `display ip relay-route`

View Any view

Parameters None

Description Use the **display ip relay-route** command to display the information of recursive routes.

Examples # Display recursive route information.

```
<Sysname> display ip relay-route
Total Number of Relay-route is: 1.
Dest/Mask: 40.40.40.0/255.255.255.0
Related instance id(s): 1(1) 2(1) 3(1) 4(1)
```

Table 50 Field descriptions of the display ip relay-route command

| Field | Description |
|-----------------------------|---|
| Total Number of Relay-route | Total number of recursive routes |
| Dest/Mask | Destination address/mask of the recursive route |
| Related instance id(s) | The number in the parentheses after each instance ID indicates the number of routes that have used the recursive route in the routing table corresponding to the instance ID. |

display ip relay-tunnel

Syntax `display ip relay-tunnel`

View Any view

Parameters None

Description Use the **display ip relay-tunnel** command to display recursive tunnel information.

Examples # Display recursive tunnel information.

```
<Sysname> display ip relay-tunnel
  Total Number of Relay-tunnel is: 1.
  Dest/Mask: 40.40.40.40/255.255.255.255
  Related instance id(s): 1(1) 2(1) 3(1) 4(1)
```

Table 51 display ip relay-tunnel command output description

| Field | Description |
|------------------------------|--|
| Total Number of Relay-tunnel | Total number of recursive tunnels |
| Dest/Mask | Destination address/mask of the recursive tunnel |
| Related instance id(s) | The number in the parentheses after each instance ID indicates the number of routes that have used the recursive tunnel in the routing table corresponding to the instance ID. |

display ip routing-table

Syntax **display ip routing-table** [**verbose** | | { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameters **verbose**: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only summary information about active routes.

|: Uses a regular expression to filter output information.

begin: Displays routing table entries starting from the one specified by the regular expression.

include: Displays routing table entries specified by the regular expression.

exclude: Displays routing table entries other than those specified by the regular expression.

regular-expression: Regular expression, a string of 1 to 256 characters used for specifying routing entries.

Table 52 Special characters for regular expressions

| Character | Meaning | Remarks |
|-----------|--|--|
| _ | Underscore, functions similarly as a wildcard and matches one of the following:
(^ \${[.(){}])
or a space, the beginning of a string, the end of a string. | If it is not the first character in a regular expression, it can appear as many times as the command line length permits.
If it is the first character in a regular expression, it can be followed with up to four underscores.
If it appears intermittently in a regular expression, only the first group takes effect. |
| (| Left parenthesis, represents a stack push operation in a program. | It is not recommended to use this character in a regular expression. |
| . | Full stop, a wildcard that matches any character, including a space. | - |
| * | Asterisk, indicates that the character(s) to its left can appear 0 or more times. | zo* matches z and zoo. |
| + | Plus, indicates that the character(s) to its left can appear one or more times. | zo+ matches zo and zoo, but not z. |

Description Use the **display ip routing-table** command to display brief information about active routes in the routing table.

Use the **display ip routing-table verbose** command to display detailed information about all routes in the routing table.

Examples # Display brief information about active routes in the routing table.

```
<Sysname> display ip routing-table
Routing Tables: Public
          Destinations : 6           Routes : 6

Destination/Mask    Proto  Pre  Cost           NextHop           Interface
10.10.3.0/24        Direct  0    0             10.10.3.1         Vlan2
10.10.3.1/32        Direct  0    0             127.0.0.1         InLoop0
127.0.0.0/8         Direct  0    0             127.0.0.1         InLoop0
127.0.0.1/32        Direct  0    0             127.0.0.1         InLoop0
192.168.0.0/24      Direct  0    0             192.168.0.72      Vlan1
192.168.0.72/32     Direct  0    0             127.0.0.1         InLoop0
```

Table 53 Field descriptions of the display ip routing-table command

| Field | Description |
|------------------|--------------------------------------|
| Destinations | Number of destination addresses |
| Routes | Number of routes |
| Destination/Mask | Destination address/mask length |
| Proto | Protocol that presents the route |
| Pre | Priority of the route |
| Cost | Cost of the route |
| NextHop | Address of the next hop on the route |

Table 53 Field descriptions of the display ip routing-table command

| Field | Description |
|-----------|--|
| Interface | Output interface for packets to be forwarded along the route |

Display detailed information about all routes in the routing table.

```
<Sysname> display ip routing-table verbose
Routing Table : Public
      Destinations : 6          Routes : 6

Destination: 10.10.3.0/24
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 10.10.3.1       Interface: Vlan-interface2
RelyNextHop: 0.0.0.0       Neighbor : 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active Adv        Age: 1d06h37m12s
  Tag: 0

Destination: 10.10.3.1/32
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 127.0.0.1       Interface: InLoopBack0
RelyNextHop: 0.0.0.0       Neighbor : 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active NoAdv      Age: 1d06h37m12s
  Tag: 0

Destination: 127.0.0.0/8
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 127.0.0.1       Interface: InLoopBack0
RelyNextHop: 0.0.0.0       Neighbor : 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active NoAdv      Age: 3d23h11m49s
  Tag: 0

Destination: 127.0.0.1/32
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 127.0.0.1       Interface: InLoopBack0
RelyNextHop: 0.0.0.0       Neighbor : 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active NoAdv      Age: 3d23h11m51s
  Tag: 0

Destination: 192.168.0.0/24
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 192.168.0.72    Interface: Vlan-interface1
RelyNextHop: 0.0.0.0       Neighbor : 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active Adv        Age: 3d23h08m38s
  Tag: 0

Destination: 192.168.0.72/32
```

```

Protocol: Direct          Process ID: 0
Preference: 0             Cost: 0
  NextHop: 127.0.0.1      Interface: InLoopBack0
RelyNextHop: 0.0.0.0     Neighbor : 0.0.0.0
Tunnel ID: 0x0           Label: NULL
  State: Active NoAdv     Age: 3d23h08m40s
  Tag: 0

```

Displayed first are statistics for the whole routing table, followed by detailed description of each route (in sequence).

Table 54 display ip routing-table verbose command output description

| Field | Description |
|-------------|--|
| Destination | Destination address/mask length |
| Protocol | Protocol that presents the route |
| Process ID | Process ID |
| Preference | Priority of the route |
| Cost | Cost of the route |
| NextHop | Address of the next hop on the route |
| Interface | Outbound interface for packets to be forwarded along the route |
| RelyNextHop | The next hop address obtained through routing stack. |
| Neighbor | Neighboring address determined by Routing Protocol |
| Tunnel ID | Tunnel ID |
| Label | Label |

Table 54 display ip routing-table verbose command output description

| Field | Description |
|------------|--|
| State | Route status: |
| Active | This is an active unicast route. |
| Adv | This route can be advertised. |
| Delete | This route is deleted. |
| Gateway | This is an indirect route. |
| Holddown | Number of holddown routes. Holddown is a route advertisement policy used in some distance vector (D-V) routing protocols, such as RIP, to avoid the propagation of some incorrect routes. It distributes a Holddown route during a period regardless of whether a new route to the same destination is found. For details, refer to corresponding routing protocols. |
| Int | The route was discovered by an Internal Gateway Protocol (IGP). |
| NoAdv | The route is not advertised when the router advertises routes based on policies. |
| NotInstall | Normally, among routes to a destination, the route with the highest preference is installed into the core routing table and advertised, while a NotInstall route cannot be installed into the core routing table but may be advertised. |
| Reject | The packets matching a Reject route will be dropped. Besides, the router sends ICMP unreachable messages to the sources of the dropped packets. The Reject routes are usually used for network testing. |
| Static | A static route is not lost when you perform the save operation and then restart the router. Routes configured manually are marked as static . |
| Unicast | Unicast routes |
| Inactive | Inactive routes |
| Invalid | Invalid routes |
| WaitQ | The route is the WaitQ during route recursion. |
| TunE | Tunnel |
| GotQ | The route is in the GotQ during route recursion. |
| Age | Time for which the route has been in the routing table, in the sequence of hour, minute, and second from left to right. |
| Tag | Route tag |

display ip routing-table acl

Syntax `display ip routing-table acl acl-number [verbose]`

View Any view

Parameters *acl-number*: Basic ACL number, in the range of 2000 to 2999.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

Description Use the **display ip routing-table acl** command to display information about routes permitted by a specified basic ACL.

This command is intended for the follow-up display of routing policies.

For more information about routing policy, refer to “IPv4 Routing Policy Configuration Commands” on page 467.



If the specified ACL does not exist or it has no rules configured, the entire routing table is displayed.

Examples # Define basic ACL 2000 and set the route filtering rules.

```
<Sysname > system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule deny source any
```

Display brief information about active routes permitted by basic ACL 2000.

```
[Sysname-acl-basic-2000] display ip routing-table acl 2000
Routes Matched by Access list : 2000
Summary Count : 2
```

| Destination/Mask | Proto | Pre | Cost | NextHop | Interface |
|------------------|--------|-----|------|---------------|-----------|
| 192.168.0.0/24 | Direct | 0 | 0 | 192.168.0.136 | Vlan1 |
| 192.168.0.136/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |

For detailed description of the above output, see Table 53.

Display detailed information about both active and inactive routes permitted by basic ACL 2000.

```
<Sysname> display ip routing-table acl 2000 verbose
Routes Matched by Access list : 2000
Summary Count : 2
```

```
Destination: 192.168.0.0/24
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 192.168.0.136   Interface: Vlan-interface1
RelyNextHop: 0.0.0.0       Neighbor : 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active Adv        Age: 1d04h26m42s
  Tag: 0
```

```
Destination: 192.168.0.136/32
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 127.0.0.1       Interface: InLoopBack0
RelyNextHop: 0.0.0.0       Neighbor : 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active NoAdv      Age: 1d04h26m42s
  Tag: 0
```

For the description of the command output above, see Table 54.

display ip routing-table ip-address

Syntax **display ip routing-table** *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *ip-address1* { *mask-length* | *mask* } *ip-address2* { *mask-length* | *mask* } [**verbose**]

View Any view

Parameters *ip-address*: Destination IP address, in dotted decimal format.

mask-length: IP address mask length in the range 0 to 32.

mask: IP address mask in dotted decimal format.

longer-match: Displays the route with the longest mask.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only summary information about active routes.

Description Use the **display ip routing-table** *ip-address* command to display information about routes to a specified destination address.

Executing the command with different parameters yields different output:

- **display ip routing-table** *ip-address*

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for an entry and this entry is active, it is displayed.

- **display ip routing-table** *ip-address mask*

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for an entry and the entry is active with a subnet mask less than or equal to the input subnet mask, the entry is displayed.

Only route entries that exactly match the input destination address and mask are displayed.

- **display ip routing-table** *ip-address longer-match*

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for multiple entries that are active, the one with longest mask length is displayed.

■ **display ip routing-table** *ip-address mask longer-match*

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for multiple entries with a mask less than or equal to the input subnet mask, the one that is active with longest mask length is displayed.

Use the **display ip routing-table** *ip-address1 { mask-length | mask } ip-address2 { mask-length | mask }* command to display route entries with destination addresses within a specified range.

Examples # Display route entries for the destination IP address 11.1.1.1.

```
<Sysname> display ip routing-table 11.1.1.1
Routing Table : Public
Summary Count : 4
```

| Destination/Mask | Proto | Pre | Cost | NextHop | Interface |
|------------------|--------|-----|------|---------|-----------|
| 0.0.0.0/0 | Static | 60 | 0 | 0.0.0.0 | NULL0 |
| 11.0.0.0/8 | Static | 60 | 0 | 0.0.0.0 | NULL0 |
| 11.1.0.0/16 | Static | 60 | 0 | 0.0.0.0 | NULL0 |
| 11.1.1.0/24 | Static | 60 | 0 | 0.0.0.0 | NULL0 |

Display route entries by specifying a destination IP address and the **longer-match** keyword.

```
<Sysname> display ip routing-table 11.1.1.1 longer-match
Routing Table : Public
Summary Count : 1
```

| Destination/Mask | Proto | Pre | Cost | NextHop | Interface |
|------------------|--------|-----|------|---------|-----------|
| 11.1.1.0/24 | Static | 60 | 0 | 0.0.0.0 | NULL0 |

Display route entries by specifying a destination IP address and mask.

```
<Sysname> display ip routing-table 11.1.1.1 24
Routing Table : Public
Summary Count : 3
```

| Destination/Mask | Proto | Pre | Cost | NextHop | Interface |
|------------------|--------|-----|------|---------|-----------|
| 11.0.0.0/8 | Static | 60 | 0 | 0.0.0.0 | NULL0 |
| 11.1.0.0/16 | Static | 60 | 0 | 0.0.0.0 | NULL0 |
| 11.1.1.0/24 | Static | 60 | 0 | 0.0.0.0 | NULL0 |

Display route entries by specifying a destination IP address and mask and the **longer-match** keyword.

```
<Sysname> display ip routing-table 11.1.1.1 24 longer-match
Routing Table : Public
Summary Count : 1
```

```

Destination/Mask    Proto  Pre  Cost           NextHop           Interface
11.1.1.0/24         Static 60   0              0.0.0.0           NULL0

```

Display route entries for destination addresses in the range 1.1.1.0 to 5.5.5.0.

```

<Sysname> display ip routing-table 1.1.1.0 24 5.5.5.0 24
Routing Table : Public

```

```

Destination/Mask    Proto  Pre  Cost           NextHop           Interface
1.1.1.0/24         Direct 0    0              1.1.1.1           Vlan1
1.1.1.1/32         Direct 0    0              127.0.0.1         InLoop0
2.2.2.0/24         Direct 0    0              2.2.2.1           Vlan2

```

For the description of the command output above, see Table 53.

display ip routing-table ip-prefix

Syntax `display ip routing-table ip-prefix ip-prefix-name [verbose]`

View Any view

Parameters *ip-prefix-name*: IP Prefix list name, a string of 1 to 19 characters.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

Description Use the **display ip routing-table ip-prefix** command to display information about routes permitted by a specified prefix list.

This command is intended for the follow-up display of routing policies. If the specified prefix list is not configured, detailed information about all routes (with the **verbose** keyword) or brief information about all active routes (without the **verbose** keyword) is displayed.

Examples # Configure a prefix list named **test**, permitting routes with a prefix of 2.2.2.0 and a mask length between 24 and 32.

```

<Sysname> system-view
[Sysname] ip ip-prefix test permit 2.2.2.0 24 less-equal 32

```

Display brief information about active routes permitted by the prefix list **test**.

```

[Sysname] display ip routing-table ip-prefix test
Routes Matched by Prefix list : test
Summary Count : 2

```

```

Destination/Mask    Proto  Pre  Cost           NextHop           Interface
2.2.2.0/24         Direct 0    0              2.2.2.1           Vlan2
2.2.2.1/32         Direct 0    0              127.0.0.1         InLoop0

```

For detailed description of the above output, see Table 53.

Display detailed information about both active and inactive routes permitted by IP prefix list **test**.

```
[Sysname] display ip routing-table ip-prefix test verbose
Routes Matched by Prefix list test :
Summary Count : 2

Destination: 2.2.2.0/24
  Protocol: Direct                      Process ID: 0
  Preference: 0                          Cost: 0
  NextHop: 2.2.2.1                       Interface: Vlan2
  RelyNextHop: 0.0.0.0                   Neighbour: 0.0.0.0
  Tunnel ID: 0x0                          Label: NULL
  State: Active Adv                       Age: Od00h20m52s
  Tag: 0

Destination: 2.2.2.1/32
  Protocol: Direct                      Process ID: 0
  Preference: 0                          Cost: 0
  NextHop: 127.0.0.1                     Interface: InLoop0
  RelyNextHop: 0.0.0.0                   Neighbour: 0.0.0.0
  Tunnel ID: 0x0                          Label: NULL
  State: Active NoAdv                     Age: Od00h20m52s
  Tag: 0
```

For detailed description of the above output, see Table 54.

display ip routing-table protocol

Syntax **display ip routing-table protocol** *protocol* [**inactive** | **verbose**]

View Any view

Parameters *protocol*: Routing protocol. It can be **BGP**, **DIRECT**, **ISIS**, **OSPF**, **RIP**, or **STATIC**.

inactive: Displays information about only inactive routes. With this argument absent, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. With this argument absent, the command displays brief routing table information.

Description Use the **display ip routing-table protocol** command to display routing information of a specified routing protocol.

Examples # Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct
Public Routing Table : Direct
Summary Count : 5

Direct Routing table Status : < Active>
Summary Count : 5
```

| Destination/Mask | Proto | Pre | Cost | NextHop | Interface |
|------------------|--------|-----|------|-----------|-----------|
| 2.2.2.0/24 | Direct | 0 | 0 | 2.2.2.1 | Vlan2 |
| 2.2.2.2/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 127.0.0.0/8 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 127.0.0.1/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 192.168.80.10/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |

Direct Routing table Status : < Inactive>
 Summary Count : 0

Display summary information about static routes.

```
<Sysname> display ip routing-table protocol static
Public Routing Table : Static
Summary Count : 1
```

Static Routing table Status : < Active>
 Summary Count : 0

Static Routing table Status : < Inactive>
 Summary Count : 1

| Destination/Mask | Proto | Pre | Cost | NextHop | Interface |
|------------------|--------|-----|------|---------|-----------|
| 1.2.3.0/24 | Static | 60 | 0 | 1.2.4.5 | Vlan10 |

For detailed description of the above output, see Table 53.

display ip routing-table statistics

Syntax `display ip routing-table statistics`

View Any view

Parameters None

Description Use the **display ip routing-table statistics** command to display statistics about the public network routing table.

Examples # Display statistics about the routes in the routing table.

```
<Sysname> display ip routing-table statistics
Proto      route      active      added      deleted      freed
DIRECT     24         4           25         1            0
STATIC     4          1           4          0            0
RIP        0          0           0          0            0
OSPF       0          0           0          0            0
IS-IS      0          0           0          0            0
BGP        0          0           0          0            0
Total      28         5           29         1            0
```

Table 55 Field descriptions of display ip routing-table statistics

| Field | Description |
|---------|---|
| Proto | Origin of the routes. Possible values include O_ASE for OSPF_ASE routes, O_NSSA for OSPF NSSA, and AGGRE for aggregated routes. |
| route | Number of routes from the origin |
| active | Number of active routes from the origin |
| added | Number of routes added into the routing table since the router starts up or the last routing table reset operation |
| deleted | Number of routes marked as deleted, which will be freed after a period. |
| freed | Number of routes that got freed, that is, got removed permanently |
| Total | Sums for the numerical items above |

display ipv6 relay-route

Syntax **display ipv6 relay-route**

View Any view

Parameters None

Description Use the **display ipv6 relay-route** command to display IPv6 recursive route information.

Examples # Display IPv6 recursive route information.

```
<Sysname> display ipv6 relay-route
Total Number of relay-route is: 1
Dest/Mask: 192::1/64
Related instance id(always 0): 0(1)
```

Table 56 Field descriptions of the display ipv6 relay-route command

| Field | Description |
|--------------------------------|--|
| Total Number of Relay-route | Total number of recursive routes |
| Dest/Mask | Destination address/mask of the recursive route |
| Related instance id (always 0) | IPv6 supports public networks only. Therefore, the instance ID can be 0 only.

The number in the parentheses after the instance ID indicates the number of routes that have used the recursive route in the routing table. |

display ipv6 relay-tunnel

Syntax **display ipv6 relay-tunnel**

View Any view

Parameters None

Description Use the **display ipv6 relay-tunnel** command to display IPv6 recursive tunnel information.

Examples # Display IPv6 recursive tunnel information.

```
<Sysname> display ipv6 relay-tunnel
Total Number of relay-tunnel is: 1.
Dest/Mask: 192::0/64
Related instance id(always 0): 0(1)
```

Table 57 display ipv6 relay-tunnel command output description

| Field | Description |
|--------------------------------|--|
| Total Number of Relay-tunnel | Total number of recursive tunnels |
| Dest/Mask | Destination address/mask of the recursive tunnel |
| Related instance id (always 0) | IPv6 supports public networks only. Therefore, the instance ID can be 0 only.

The number in the parentheses after the instance ID indicates the number of routes that have used the recursive route in the routing table. |

display ipv6 routing-table

Syntax **display ipv6 routing-table**

View Any view

Parameters None

Description Use the **display ipv6 routing-table** command to display brief routing table information, including destination IP address and prefix, protocol type, priority, metric, next hop and outbound interface.

The command displays only active routes, namely, the brief information about the current optimal routes.

Examples # Display brief routing table information

```
<Sysname> display ipv6 routing-table
Routing Table :
Destinations : 1          Routes : 1

Destination : ::1/128          Protocol : Direct
NextHop     : ::1              Preference : 0
Interface   : InLoop0         Cost      : 0
```

Table 58 Field descriptions of the display ipv6 routing-table command

| Field | Description |
|-------------|--------------------------|
| Destination | Destination IPv6 address |
| NextHop | Next hop |
| Preference | Routing preference |
| Interface | Outbound interface |

Table 58 Field descriptions of the display ipv6 routing-table command

| Field | Description |
|----------|-------------------------------|
| Protocol | Routing protocol of the route |
| Cost | Routing cost |

display ipv6 routing-table acl

Syntax **display ipv6 routing-table acl** *acl6-number* [**verbose**]

View Any view

Parameters *acl6-number*: Basic IPv6 ACL number, in the range 2000 to 2999.

verbose: Displays both active and inactive verbose routing information permitted by the ACL. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table acl** command to display routing information permitted by the IPv6 ACL.

If the specified IPv6 ACL is not available, all routing information is displayed.

Examples # Display brief routing information permitted by ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000
Routes Matched by Access list 2000 :
Summary Count : 2
```

```
Destination : ::1/128                Protocol   : Direct
NextHop      : ::1                    Preference : 0
Interface    : InLoop0                Cost       : 0
```

```
Destination : 1:1::/64                Protocol   : Static
NextHop      : ::                     Preference : 60
Interface    : NULL0                  Cost       : 0
```

Refer to Table 58 for description about the above output.

display ipv6 routing-table ipv6-address

Syntax **display ipv6 routing-table** *ipv6-address prefix-length* [**longer-match**] [**verbose**]

View Any view

Parameters *ipv6-address*: Destination IPv6 address.

prefix-length: Prefix length, in the range 0 to 128.

longer-match: Displays the matched route having the longest prefix length.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table** *ipv6-address* command to display routing information about the specified destination IPv6 address.

Executing the command with different parameters yields different output:

■ **display ipv6 routing-table** *ipv6-address prefix-length*

The system ANDs the input destination IPv6 address with the input prefix length, and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for an entry and the entry is active with a prefix length less than or equal to the input prefix length, the entry is displayed.

Only route entries that exactly match the input destination address and prefix length are displayed.

■ **display ipv6 routing-table** *ipv6-address prefix-length longer-match*

The system ANDs the input destination IPv6 address with the input prefix length; and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for multiple entries with a prefix length less than or equal to the input prefix length, the one that is active with the longest prefix length is displayed.

Examples # Display brief information about the route matching the specified destination IPv6 address.

```
<Sysname> display ipv6 routing-table 10::1 127
Routing Table:
Summary Count: 3
```

```
Destination: 10::/64                Protocol : Static
NextHop      : ::                    Preference: 60
Interface    : NULL0                 Cost      : 0
```

```
Destination: 10::/68                Protocol : Static
NextHop      : ::                    Preference: 60
Interface    : NULL0                 Cost      : 0
```

```
Destination: 10::/120               Protocol : Static
NextHop      : ::                    Preference: 60
Interface    : NULL0                 Cost      : 0
```

Display brief information about the matched route with the longest prefix length.

```
<Sysname> display ipv6 routing-table 10:: 127 longer-match
Routing Tables:
Summary Count : 1
```

```

Destination: 10::/120                                Protocol : St
atic
NextHop      : ::                                     Preference: 60
Interface   : NULL0                                  Cost      : 0

```

Refer to Table 58 for description about the above output.

display ipv6 routing-table ipv6-address1 ipv6-address2

Syntax **display ipv6 routing-table** *ipv6-address1 prefix-length1 ipv6-address2 prefix-length2* [**verbose**]

View Any view

Parameters *ipv6-address1/ipv6-address2*: An IPv6 address range from IPv6 address1 to IPv6 address2.

prefix-length1/prefix-length2: Prefix length, in the range 0 to 128.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table** *ipv6-address1 ipv6-address2* command to display routes with destinations falling into the specified IPv6 address range.

Examples # Display routes with destinations falling into the IPv6 address range.

```

<Sysname> display ipv6 routing-table 100:: 64 400:: 64
Routing Table :
Summary Count : 3

Destination: 100::/64                                Protocol : Static
NextHop      : 1::2                                   Preference: 60
Interface    : Vlan1                                  Cost      : 0

Destination: 200::/64                                Protocol : Static
NextHop      : 1::2                                   Preference: 60
Interface    : Vlan1                                  Cost      : 0

Destination: 300::/64                                Protocol : Static
NextHop      : 1::2                                   Preference: 60
Interface    : Vlan1                                  Cost      : 0

```

Refer to Table 58 for description about the above output.

display ipv6 routing-table ipv6-prefix

Syntax **display ipv6 routing-table ipv6-prefix** *ipv6-prefix-name* [**verbose**]

View Any view

Parameters *ipv6-prefix-name*: Name of the IPv6 prefix list, in the range 1 to 19 characters.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table ipv6-prefix** command to display routes permitted by the IPv6 prefix list.

Examples # Display brief active routing information permitted by the IPv6 prefix list **test2**.

```
<Sysname> display ipv6 routing-table ipv6-prefix test2
Routes Matched by Prefix list test2 :
Summary Count : 1

Destination: 100::/64                Protocol : Static
NextHop      : ::                    Preference: 60
Interface    : NULL0                 Cost      : 0
```

Refer to Table 58 for description about the above output.

display ipv6 routing-table protocol

Syntax **display ipv6 routing-table protocol** *protocol* [**inactive** | **verbose**]

View Any view

Parameters *protocol*: Displays routes of a routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng** and **static**.

inactive: Displays only inactive routes. Without the keyword, all active and inactive routes are displayed.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table protocol** command to display routes of a specified routing protocol.

Examples # Display brief information about all direct routes.

```
<Sysname> display ipv6 routing-table protocol direct
Direct Routing Table :
Summary Count : 1

Direct Routing Table's Status : < Active >
Summary Count : 1

Destination: ::1/128                Protocol : Direct
NextHop      : ::1                  Preference: 0
Interface    : InLoop0             Cost      : 0

Direct Routing Table's Status : < Inactive >
Summary Count : 0
```

Refer to Table 58 for description about the above output.

display ipv6 routing-table statistics

Syntax `display ipv6 routing-table statistics`

View Any view

Parameters None

Description Use the **display ipv6 routing-table statistics** command to display routing statistics, including total route number, added route number and deleted route number.

Examples # Display routing statistics.

```
<Sysname> display ipv6 routing-table statistics
Protocol  route    active   added    deleted  freed
DIRECT   1         1        1        0        0
STATIC   3         0        3        0        0
RIPng    0         0        0        0        0
OSPFv3   0         0        0        0        0
IS-ISv6  0         0        0        0        0
BGP4+    0         0        0        0        0
Total    4         1        4        0        0
```

Table 59 Field descriptions of the display ipv6 routing-table statistics command

| Field | Description |
|----------|--|
| Protocol | Routing protocol |
| route | Route number of the protocol |
| active | Active route number |
| added | Routes added after the last startup of the router |
| deleted | Deleted routes, which will be released after a specified time |
| freed | Released (totally removed from the routing table) route number |
| Total | Total route number |

display ipv6 routing-table verbose

Syntax `display ipv6 routing-table verbose`

View Any view

Parameters None

Description Use the **display ipv6 routing-table verbose** command to display detailed information about all active and inactive routes, including the statistics of the entire routing table and information for each route.

Examples # Display detailed information about all active and inactive routes.

```

<Sysname> display ipv6 routing-table verbose
Routing Table :
    Destinations : 1          Routes : 1

Destination : ::1          PrefixLength : 128
NextHop     : ::1          Preference   : 0
RelayNextHop : ::         Tag          : 0H
Neighbour   : ::         ProcessID    : 0
Interface   : InLoopBack0 Protocol      : Direct
State       : Active NoAdv Cost          : 0
Tunnel ID   : 0x0         Label       : NULL
Age         : 22161sec

```

Table 60 Field descriptions of the display ipv6 routing-table verbose command

| Field | Description |
|--------------|---|
| Destination | Destination IPv6 address |
| PrefixLength | Prefix length of the address |
| Nexthop | Next hop |
| Preference | Routing preference |
| RelayNextHop | Relay next hop |
| Tag | Tag of the route |
| Neighbor | Neighbor address |
| ProcessID | Process ID |
| Interface | Outbound interface |
| Protocol | Routing protocol |
| State | State of the route, Active, Inactive, Adv (advertised), or NoAdv (not advertised) |
| Cost | Cost of the route |
| Tunnel ID | Tunnel ID |
| Label | Label |
| Age | Time that has elapsed since the route was generated |

reset ip routing-table statistics protocol

Syntax `reset ip routing-table statistics protocol { all | protocol }`

View User view

Parameters **all**: Clears statistics for all routing protocols.

protocol: Clears statistics for the routing protocol, which can be **bgp**, **direct**, **is-is**, **ospf**, **rip**, or **static**.

Description Use the **reset ip routing-table statistics protocol** command to clear the routing statistics of the routing table.

Examples # Clear the routing statistics of the routing table.

```
<Sysname> reset ip routing-table statistics protocol all
```

reset ipv6 routing-table statistics

Syntax `reset ipv6 routing-table statistics protocol { all | protocol }`

View User view

Parameters **all**: Clears statistics for all routing protocols.

protocol: Clears statistics for the routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

Description Use the **reset ipv6 routing-table statistics** command to clear the route statistics of the routing table.

Examples # Clear statistics for all routing protocols.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```


22

STATIC ROUTING CONFIGURATION COMMANDS



The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

delete static-routes all

Syntax `delete static-routes all`

View System view

Parameters None

Description Use the **delete static-routes all** command to delete all static routes.

When you use this command to delete static routes, the system will prompt you to confirm the operation before deleting all the static routes.

Related commands: `display ip routing-table`, `ip route-static`.

Examples # Delete all static routes on the router.

```
<Sysname> system-view
[Sysname] delete static-routes all
This will erase all ipv4 static routes and their configurations, you
must reconf
figure all static routes
Are you sure?[Y/N]:Y
```

ip route-static

Syntax `ip route-static dest-address { mask | mask-length } { gateway-address | interface-type interface-number [gateway-address] } [preference preference-value] [tag tag-value] [description description-text]`

`undo ip route-static dest-address { mask | mask-length } [gateway-address | interface-type interface-number [gateway-address]] [preference preference-value]`

View System view

Parameters `dest-address`: Destination IP address of the static route, in dotted decimal notation.

mask: Mask of the IP address, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

gateway-address: IP address of the next hop, in dotted decimal notation.

interface-type interface-number: Specifies the output interface by its type and number. If the output interface is a broadcast interface, such as an Ethernet interface, a virtual template or a VLAN interface, the next hop address must be specified.

preference *preference-value*: Specifies the preference of the static route, which is in the range of 1 to 255 and defaults to 60.

tag *tag-value*: Sets a tag value for the static route from 1 to 4294967295. The default is 0. Tags of routes are used in routing policies to control routing.

description *description-text*: Configures a description for the static route, which consists of 1 to 60 characters, including special characters like space, but excluding "?".

Description Use the **ip route-static** command to configure a unicast static route.

Use the **undo ip route-static** command to delete a unicast static route.

When configuring a unicast static route, note that:

- 1 If the destination IP address and the mask are both 0.0.0.0, the configured route is a default route. If routing table searching fails, the router will use the default route for packet forwarding.
- 2 Different route management policies can be implemented for different route preference configurations. For example, specifying the same preference for different routes to the same destination address enables load sharing, while specifying different preferences for these routes enables route backup.
- 3 When configuring a static route, you can specify the output interface or the next hop address based on the actual requirement. Note that the next hop address must not be the IP address of the local interface; otherwise, the route configuration will not take effect. For interfaces that support network address to link layer address resolution or point-to-point interfaces, you can specify the output interface or next hop address. When specifying the output interface, note that:
- 4 For a NULL0 or loopback interface, if the output interface has already been configured, there is no need to configure the next hop address.
- 5 It is not recommended to specify a broadcast interface (such as VLAN interface) as the output interface for a static route, because a broadcast interface may have multiple next hops. If you have to do so, you must specify the corresponding next hop of the interface at the same time.

Related commands: **display ip routing-table**, **ip route-static default-preference**.



The static route does not take effect if you specify its next hop address first and then configure the address as the IP address of a local interface, such as VLAN interface.

Examples # Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, tag value is 45, and description information is **for internet & intranet**.

```
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for
internet & intranet
```

ip route-static default-preference

Syntax **ip route-static default-preference** *default-preference-value*

undo ip route-static default-preference

View System view

Parameters *default-preference-value*: Default preference for static routes, which is in the range of 1 to 255.

Description Use the **ip route-static default-preference** command to configure the default preference for static routes.

Use the **undo ip route-static default-preference** command to restore the default.

By default, the default preference of static routes is 60.

Note that:

- If no preference is specified when configuring a static route, the default preference is used.
- When the default preference is re-configured, it applies to newly added static routes only.

Related commands: **display ip routing-table**, **ip route-static**.

Examples # Set the default preference of static routes to 120.

```
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```


23

RIP CONFIGURATION COMMANDS



The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

checkzero

Syntax **checkzero**
undo checkzero

View RIP view

Parameters None

Description Use the **checkzero** command to enable the zero field check on RIPv1 messages.

Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

After the zero field check is enabled, the router discards RIPv1 messages in which zero fields are non-zero. If all messages are trustworthy, you can disable this feature to spare the processing time of the CPU.

Examples # Disable the zero field check on RIPv1 messages for RIP process 100.

```
<Sysname> system-view  
[Sysname] rip 100  
[Sysname-rip-100] undo checkzero
```

default cost

Syntax **default cost** *value*
undo default cost

View RIP view

Parameters *value*: Default metric of redistributed routes, in the range of 0 to 16.

Description Use the **default cost** command to configure the default metric for redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default metric of redistributed routes is 0.

When you use the **import-route** command to redistribute routes from other protocols without specifying a metric, the metric specified by the **default cost** command applies.

Related command: **import-route**.

Examples # Set the default metric for redistributed routes to 3.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default cost 3
```

default-route originate

Syntax **default-route originate cost** *value*

undo default-route originate

View RIP view

Parameters *value*: Cost of the default route, in the range of 1 to 15.

Description Use the **default-route originate cost** command to advertise a default route with the specified metric to RIP neighbors.

Use the **undo default-route originate** command to disable the sending of a default route.

By default, no default route is sent to RIP neighbors.

The RIP router with this feature configured will not receive any default routes from RIP neighbors.

Examples # Send a default route with a metric of 2 to RIP neighbors.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default-route originate cost 2
```

Disable default route sending.

```
[Sysname-rip-100] undo default-route originate
```

display rip

Syntax **display rip** [*process-id*]

View Any view

Parameters *process-id*: RIP process ID, in the range of 1 to 65535.

Description Use the **display rip** command to display the current status and configuration information of the specified RIP process.

If *process-id* is not specified, information about all configured RIP processes is displayed.

Examples # Display the current status and configuration information of all configured RIP processes.

```
<Sysname> display rip
Public VPN-instance name :

RIP process : 1
RIP version : 1
Preference : 100
Checkzero : Enabled
Default-cost : 0
Summary : Enabled
Hostroutes : Enabled
Maximum number of balanced paths : 4
Update time   : 30 sec(s) Timeout time       : 180 sec(s)
Suppress time : 120 sec(s) Garbage-collect time : 120 sec(s)
TRIP retransmit time : 5 sec(s)
TRIP response packets retransmit count : 36
Silent interfaces : None
Default routes : Disabled
Verify-source : Enabled
Networks :
  192.168.1.0
Configured peers : None
Triggered updates sent : 0
Number of routes changes : 0
Number of replies to queries : 0
```

Table 61 Field descriptions of the display rip command

| Field | Description |
|---|--|
| Public VPN-instance name (or Private VPN-instance name) | The RIP process runs under a public VPN instance/The RIP process runs under a private VPN instance |
| RIP process | RIP process ID |
| RIP version | RIP version 1 or 2 |
| Preference | RIP route priority |
| Checkzero | Indicates whether the zero field check is enabled for RIPv1 messages. |
| Default-cost | Default cost of the redistributed routes |
| Summary | Indicates whether the routing summarization is enabled |

Table 61 Field descriptions of the display rip command

| | |
|--|--|
| Hostroutes | Indicates whether to receive host routes |
| Maximum number of balanced paths | Maximum number of load balanced routes |
| Update time | RIP update interval |
| Timeout time | RIP timeout time |
| Suppress time | RIP suppress interval |
| Garbage-collect time | RIP garbage collection interval |
| TRIP retransmit time | TRIP retransmit interval for sending update requests and responses. |
| TRIP response packets retransmit count | Maximum retransmit times for update requests and responses |
| Silent interfaces | Number of silent interfaces, which do not periodically send updates |
| Default routes | Indicates whether a default route is sent to RIP neighbors |
| Verify-source | Indicates whether the source IP address is checked on the received RIP routing updates |
| Networks | Networks enabled with RIP |
| Configured peers | Configured neighbors |
| Triggered updates sent | Number of sent triggered updates |
| Number of routes changes | Number of changed routes in the database |
| Number of replies to queries | Number of RIP responses |

display rip database

Syntax `display rip process-id database`

View Any view

Parameters *process-id*: RIP process ID, in the range of 1 to 65535.

Description Use the **display rip database** command to display the active routes in the RIP database, which are sent in normal RIP routing updates.

Examples # Display the active routes in the database of RIP process 100.

```
<Sysname> display rip 100 database
 10.0.0.0/8, cost 1, ClassfulSumm
 10.0.0.0/24, cost 1, nexthop 10.0.0.1, Rip-interface
 11.0.0.0/8, cost 1, ClassfulSumm
 11.0.0.0/24, cost 1, nexthop 10.0.0.1, Imported
```

Table 62 Description on fields of the display rip database command

| Field | Description |
|---------------|---|
| X.X.X.X/X | Destination address and subnet mask |
| cost | Cost of the route |
| classful-summ | Indicates the route is a RIP summary route. |
| Nexthop | Address of the next hop |

Table 62 Description on fields of the display rip database command

| | |
|---------------|---|
| Rip-interface | Routes learnt from a RIP-enabled interface |
| imported | Routes redistributed from other routing protocols |

display rip interface

Syntax **display rip** *process-id* **interface** [*interface-type interface-number*]

View Any view

Parameters *process-id*: RIP process ID, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface.

Description Use the **display rip interface** command to display the RIP interface information of the RIP process.

If no interface is specified, information about all RIP interfaces of the RIP process is displayed.

Examples # Display all the interface information of RIP process 1.

```
<Sysname> display rip 1 interface
```

```
Interface-name: Vlan-interface1
Address/Mask:1.1.1.1/24           MetricIn/Out:0/1   Version: RIPv1
Split-horizon/Poison-reverse:on/off   Input/Output:on/on
Current packets number/Maximum packets number: 234/2000
```

Table 63 Field descriptions of the display rip interface command

| Field | Description |
|---|---|
| Interface-name | The name of an interface running RIP. |
| Address/Mask | The IP address and Mask of the interface. |
| MetricIn/Out | Additional routing metric added to the incoming and outgoing routes |
| Version | RIP version running on the interface |
| Split-horizon | Indicates whether the split-horizon is enabled (ON: enabled, OFF: disabled). |
| Poison-reverse | Indicates whether the poison-reverse is enabled (ON: enabled, OFF: disabled) |
| Input/Output | Indicates if the interface is allowed to receive (Input) or send (Output) RIP messages (on is allowed, off is not allowed). |
| Current packets number/Maximum packets number | Packets to be sent/Maximum packets that can be sent on the interface |

display rip route

Syntax **display rip** *process-id* **route** [**statistics** | *ip-address* { *mask* | *mask-length* } | **peer** *ip-address*]

View Any view

Parameters *process-id*: RIP process ID, in the range of 1 to 65535.

statistics: Displays the route statistics, including total number of routes and number of routes of each neighbor.

ip-address { *mask* | *mask-length* }: Displays route information about a specified IP address.

peer *ip-address*: Displays all routing information learned from a specified neighbor.

Description Use the **display rip route** command to display the routing information of a specified RIP process.

Examples # Display all routing information of RIP process 1.

```
<Sysname> display rip 1 route
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
```

```
-----
Peer 21.0.0.23 on Vlan-interfacel
Destination/Mask  NextHop      Cost      Tag      Flags      Sec
56.0.0.0/8       21.0.0.23     1         0        RA         102
34.0.0.0/8       21.0.0.23     1         0        RA         23
Peer 21.0.0.12 on Vlan-interfacel
Destination/Mask  NextHop      Cost      Tag      Flags      Sec
56.0.0.0/8       21.0.0.12     1         0        RA         34
12.0.0.0/8       21.0.0.12     1         0        RA         12
```

Display routing information for network 56.0.0.0/8 of RIP process 1.

```
<Sysname> display rip 1 route 56.0.0.0 8
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
```

```
-----
Peer 21.0.0.23 on Vlan-interfacel
Destination/Mask  NextHop      Cost      Tag      Flags      Sec
56.0.0.0/8       21.0.0.23     1         0        RA         102
Peer 21.0.0.12 on Vlan-interfacel
Destination/Mask  NextHop      Cost      Tag      Flags      Sec
56.0.0.0/8       21.0.0.12     1         0        RA         34
```

Display RIP process1 routing information learned from the specified neighbor.

```
<Sysname> display rip 1 route peer 21.0.0.23
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
```

```
-----
Peer 21.0.0.23 on Vlan-interfacel
Destination/Mask  NextHop      Cost      Tag      Flags      Sec
```

```
56.0.0.0/8      21.0.0.23      1      0      RA      102
34.0.0.0/8      21.0.0.23      1      0      RA      23
```

Table 64 Field descriptions of the display rip route command

| Field | Description |
|-----------------------------------|--|
| Route Flags | R - RIP route
T - TRIP route
P - The route never expires
A - The route is aging
S - The route is suppressed
G - The route is in Garbage-collect state |
| Peer 21.0.0.23 on Vlan-interface1 | Routing information learned on a RIP interface from the specified neighbor |
| Destination/Mask | Destination IP address and subnet mask |
| Nexthop | Next hop of the route |
| Cost | Cost of the route |
| Tag | Route tag |
| Flags | Indicates the route state |
| Sec | Remaining time of the timer corresponding to the route state |

Display the routing statistics of RIP process 1.

```
<Sysname> display rip 1 route statistics
Peer      Aging      Permanent      Garbage
21.0.0.23  2          0              3
21.0.0.12  2          0              4
Total     4          0              7
```

Table 65 Field descriptions of the display rip route statistics command

| Field | Description |
|-----------|--|
| Peer | IP address of a neighbor |
| Aging | Total number of aging routes learned from the specified neighbor |
| Permanent | Total number of permanent routes learned from the specified neighbor |
| Garbage | Total number of routes in the garbage-collection state learned from the specified neighbor |
| Total | Total number of routes learned from all RIP neighbors |

filter-policy export

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]] [*interface-type* *interface-number*]

undo filter-policy export [*protocol* [*process-id*]] [*interface-type* *interface-number*]

View RIP view

Parameters *acl-number*: Number of an ACL used to filter outbound routes, in the range of 2000 to 3999.

ip-prefix *ip-prefix-name*: Name of an IP prefix list used to filter outbound routes, a string of 1 to 19 characters.

protocol: Filters outbound routes redistributed from a specified routing protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, and **static**.

process-id: Process ID of the specified routing protocol, in the range of 1 to 65535. You need to specify a process ID when the routing protocol is **rip**, **ospf**, or **isis**.

interface-type interface-number: Specifies an interface.

Description Use the **filter-policy export** command to configure the filtering of RIP outgoing routes. Only routes not filtered out can be advertised.

Use the **undo filter-policy export** command to remove the filtering.

By default, RIP does not filter outbound routes.

Note that:

- If *protocol* is specified, RIP filters only the outgoing routes redistributed from the specified routing protocol. Otherwise, RIP filters all routes to be advertised.
- If *interface-type interface-number* is specified, RIP filters only the routes advertised by the specified interface. Otherwise, RIP filters routes advertised by all RIP interfaces.

Related commands: **acl**, **import-route**, and **ip ip-prefix**.

Examples # Reference ACL 2000 to filter outbound routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

Reference IP prefix list abc to filter outbound routes on VLAN-interface 10.

```
[Sysname-rip-1] filter-policy ip-prefix abc export vlan-interface 10
```

filter-policy import

Syntax **filter-policy** { *acl-number* | **gateway** *ip-prefix-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import** [*interface-type interface-number*]

undo filter-policy import [*interface-type interface-number*]

View RIP view

Parameters *acl-number*: Number of the Access Control List (ACL) used for filtering incoming routes, in the range of 2000 to 3999.

ip-prefix *ip-prefix-name*: References an IP prefix list to filter incoming routes. The *ip-prefix-name* is a string of 1 to 19 characters.

gateway *ip-prefix-name*: References an IP prefix list to filter routes from the gateway.

interface-type interface-number: Specifies an interface.

Description Use the **filter-policy import** command to filter the incoming routes.
Use the **undo filter-policy import** command to restore the default.
By default, RIP does not filter incoming routes.

Related commands: **acl** and **ip ip-prefix**.

Examples # Reference ACL 2000 to filter incoming routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 import
```


Reference IP prefix list abc on VLAN-interface 10 to filter all received RIP routes.

```
[Sysname-rip-1] filter-policy ip-prefix abc import vlan-interface 10
```

host-route

Syntax **host-route**

undo host-route

View RIP view

Parameters None

Description Use the **host-route** command to enable host route reception.
Use the **undo host-route** command to disable host route reception.
By default, receiving host routes is enabled.

In some cases, a router may receive many host routes from the same network segment. These routes are not helpful for routing and occupy a large amount of network resources. You can use the **undo host-route** command to disable receiving of host routes.



RIPv2 can be disabled from receiving host routes, but RIPv1 cannot.

Examples # Disable RIP from receiving host routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

import-route

Syntax **import-route** *protocol* [*process-id*] [**allow-ibgp**] [**cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag*]*

undo import-route *protocol* [*process-id*]

View RIP view

Parameters *protocol*: Specify a routing protocol from which to redistribute routes, currently including **bgp**, **direct**, **isis**, **ospf**, **rip**, **rip** and **static**.

process-id: Process number of the routing protocol, in the range of 1 to 65535, used for **isis**, **rip**, and **ospf**.

cost: Cost for redistributed routes, in the range of 0 to 16. If *cost* is not specified, the default cost specified by the **default cost** command applies.

tag: Tag marking redistributed routes, in the range of 0 to 65,535. The default is 0.

route-policy *route-policy-name*: Specifies a routing policy with 1 to 19 characters.

allow-ibgp: When the *protocol* argument is set to **bgp**, **allow-ibgp** is an optional keyword. The **import-route bgp** command only redistributes EBGP routes, while the **import-route bgp allow-ibgp** command additionally redistributes IBGP routes, which may cause routing loops. Be cautious when using it.

Description Use the **import-route** command to enable route redistribution from another routing protocol.

Use the **undo import-route** command to disable route redistribution.

By default, RIP does not redistribute routes from other routing protocols.

- You can specify a routing policy using keyword **route-policy** to redistribute only the specified routes.
- You can configure a cost for redistributed routes using keyword **cost**.
- You can configure a tag value for redistributed routes using keyword **tag**.

Related commands: **default cost**.

Examples # Redistribute static routes, and set the cost to 4.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

Set the default cost for redistributed routes to 3.

```
[Sysname-rip-1] default cost 3
```

```
# Redistribute OSPF routes with the cost being the default cost.
```

```
[Sysname-rip-1] import-route ospf
```

maximum load-balancing

Syntax **maximum load-balancing** *number*

undo maximum load-balancing

View RIP view

Parameters *number*: Maximum number of load balanced routes, in the range 1 to 4.

Description Use the **maximum load-balancing** command to specify the maximum number of load balanced routes in load sharing mode.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of load balanced routes is 4.

Examples # Specify the maximum number of load balanced routes as 2.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] maximum load-balancing 2
```

network

Syntax **network** *network-address*

undo network *network-address*

View RIP view

Parameters *network-address*: IP address of a network segment, which can be the IP network address of any interface.

Description Use the **network** command to enable RIP on the interface attached to the specified network.

Use the **undo network** command to disable RIP on the interface attached to the specified network.

RIP runs only on the interfaces attached to the specified network. For an interface not on the specified network, RIP neither receives/sends routes on it nor forwards interface route through it. Therefore, you need to specify the network after enabling RIP to validate RIP on a specific interface.

Use the **network** 0.0.0.0 command to enable RIP on all interfaces.

RIP is disabled on an interface by default.

Examples # Enable RIP on the interface attached to the network 129.102.0.0.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] network 129.102.0.0
```

peer

Syntax **peer** *ip-address*

undo peer *ip-address*

View RIP view

Parameters *ip-address*: IP address of a RIP neighbor, in dotted decimal format.

Description Use the **peer** command to specify the IP address of a neighbor in the non-broadcast multi-access (NBMA) network, where routing updates destined to the peer are unicast, rather than multicast or broadcast.

Use the **undo peer** command to remove the IP address of a neighbor.

By default, no neighbor is specified.

Note: you need not use the **peer ip-address** command when the neighbor is directly connected; otherwise the neighbor may receive both the unicast and multicast (or broadcast) of the same routing information.

Examples # Specify to send unicast updates to peer 202.38.165.1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] peer 202.38.165.1
```

preference

Syntax **preference** [**route-policy** *route-policy-name*] *value*

undo preference [**route-policy**]

View RIP view

Parameters *route-policy-name*: Routing policy name with 1 to 19 characters.

value: Priority for RIP route, in the range of 1 to 255. The smaller the value, the higher the priority.

Description Use the **preference** command to specify the RIP route priority.

Use the **undo preference route-policy** command to restore the default.

By default, the priority of RIP route is 100.

You can specify a routing policy using keyword **route-policy** to set the specified priority to routes matching the routing policy.

- If a priority is set for matched routes in the routing policy, the priority applies to these routes. The priority of other routes is the one set by the **preference** command.
- If no priority is set for matched routes in the routing policy, the priority of all routes is the one set by the **preference** command.

Examples # Set the RIP route priority to 120.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] preference 120
```

reset rip statistics

Syntax **reset rip** *process-id* **statistics**

View User view

Parameters *process-id*: RIP process ID, in the range of 1 to 65535.

Description Use the **reset rip statistics** command to clear the statistics of the specified RIP process.

Examples # Clear statistics in RIP process 100.

```
<Sysname> reset rip 100 statistics
```

rip

Syntax **rip** [*process-id*]
undo rip [*process-id*]

View System view

Parameters *process-id*: RIP process ID, in the range of 1 to 65535. The default is 1.

Description Use the **rip** command to create a RIP process and enter RIP view.

Use the **undo rip** command to disable a RIP process.

By default, no RIP process runs.

Note that:

- You must enable the RIP process before configuring the global parameters. This limitation is not for configuration of interface parameters.
- The configured interface parameters become invalid after you disable the RIP process.

Examples # Create a RIP process and enter RIP process view.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1]
```

rip authentication-mode

Syntax **rip authentication-mode** { **md5** { **rfc2082** *key-string* *key-id* | **rfc2453** *key-string* } | **simple** *password* }

undo rip authentication-mode

View Interface view

Parameters **md5**: MD5 authentication mode.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

rfc2082: Uses the message format defined in RFC 2082.

key-id: MD5 key number, in the range of 1 to 255.

key-string: MD5 key string with 1 to 16 characters in plain text format, or 24 characters in cipher text format. When the **display current-configuration** command is used to display system information, a 24-character cipher string is displayed as the MD5 key string.

simple: Plain text authentication mode.

password: Plain text authentication string with 1 to 16 characters.

Description Use the **rip authentication-mode** command to configure RIPv2 authentication mode and parameters.

Use the **undo rip authentication-mode** command to cancel authentication.

Note that the key string you configured can overwrite the old one if there is any.

Related commands: **rip version**.

Examples # Configure MD5 authentication on VLAN-interface 10 with the key string being **rose** in the format defined in RFC 2453.

```

<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2
[Sysname-Vlan-interface10] rip authentication-mode md5 rfc2453 rose

```

rip input

Syntax **rip input**
undo rip input

View Interface view

Parameters None

Description Use the **rip input** command to enable the interface to receive RIP messages.
 Use the **undo rip input** command to disable the interface from receiving RIP messages.

By default, an interface is enabled to receive RIP messages.

Related commands: **rip output.**

Examples # Disable VLAN-interface 10 from receiving RIP messages.

```

<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip input

```

rip metricin

Syntax **rip metricin** *value*
undo rip metricin

View Interface view

Parameters *value*: Additional metric added to received routes, in the range of 0 to 16.

Description Use the **rip metricin** command to add a metric to the received routes.

Use the **undo rip metricin** command to restore the default.

By default, the additional metric of a received route is 0.

When a valid RIP route is received, the system adds a metric to it and then installs it into the routing table. Therefore, the metric of routes received on the configured interface is increased.

Related commands: **rip metricout.**

Examples # Configure an additional metric for routes received on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricin 2
```

rip metricout

Syntax **rip metricout** *value*

undo rip metricout

View Interface view

Parameters *value*: Additional metric of sent routes, in the range of 1 to 16.

Description Use the **rip metricout** command to add a metric to a sent route.

Use the **undo rip metricout** command to restore the default.

By default, the additional metric for sent routes is 1.

Before a RIP route is sent, a metric will be added to it. Therefore, when the metric is configured on an interface, the metric of RIP routes sent on the interface will be increased.

Related commands: **rip metricin.**

Examples # Configure an additional metric of 12 for RIP routes sent on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricout 12
```

rip mib-binding

Syntax **rip mib-binding** *process-id*

undo rip mib-binding

View System view

Parameters *process-id*: RIP process ID, in the range of 1 to 65535.

Description Use the **rip mib-binding** command to bind MIB operations with a specified RIP process.

Use the **undo rip mib-binding** command to restore the default.

By default, MIB operations are bound to the RIP process with the smallest process ID.

Examples # Configure RIP 100 to accept SNMP requests.

```
<Sysname> system-view
[Sysname] rip mib-binding 100

# Restore the default.

[Sysname] undo rip mib-binding
```

rip output

Syntax **rip output**
undo rip output

View Interface view

Parameters None

Description Use the **rip output** command to enable the interface to send RIP messages.

Use the **undo rip output** command to disable the interface from sending RIP messages.

Sending RIP messages is enabled on an interface by default.

Related commands: **rip input.**

Examples # Disable VLAN-interface 10 from receiving RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip output
```

rip poison-reverse

Syntax **rip poison-reverse**
undo rip poison-reverse

View Interface view

Parameters **None**

Description Use the **rip poison-reverse** command to enable the poison reverse function.

Use the **undo rip poison-reverse** command to disable the poison reverse function.

By default, the poison reverse function is disabled.

Examples # Enable the poison reverse function for RIP routing updates on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip poison-reverse
```

rip split-horizon

Syntax **rip split-horizon**
undo rip split-horizon

View Interface view

Parameters None

Description Use the **rip split-horizon** command to enable the split horizon function.

Use the **undo rip split-horizon** command to disable the split horizon function.

The split horizon function is enabled by default.

- The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.
- In special cases, make sure it is necessary to disable the split horizon function.



Only the poison reverse function takes effect if both the split horizon and poison reverse functions are enabled.

Examples # Enable the split horizon function on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip split-horizon
```

rip summary-address

Syntax **rip summary-address** *ip-address* { *mask* | *mask-length* }
undo rip summary-address *ip-address* { *mask* | *mask-length* }

View Interface view

Parameters *ip-address*: Summary IP address.

mask: Subnet mask in dotted decimal format.

mask-length: Subnet mask length.

Description Use the **rip summary-address** command to configure RIPv2 to advertise a summary route through the interface.

Use the **undo rip summary-address** command to remove the configuration.

Note that the summary address is valid only when the automatic summarization is disabled.

Related commands: **summary**.

Examples # Advertise a local summary address on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip summary-address 10.0.0.0 255.255.255.0
```

rip version

Syntax **rip version { 1 | 2 [broadcast | multicast] }**

undo rip version

View Interface view

Parameters **1**: RIP version 1.

2: RIP version 2.

broadcast: Sends RIPv2 messages in broadcast mode.

multicast: Sends RIPv2 messages in multicast mode.

Description Use the **rip version** command to specify a RIP version for the interface.

Use the **undo rip version** command to remove the specified RIP version.

By default, no RIP version is configured for an interface, which uses the global RIP version. If the global RIP version is not configured, the interface can only send RIPv1 broadcasts and can receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts and unicasts.

If RIPv2 is specified with no sending mode configured, RIPv2 messages will be sent in multicast mode.

When RIPv1 runs on an interface, the interface will:

- Send RIPv1 broadcast messages
- Receive RIPv1 broadcast messages

- Receive RIPv1 unicast messages

When RIPv2 runs on the interface in broadcast mode, the interface will:

- Send RIPv2 broadcast messages
- Receive RIPv1 broadcast messages
- Receive RIPv1 unicast messages
- Receive RIPv2 broadcast messages
- Receive RIPv2 multicast messages
- Receive RIPv2 unicast messages

When RIPv2 runs on the interface in multicast mode, the interface will:

- Send RIPv2 multicast messages
- Receive RIPv2 broadcast messages
- Receive RIPv2 multicast messages
- Receive RIPv2 unicast messages

Examples # Configure VLAN-interface 10 to broadcast RIPv2 messages.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 10
[Sysname-Vlan-interface10] rip version 2 broadcast
```

silent-interface

Syntax **silent-interface** { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

View RIP view

Parameters **all**: Silents all interfaces.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **silent-interface** command to disable an interface or all interfaces from sending routing updates. That is, the interface only receives but does not send RIP messages.

Use the **undo silent-interface** command to restore the default.

By default, all interfaces are allowed to send routing updates.

Examples # Configure all VLAN interfaces to work in the silent state, and activate VLAN-interface 10.

```
<Sysname> system-view
[Sysname] rip 100
```



```
[Sysname-rip-100] silent-interface all
[Sysname-rip-100] undo silent-interface vlan-interface 10
[Sysname-rip-100] network 131.108.0.0
```

summary

Syntax **summary**

undo summary

View RIP view

Parameters None

Description Use the **summary** command to enable automatic RIPv2 summarization. Natural masks are used to advertise summary routes so as to reduce the size of routing tables.

Use the **undo summary** command to disable automatic RIPv2 summarization so that all subnet routes can be broadcast.

By default, automatic RIPv2 summarization is enabled.

Enabling automatic RIPv2 summarization can reduce the size of the routing table to enhance the scalability and efficiency of large networks.

Related commands: **rip version.**

Examples # Enable RIPv2 automatic summarization.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] summary
```

timers

Syntax **timers** { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* }*

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

View RIP view

Parameters *garbage-collect-value*: Garbage-collect timer time in seconds, in the range of 1 to 3600.

suppress-value: Suppress timer time in seconds, in the range of 0 to 3600.

timeout-value: Timeout timer time in seconds, in the range of 1 to 3600.

update-value: Update timer time in seconds, in the range of 1 to 3600.

Description Use the **timers** command to configure RIP timers. By adjusting RIP timers, you can improve network performance.

Use the **undo timers** command to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIP is controlled by the above four timers.

- The update timer defines the interval between routing updates.
- The timeout timer defines the route aging time. If no routing update related to a route is received after the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines how long a RIP route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no routing update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.

Note that:

- Generally, you are not recommended to change the default values of these timers.
- The time lengths of these timers must be kept consistent on all routers and access servers in the network.

Examples # Specifies the update, timeout, suppress, and garbage-collect timers as 5, 15, 15 and 30 respectively.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] timers update 5
[Sysname-rip-100] timers timeout 15
[Sysname-rip-100] timers suppress 15
[Sysname-rip-100] timers garbage-collect 30
```

validate-source-address

Syntax **validate-source-address**

undo validate-source-address

View RIP view

Parameters None

Description Use the **validate-source-address** command to enable the source IP address validation on incoming RIP routing updates.

Use the **undo validate-source-address** command to disable the source IP address validation.

The source IP address validation is enabled by default.

Generally, disabling the validation is not recommended.

Examples # Enable the source IP address validation on incoming messages.

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] validate-source-address
```

version

Syntax **version { 1 | 2 }**

undo version

View RIP view

Parameters **1**: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2. RIPv2 messages are multicast.

Description Use the **version** command to specify a global RIP version.

Use the **undo version** command to remove the configured global RIP version.

By default, if an interface has a RIP version specified, the RIP version takes effect; if it has no RIP version specified, it can send RIPv1 broadcasts, and receive RIPv1 broadcasts, RIPv1 unicasts, RIPv2 broadcasts, RIPv2 multicasts, and RIPv2 unicasts.

Note that:

- If an interface has an RIP version specified, the RIP version takes precedence over the global RIP version.
- If no RIP version is specified for the interface and the global version is RIPv1, the interface inherits RIPv1, and it can send RIPv1 broadcasts, and receive RIPv1 broadcasts and unicasts.
- If no RIP version is specified for the interface and the global version is RIPv2, the interface operates in the RIPv2 multicast mode, and it can send RIPv2 multicasts, and receive RIPv2 broadcasts, multicasts and unicasts.

Examples # Specify RIPv2 as the global RIP version.

```
<Sysname> system-view  
[Sysname] rip 100  
[Sysname-rip-100] version 2
```

24

OSPF CONFIGURATION COMMANDS



The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running routing protocols.

abr-summary

Syntax **abr-summary** *ip-address* { *mask* | *mask-length* } [**advertise** | **not-advertise**] [**cost** *cost*]

undo abr-summary *ip-address* { *mask* | *mask-length* }

View OSPF area view

Parameters *ip-address*: Destination IP address of the summary route, in dotted decimal format.

mask: Mask of the IP address in dotted decimal format.

mask-length: Mask length, in the range 0 to 32 bits.

advertise | **not-advertise**: Advertises the summary route or not. By default, the summary route is advertised.

cost *cost*: Specifies the cost of the summary route, in the range 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

Description Use the **abr-summary** command to configure a summary route on the area border router.

Use the **undo abr-summary** command to remove a summary route.

By default, no route summarization is configured on an ABR.

You can enable advertising the summary route or not, and specify a route cost.

This command is usable only on an ABR. Multiple contiguous networks may be available in an area, where you can summarize them with one network on the ABR for advertisement. The ABR advertises only the summary route to other areas.

With the **undo abr-summary** command used, summarized routes will be advertised.

Examples # Summarize networks 36.42.10.0/24 and 36.42.110.0/24 in Area 1 with 36.42.0.0/16.

```

<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0

```

area

Syntax `area area-id`

`undo area area-id`

View OSPF view

Parameters *area-id*: ID of an area, a decimal integer in the range 0 to 4294967295 that is translated into the IP address format by the system, or an IP address.

Description Use the **area** command to create an area and enter area view.

Use the **undo area** command to remove a specified area.

No OSPF area is created by default.

Examples # Create Area 0 and enter Area 0 view

```

<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]

```

asbr-summary

Syntax `asbr-summary ip-address { mask | mask-length } [tag tag | not-advertise | cost cost]*`

`undo asbr-summary ip-address { mask | mask-length }`

View OSPF view

Parameters *ip-address*: IP address of the summary route in dotted decimal notation.

mask: IP address mask in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32 bits.

not-advertise: Disables advertising the summary route. If the keyword is not specified, the route is advertised.

tag tag: Specifies a tag value for the summary route, used by a route policy to control route advertisement, in the range 0 to 4294967295. The default is 1.

cost cost: Specifies the cost of the summary route, in the range 1 to 16777214. For Type-1 external routes, the cost defaults to the largest cost among routes that are summarized. For Type-2 external routes, the cost defaults to the largest cost among routes that are summarized plus 1.

Description Use the **asbr-summary** command to configure a summary route.

Use the **undo asbr-summary** command to remove a summary route.

No ASBR route summarization is configured by default.

With the **asbr-summary** command configured on an ASBR, it summarizes redistributed routes that fall into the specified address range with a single route. If the ASBR resides in an NSSA area, it advertises the summary route in a Type-7 LSA into the area.

With the **asbr-summary** command configured on an NSSA ABR, it summarizes routes described by Type-5 LSAs translated from Type-7 LSAs with a single route and advertises the summary route to other areas. This command does not take effect on non NSSA ABRs.

With the **undo asbr-summary** command used, summarized routes will be advertised.

Related command: **display ospf asbr-summary.**

Examples # Summarize redistributed routes with a single route.

```
<Sysname> system-view
[Sysname] ip route-static 10.2.1.0 24 null 0
[Sysname] ip route-static 10.2.2.0 24 null 0
[Sysname] ospf 100
[Sysname-ospf-100] import-route static
[Sysname-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

authentication-mode

Syntax **authentication-mode** { **simple** | **md5** }

undo authentication-mode

View OSPF area view

Parameters **simple:** Specifies the simple authentication mode.

md5: Specifies the MD5 ciphertext authentication mode.

Description Use the **authentication-mode** command to specify an authentication mode for the OSPF area.

Use the **undo authentication-mode** command to remove the authentication mode.

By default, no authentication mode is configured for an OSPF area.

Routers that reside in the same area must have the same authentication mode: non-authentication, simple, or MD5.

Related commands: **ospf authentication-mode.**

Examples # Specify the MD5 ciphertext authentication mode for OSPF area0.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5
```

bandwidth-reference

Syntax **bandwidth-reference** *value*

undo bandwidth-reference

View OSPF view

Parameters *value*: Bandwidth reference value for link cost calculation, in the range 1 to 2147483648 Mbps.

Description Use the **bandwidth-reference** command to specify a reference bandwidth value for link cost calculation.

Use the **undo bandwidth-reference** command to restore the default value.

The default value is 100 Mbps.

When links have no cost values configured, OSPF calculates their cost values: Cost=Reference bandwidth value / Link bandwidth. If the calculated cost is greater than 65535, the value of 65535 is used.

Examples # Specify the reference bandwidth value as 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] bandwidth-reference 1000
```

default

Syntax **default** { **cost** *cost* | **limit** *limit* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **limit** | **tag** | **type** } *

View OSPF view

Parameters *cost*: Specifies the default cost for redistributed routes, in the range 0 to 16777214.

limit: Specifies the default upper limit of routes redistributed per time, in the range 1 to 2147483647.

tag: Specifies the default tag for redistributed routes, in the range 0 to 4294967295.

type: Specifies the default type for redistributed routes: 1 or 2.

Description Use the **default** command to configure default parameters for redistributed routes.

Use the **undo default** command to restore default values.

The cost, route type, tag, and the upper limit are 1, 2, 1 and 1000 by default.

Related commands: **import-route**.

Examples # Configure the default cost, upper limit, tag and type as 10, 20000, 100 and 2 respectively for redistributed external routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default cost 10 limit 20000 tag 100 type 2
```

default-cost

Syntax **default-cost** *cost*
undo default-cost

View OSPF area view

Parameters *cost*: Specifies a cost for the default route advertised to the Stub or NSSA area, in the range 0 to 16777214.

Description Use the **default-cost** command to specify a cost for the default route advertised to the stub or NSSA area.

Use the **undo default-cost** command to restore the default value.

The cost defaults to 1.

This command is only applicable to the ABR of a stub area or the ABR/ASBR of an NSSA area.

Related commands: **stub**, **nssa**.

Examples # Configure Area 1 as a stub area, and specify the cost of the default route advertised to the stub area as 20.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
[Sysname-ospf-100-area-0.0.0.1] default-cost 20
```

default-route-advertise

Syntax **default-route-advertise** [[**always** | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name*] * | **summary** **cost** *cost*]

undo default-route-advertise

View OSPF view

Parameters **always**: If the local routing table has no default route, using this keyword generates a default route in an ASE LSA into the OSPF routing domain. Without this keyword used, the router can generate the default route only when the local routing table has a default route.

cost *cost*: Specifies a cost for the default route, in the range 0 to 16777214. The default is 1.

type *type*: Specifies a type for the ASE LSA: 1 or 2, which defaults to 2.

route-policy *route-policy-name*: Specifies a route policy name, a string of 1 to 19 characters. If the default route matches the specified route policy, the route policy modifies some values in the ASE LSA.

summary: Advertises the Type-3 summary LSA of the specified default route.

Description Use the **default-route-advertise** command to generate a default route into the OSPF routing domain.

Use the **undo default-route-advertise** command to disable OSPF from distributing a default external route.

By default, no default route is distributed.

Using the **import-route** command cannot redistribute a default route. To do so, use the **default-route-advertise** command. If no default route is available in the local routing table, the **always** keyword should be included to generate a default route in a Type-5 LSA.

The **default-route-advertise summary cost** command is applicable only to VPNs, and the default route is redistributed in a Type-3 LSA. The PE router advertises the redistributed default route to the CE router. Currently, this command is not supported on switches.

Related commands: **import-route.**

Examples # Generate a default route in an ASE LSA into the OSPF routing domain (no default route is available in the local routing table).

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default-route-advertise always
```

description

Syntax **description** *description*

undo description

View OSPF view/OSPF area view

Parameters *description*: Configures a description for the OSPF process in OSPF view, or for the OSPF area in OSPF area view. *description* is a string of up to 80 characters.

Description Use the **description** command to configure a description for an OSPF process or area.

Use the **undo description** command to remove the description.

No description is configured by default.

Use of this command is only for the identification of an OSPF process or area. The description has no special meaning.

Examples # Describe the OSPF process 100 as **abc**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] description abc
```

Describe the OSPF area0 as **bone area**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] description bone area
```

display ospf abr-asbr

Syntax **display ospf** [*process-id*] **abr-asbr**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf abr-asbr** command to display ABR/ASBR information.

If no process is specified, the ABR/ASBR information of all OSPF processes is displayed.

If you use this command on routers in a stub area, no ASBR information is displayed.

Examples # Display ABR/ASBR information.

```
<Sysname> display ospf abr-asbr
```

```
OSPF Process 1 with Router ID 192.168.1.2
Routing Table to ABR and ASBR
```

| Type | Destination | Area | Cost | Nexthop | RtType |
|-------|-------------|---------|------|----------|--------|
| Inter | 3.3.3.3 | 0.0.0.0 | 3124 | 10.1.1.2 | ASBR |
| Intra | 2.2.2.2 | 0.0.0.0 | 1562 | 10.1.1.2 | ABR |

Table 66 Field descriptions of the display ospf abr-asbr command

| Field | Description |
|-------------|--|
| Type | Intra-area router or Inter-area router |
| Destination | Router ID of an ABR/ASBR |
| Area | ID of the area of the next hop |
| Cost | Cost from the router to the ABR/ASBR |
| Nexthop | Next hop address |
| RtType | Router type: ABR, ASBR |

display ospf asbr-summary

Syntax **display ospf** [*process-id*] **asbr-summary** [*ip-address* { *mask* | *mask-length* }]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

ip-address: IP address, in dotted decimal format.

mask: IP address mask, in dotted decimal format.

mask-length: Mask length, in the range 0 to 32 bits.

Description Use the **display ospf asbr-summary** command to display information about the redistributed routes that are summarized.

If no OSPF process is specified, related information of all OSPF processes is displayed.

If no IP address is specified, information about all summarized redistributed routes will be displayed.

Related commands: **asbr-summary**.

Examples # Display information about all summarized redistributed routes.

```
<Sysname> display ospf asbr-summary
```

```
OSPF Process 1 with Router ID 2.2.2.2
Summary Addresses
```

```
Total Summary Address Count: 1
```

```
Summary Address
```

```
Net          : 30.1.0.0
Mask         : 255.255.0.0
Tag          : 20
Status       : Advertise
Cost         : 10 (Configured)
The Count of Route is : 2
```

| Destination | Net Mask | Proto | Process | Type | Metric |
|-------------|---------------|-------|---------|------|--------|
| 30.1.2.0 | 255.255.255.0 | OSPF | 1 | 2 | 1 |
| 30.1.1.0 | 255.255.255.0 | OSPF | 1 | 2 | 1 |

Table 67 Field descriptions of the display ospf asbr-summary command

| Field | Description |
|-----------------------------|---|
| Total Summary Address Count | Total summary route number |
| Net | The address of the summary route |
| Mask | The mask of the summary route address |
| Tag | The tag of the summary route |
| Status | The advertisement status of the summary route |
| Cost | The cost to the summary net |
| The Count of Route | The count of routes that are summarized |
| Destination | Destination address of a summarized route |
| Net Mask | Network mask of a summarized route |
| Proto | Routing protocol |
| Process | Process ID of routing protocol |
| Type | Type of a summarized route |
| Metric | Metric of a summarized route |

display ospf brief

Syntax **display ospf** [*process-id*] **brief**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf brief** command to display OSPF brief information. If no OSPF process is specified, brief information about all OSPF processes is displayed.

Examples # Display OSPF brief information.

```

<Sysname> display ospf brief

                OSPF Process 1 with Router ID 192.168.1.2
                  OSPF Protocol Information

RouterID: 192.168.1.2      Border Router:  NSSA
Route Tag: 0
Multi-VPN-Instance is not enabled
Applications Supported: MPLS Traffic-Engineering
SPF-schedule-interval: 5 0 5000
LSA generation interval: 5 0 5000
LSA arrival interval: 1000
Default ASE Parameter: Metric: 1 Tag: 1 Type: 2
Route Preference: 10
ASE Route Preference: 150
SPF Computation Count: 22
RFC 1583 Compatible
Graceful restart interval: 120
Area Count: 1  Nssa Area Count: 1
ExChange/Loading Neighbors: 0

Area: 0.0.0.1            (MPLS TE  not enabled)
Authtype: None Area flag: NSSA
SPF Scheduled Count: 5
ExChange/Loading Neighbors: 0

Interface: 192.168.1.2 (Vlan-interfacel)
Cost: 1      State: DR      Type: Broadcast      MTU: 1500
Priority: 1
Designated Router: 192.168.1.2
Backup Designated Router: 192.168.1.1
Timers: Hello 10 , Dead 40 , Poll 40 , Retransmit 5 , Transmit Delay 1

```

Table 68 Field descriptions of the display ospf brief command

| Field | Description |
|-----------------------------------|---|
| RouterID | Router ID |
| Border Router | ABR, ASBR or NSSA ABR |
| Route Tag | The tag of redistributed routes |
| Multi-VPN-Instance is not enabled | The OSPF process does not support multi-VPN-instance. |
| Applications Supported | Applications supported |
| SPF-schedule-interval | Interval for SPF calculations |
| LSA generation interval | LSA generation interval |
| LSA arrival interval | Minimum LSA repeat arrival interval |
| Default ASE Parameter | Default ASE Parameters: metric, tag, route type. |
| Route Preference | Internal route priority |
| ASE Route Preference | External route priority |
| SPF Computation count | SPF computation count of the OSPF process |
| RFC1583 Compatible | Compatible with routing rules defined in RFC1583 |
| Graceful restart interval | GR restart interval |
| Area Count | Area number of the current process |
| Nssa Area Count | NSSA area number of the current process |
| ExChange/Loading Neighbors | Neighbors in ExChange/Loading state |
| Area | Area ID in the IP address format |
| Authtype | Authentication type of the area: Non-authentication, simple authentication, or MD5 authentication |

Table 68 Field descriptions of the display ospf brief command

| Field | Description |
|--------------------------|--|
| Area flag | The type of the area |
| SPF scheduled Count | SPF calculation count in the OSPF area |
| Interface | IP address of the interface |
| Cost | Interface cost |
| State | Interface state |
| Type | Interface network type |
| MTU | Interface MTU |
| Priority | Router priority |
| Designated Router | The Designated Router |
| Backup Designated Router | The Backup Designated Router |
| Timers | Intervals of timers: hello, dead, poll, retransmit, and transmit delay |

display ospf cumulative

Syntax `display ospf [process-id] cumulative`

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf cumulative** command to display OSPF statistics.
Use of this command is helpful for troubleshooting.

Examples # Display OSPF statistics.

```
<Sysname> display ospf cumulative
          OSPF Process 1 with Router ID 2.2.2.2
          Cumulations

          IO Statistics
                Type           Input      Output
                Hello          61         122
          DB Description          2          3
                Link-State Req    1          1
Link-State Update          3          3
                Link-State Ack    3          2

          LSAs originated by this router
Router: 4
Network: 0
Sum-Net: 0
Sum-Asbr: 0
External: 0
NSSA: 0
Opq-Link: 0
Opq-Area: 0
```

```

Opq-As: 0

LSAs Originated: 4  LSAs Received: 7

Routing Table:
  Intra Area: 2  Inter Area: 3  ASE/NSSA: 0

```

Table 69 Field descriptions of the display ospf cumulative command

| Field | Description |
|--------------------------------|--|
| IO statistics | Statistics about input/output packets and LSAs |
| Type | OSPF packet type |
| Input | Packets received |
| Output | Packets sent |
| Hello | Hell packet |
| DB Description | Database Description packet |
| Link-State Req | Link-State Request packet |
| Link-State Update | Link-State Update packet |
| Link-State Ack | Link-State Acknowledge packet |
| LSAs originated by this router | LSAs originated by this router |
| Router | Type-1 LSA |
| Network | Type-2 LSA |
| Sum-Net | Type-3 LSA |
| Sum-Asbr | Type-4 LSA |
| External | Type-5 LSA |
| NSSA | Type-7 LSA |
| Opq-Link | Type-9 LSA |
| Opq-Area | Type-10 LSA |
| Opq-As | Type-11 LSA |
| LSAs originated | LSAs originated |
| LSAs Received | LSAs received |
| Routing Table | Routing table |
| Intra Area | Intra-area route number |
| Inter Area | Inter-area route number |
| ASE | ASE route number |

display ospf error

Syntax `display ospf [process-id] error`

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf error** command to display OSPF error information.

If no process is specified, the OSPF error information of all OSPF processes is displayed.

Examples # Display OSPF error information.

```
<Sysname> display ospf error
```

```
OSPF Process 1 with Router ID 192.168.80.100
OSPF Packet Error Statistics
```

```
0 : OSPF Router ID confusion      0 : OSPF bad packet
0 : OSPF bad version              0 : OSPF bad checksum
0 : OSPF bad area ID              0 : OSPF drop on unnumber interface
0 : OSPF bad virtual link         0 : OSPF bad authentication type
0 : OSPF bad authentication key   0 : OSPF packet too small
0 : OSPF Neighbor state low       0 : OSPF transmit error
0 : OSPF interface down           0 : OSPF unknown neighbor
0 : HELLO: Netmask mismatch       0 : HELLO: Hello timer mismatch
0 : HELLO: Dead timer mismatch   0 : HELLO: Extern option mismatch
0 : HELLO: NBMA neighbor unknown 0 : DD: MTU option mismatch
0 : DD: Unknown LSA type          0 : DD: Extern option mismatch
0 : LS ACK: Bad ack               0 : LS ACK: Unknown LSA type
0 : LS REQ: Empty request         0 : LS REQ: Bad request
0 : LS UPD: LSA checksum bad      0 : LS UPD: Received less recent LSA
0 : LS UPD: Unknown LSA type
```

Table 70 Field descriptions of the display ospf error command

| Field | Description |
|---------------------------------|--|
| OSPF Router ID confusion | Packets with duplicate route ID |
| OSPF bad packet | Packets illegal |
| OSPF bad version | Packets with wrong version |
| OSPF bad checksum | Packets with wrong checksum |
| OSPF bad area ID | Packets with invalid area ID |
| OSPF drop on unnumber interface | Packets dropped on the unnumbered interface |
| OSPF bad virtual link | Packets on wrong virtual links |
| OSPF bad authentication type | Packets with invalid authentication type |
| OSPF bad authentication key | Packets with invalid authentication key |
| OSPF packet too small | Packets too small in length |
| OSPF Neighbor state low | Packets received in low neighbor state |
| OSPF transmit error | Packets with error when being transmitted |
| OSPF interface down | Shutdown times of the interface |
| OSPF unknown neighbor | Packets received from unknown neighbors |
| HELLO: Netmask mismatch | Hello packets with mismatched mask |
| HELLO: Hello timer mismatch | Hello packets with mismatched hello timer |
| HELLO: Dead timer mismatch | Hello packets with mismatched dead timer |
| HELLO: Extern option mismatch | Hello packets with mismatched option field |
| HELLO: NBMA neighbor unknown | Hello packets received from unknown NBMA neighbors |
| DD: MTU option mismatch | DD packets with mismatched MTU |
| DD: Unknown LSA type | DD packets with unknown LSA type |
| DD: Extern option mismatch | DD packets with mismatched option field |
| LS ACK: Bad ack | Bad LSack packets for LSU packets |
| LS ACK: Unknown LSA type | LSack packets with unknown LSA type |

Table 70 Field descriptions of the display ospf error command

| Field | Description |
|----------------------------------|---|
| LS REQ: Empty request | LSR packets with no request information |
| LS REQ: Bad request | Bad LSR packets |
| LS UPD: LSA checksum bad | LSU packets with wrong LSA checksum |
| LS UPD: Received less recent LSA | LSU packets without latest LSA |
| LS UPD: Unknown LSA type | LSU packets with unknown LSA type |

display ospf interface

Syntax `display ospf [process-id] interface [all | interface-type interface-number]`

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

all: Display the OSPF information of all interfaces.

interface-type interface-number: Interface type and interface number.

Description Use the **display ospf interface** command to display OSPF interface information.

If no OSPF process is specified, the OSPF interface information of all OSPF processes is displayed.

Examples # Display OSPF interface information.

```
<Sysname> display ospf interface
```

```
OSPF Process 1 with Router ID 192.168.1.1
  Interfaces
```

```
Area: 0.0.0.0
```

| IP Address | Type | State | Cost | Pri | DR | BDR |
|-------------|------|-------|------|-----|---------|---------|
| 192.168.1.1 | PTP | P-2-P | 1562 | 1 | 0.0.0.0 | 0.0.0.0 |

```
Area: 0.0.0.1
```

| IP Address | Type | State | Cost | Pri | DR | BDR |
|------------|-----------|-------|------|-----|------------|---------|
| 172.16.0.1 | Broadcast | DR | 1 | 1 | 172.16.0.1 | 0.0.0.0 |

Table 71 Field descriptions of the display ospf interface command

| Field | Description |
|------------|---|
| Area | Area ID of the interface |
| IP address | Interface IP address (regardless of whether TE is enabled or not) |
| Type | Interface network type: PTP, PTMP, Broadcast, or NBMA |
| State | Interface state defined by interface state machine: DOWN, Waiting, p-2-p, DR, BDR, or DROther |
| Cost | Interface cost |
| Pri | Router priority |
| DR | The DR on the interface's network segment |

Table 71 Field descriptions of the display ospf interface command

| Field | Description |
|-------|--|
| BDR | The BDR on the interface's network segment |

display ospf lsdb

Syntax **display ospf** [*process-id*] **lsdb** [**brief** | [{ **ase** | **router** | **network** | **summary** | **asbr** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as** } [*link-state-id*]] [**originate-router** *advertising-router-id* | **self-originate**]]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

brief: Displays brief LSDB information.

ase: Displays Type-5 LSA (AS External LSA) information in the LSDB.

router: Displays Type-1 LSA (Router LSA) information in the LSDB.

network: Displays Type-2 LSA (Network LSA) information in the LSDB.

summary: Displays Type-3 LSA (Network Summary LSA) information in the LSDB.

asbr: Displays Type-4 LSA (ASBR Summary LSA) information in the LSDB.

nssa: Displays Type-7 LSA (NSSA External LSA) information in the LSDB.

opaque-link: Displays Type-9 LSA (Opaque-link LSA) information in the LSDB.

opaque-area: Displays Type-10 LSA (Opaque-area LSA) information in the LSDB.

opaque-as: Displays Type-11 LSA (Opaque-AS LSA) information in the LSDB.

link-state-id: Link state ID, in the IP address format.

originate-router *advertising-router-id*: Displays information about LSAs originated by the specified router.

self-originate: Displays information about self-originated LSAs.

Description Use the **display ospf lsdb** command to display LSDB information.

If no OSPF process is specified, LSDB information of all OSPF processes is displayed.

Examples # Display OSPF LSDB information.

```
<Sysname> display ospf lsdb
      OSPF Process 1 with Router ID 192.168.0.1
      Link State Database

                Area: 0.0.0.0
Type          LinkState ID      AdvRouter          Age Len  Sequence  Metric
```

| | | | | | | |
|---------------|--------------|-------------|-----|-----|----------|--------|
| Router | 192.168.0.2 | 192.168.0.2 | 474 | 36 | 80000004 | 0 |
| Router | 192.168.0.1 | 192.168.0.1 | 21 | 36 | 80000009 | 0 |
| Network | 192.168.0.1 | 192.168.0.1 | 321 | 32 | 80000003 | 0 |
| Sum-Net | 192.168.1.0 | 192.168.0.1 | 321 | 28 | 80000002 | 1 |
| Sum-Net | 192.168.2.0 | 192.168.0.2 | 474 | 28 | 80000002 | 1 |
| Area: 0.0.0.1 | | | | | | |
| Type | LinkState ID | AdvRouter | Age | Len | Sequence | Metric |
| Router | 192.168.0.1 | 192.168.0.1 | 21 | 36 | 80000005 | 0 |
| Sum-Net | 192.168.2.0 | 192.168.0.1 | 321 | 28 | 80000002 | 2 |
| Sum-Net | 192.168.0.0 | 192.168.0.1 | 321 | 28 | 80000002 | 1 |

Table 72 Field descriptions of the display ospf lsdb command

| Field | Description |
|--------------|------------------------------------|
| Area | Area |
| Type | LSA type |
| LinkState ID | Linkstate ID |
| AdvRouter | The router that advertised the LSA |
| Age | Age of the LSA |
| Len | Length of the LSA |
| Sequence | Sequence number of the LSA |
| Metric | Cost of the LSA |

Display Type2 LSA (Network LSA) information in the LSDB.

[Sysname] display ospf 1 lsdb network

```

OSPF Process 1 with Router ID 192.168.1.1
      Area: 0.0.0.0
      Link State Database
    
```

```

Type      : Network
LS ID     : 192.168.0.2
Adv Rtr   : 192.168.2.1
LS Age    : 922
Len       : 32
Options   : E
Seq#      : 80000003
Chksum    : 0x8d1b
Net Mask  : 255.255.255.0
  Attached Router 192.168.1.1
  Attached Router 192.168.2.1
    
```

Table 73 Field descriptions of the display ospf 1 lsdb network command

| Field | Description |
|---------|--------------------------------|
| Type | LSA type |
| LS ID | DR IP address |
| Adv Rtr | Router that advertised the LSA |
| LS Age | LSA age time |
| Len | LSA length |
| Options | LSA options |
| Seq# | LSA sequence number |
| Chksum | LSA checksum |

Table 73 Field descriptions of the display ospf 1 lsdb network command

| Field | Description |
|-----------------|--|
| Net Mask | Network mask |
| Attached Router | ID of the router that established adjacency with the DR, and ID of the DR itself |

display ospf nexthop

Syntax **display ospf** [*process-id*] **nexthop**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf nexthop** command to display OSPF next hop information. If no OSPF process is specified, the next hop information of all OSPF processes is displayed.

Examples # Display OSPF next hop information.

```
<Sysname> display ospf nexthop
      OSPF Process 1 with Router ID 192.168.0.1
      Routing Nexthop Information
```

```
Next Hops:
```

| Address | Refcount | IntfAddr | Intf Name |
|-------------|----------|-------------|------------------|
| 192.168.0.1 | 1 | 192.168.0.1 | Vlan-interface1 |
| 192.168.0.2 | 1 | 192.168.0.1 | Vlan-interface1 |
| 192.168.1.1 | 1 | 192.168.1.1 | Vlan-interface10 |

Table 74 Field descriptions of the display ospf nexthop command

| Field | Description |
|-----------|---|
| Next hops | Information about Next hops |
| Address | Next hop address |
| Refcount | Reference count, namely, routes that reference the next hop |
| IntfAddr | Outbound interface address |
| Intf Name | Outbound interface name |

display ospf peer

Syntax **display ospf** [*process-id*] **peer** [**verbose**] [*interface-type interface-number*] [*neighbor-id*]]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

verbose: Displays detailed neighbor information.

interface-type interface-number: Interface type and interface number.

neighbor-id: Neighbor router ID.

Description Use the **display ospf peer** command to display information about OSPF neighbors.

Note that:

If no OSPF process is specified, OSPF neighbor information of all OSPF processes is displayed.

If an interface is specified, the neighbor on the interface is displayed.

If a neighbor ID is specified, detailed information about the neighbor is displayed,

If neither interface nor neighbor ID is specified, brief information about neighbors of the specified OSPF process or all OSPF processes is displayed.

Examples # Display detailed OSPF neighbor information.

```
<Sysname> display ospf peer verbose
```

```
OSPF Process 1 with Router ID 192.168.0.138
Neighbors
```

```
Area 0.0.0.1 interface 192.168.0.138(Vlan-interface1)'s neighbors
Router ID: 192.168.0.136   Address: 192.168.0.136   GR State: Normal
State: Full Mode: Nbr is Slave Priority: 1
DR: 192.168.0.138 BDR: 192.168.0.136 MTU: 0
Dead timer due in 40 sec
Neighbor is up for 00:12:59
Authentication Sequence: [ 0 ]
Neighbor state change count: 5
```

Table 75 Field descriptions of the display ospf peer verbose command

| Field | Description |
|-----------------------------|--|
| Router ID | Neighbor router ID |
| Address | Neighbor router address |
| GR State | GR state |
| State | Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading or Full |
| Mode | Neighbor mode for DD exchange: master or slave |
| Priority | Router priority |
| DR | The DR on the interface's network segment |
| BDR | The BDR on the interface's network segment |
| MTU | Interface MTU |
| Dead timer due in 40 sec | Dead timer times out in 40 seconds |
| Neighbor is up for 00:12:59 | The neighbor has been up for 00:12:59 |
| Authentication Sequence | Authentication sequence number |
| Neighbor state change count | Count of neighbor state changes |

Display brief OSPF neighbor information.

```
<Sysname> display ospf peer
```

```
OSPF Process 1 with Router ID 192.168.0.138
Neighbor Brief Information
```

```
Area: 0.0.0.1
Router ID      Address          Pri Dead-Time Interface      State
192.168.0.136 192.168.0.136   1   37          Vlan1           Full/BDR
```

Table 76 Field descriptions of the display ospf peer command

| Field | Description |
|--------------|--|
| Area | Neighbor area |
| Router ID | Neighbor router ID |
| Address | Neighbor interface address |
| Pri | Router priority |
| Dead time(s) | Dead interval remained |
| Interface | Interface connected to the neighbor |
| State | Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading or Full |

display ospf peer statistics

Syntax `display ospf [process-id] peer statistics`

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf peer statistics** command to display OSPF neighbor statistics.

If no OSPF process is specified, OSPF neighbor statistics of all OSPF processes is displayed.

Examples # Display OSPF neighbor statistics.

```
<Sysname> display ospf peer statistics
OSPF Process 1 with Router ID 1.1.1.1
Neighbor Statistics

Area ID      Down  Attempt  Init  2-Way  ExStart  Exchange  Loading  Full  Total
0.0.0.1      0     0         0     0     0     0         0         0     1     1
Total        0     0         0     0     0     0         0         0     1     1
```

Table 77 Field descriptions of the display ospf peer statistics command

| Field | Description |
|---------|---|
| Area ID | Area ID |
| Down | Under this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time. |

Table 77 Field descriptions of the display ospf peer statistics command

| Field | Description |
|----------|---|
| Attempt | Available only in an NBMA network, such as Frame Relay, X.25 or ATM. Under this state, the OSPF router has not received any information from a neighbor for a period but can send Hello packets with a longer interval to keep neighbor relationship. |
| Init | Under this state, the router has received a hello packet from a neighbor but the packet contains no IP address of itself, so mutual communication is not established. |
| 2-Way | Indicates mutual communication between the router and its neighbor is established. DR/BDR election is finished under this state (or higher). |
| ExStart | Under this state, the router decides on sequence numbers for DD packets. |
| Exchange | Under this state, the router exchanges link state information with the neighbor. |
| Loading | Under this state, the router requests the neighbor for needed LSAs. |
| Full | Indicates LSDB synchronization has been accomplished between neighbors. |
| Total | Total number of neighbors under the same state |

display ospf request-queue

Syntax **display ospf** [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

interface-type interface-number: Interface type and number.

neighbor-id: Neighbor's router ID.

Description Use the **display ospf request-queue** command to display OSPF request queue information.

If no OSPF process is specified, the OSPF request queue information of all OSPF processes is displayed.

Examples # Display OSPF request queue information.

```
<Sysname> display ospf request-queue
```

```

      OSPF Process 1 with Router ID 1.1.1.1
      OSPF Request List

The Router's Neighbor is Router ID 2.2.2.2      Address 10.1.1.2
Interface 10.1.1.1      Area 0.0.0.0
Request list:
  Type      LinkState ID      AdvRouter      Sequence      Age
  Router    2.2.2.2            1.1.1.1        80000004      1
  Network   192.168.0.1        1.1.1.1        80000003      1
  Sum-Net   192.168.1.0        1.1.1.1        80000002      2

```


Table 78 Field descriptions of the display ospf request queue command

| Field | Description |
|------------------------------------|-------------------------------|
| The Router's Neighbor is Router ID | Neighbor router ID |
| Address | Neighbor interface IP address |
| Interface | Local interface IP address |
| Area | Area ID |
| Request list | Request list information |
| Type | LSA type |
| LinkState ID | Link state ID |
| AdvRouter | Advertising router |
| Sequence | LSA sequence number |
| Age | LSA age |

display ospf retrans-queue

Syntax **display ospf** [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.
interface-type interface-number: Interface type and interface number.
neighbor-id: Neighbor's router ID.

Description Use the **display ospf retrans-queue** command to display retransmission queue information.

If no OSPF process is specified, the retransmission queue information of all OSPF processes is displayed.

Examples # Display OSPF retransmission queue information.

```
<Sysname> display ospf retrans-queue

          OSPF Process 1 with Router ID 1.1.1.1
          OSPF Retransmit List

The Router's Neighbor is Router ID 2.2.2.2      Address 10.1.1.2
Interface 10.1.1.1          Area 0.0.0.0
Retransmit list:
  Type      LinkState ID      AdvRouter      Sequence      Age
  Router    2.2.2.2                  2.2.2.2        80000004      1
  Network   12.18.0.1                 2.2.2.2        80000003      1
  Sum-Net   12.18.1.0                 2.2.2.2        80000002      2
```

Table 79 Field descriptions of the display ospf retrans-queue command

| Field | Description |
|------------------------------------|--------------------|
| The Router's Neighbor is Router ID | Neighbor router ID |

Table 79 Field descriptions of the display ospf retrans-queue command

| Field | Description |
|-----------------|---------------------------------|
| Address | Neighbor interface IP address |
| Interface | Interface address of the router |
| Area | Area ID |
| Retransmit list | Retransmission list |
| Type | LSA type |
| LinkState ID | Link state ID |
| AdvRouter | Advertising router |
| Sequence | LSA sequence number |
| Age | LSA age |

display ospf routing

Syntax **display ospf** [*process-id*] **routing** [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

interface *interface-type interface-number*: Displays OSPF routing information advertised via the interface.

nexthop *nexthop-address*: Displays OSPF routing information with the specified next hop.

Description Use the **display ospf routing** command to display OSPF routing information.

If no OSPF process is specified, the routing information of all OSPF processes is displayed.

Examples # Display OSPF routing information.

```
<Sysname> display ospf routing
```

```
OSPF Process 1 with Router ID 192.168.1.2
Routing Tables
```

```
Routing for Network
```

| Destination | Cost | Type | NextHop | AdvRouter | Area |
|----------------|------|-------|-------------|-------------|---------|
| 192.168.1.0/24 | 1562 | stub | 192.168.1.2 | 192.168.1.2 | 0.0.0.0 |
| 172.16.0.0/16 | 1563 | Inter | 192.168.1.1 | 192.168.1.1 | 0.0.0.0 |

```
Total Nets: 2
```

```
Intra Area: 1 Inter Area: 1 ASE: 0 NSSA: 0
```

Table 80 Field descriptions of the display ospf routing command

| Field | Description |
|-------------|---------------------|
| Destination | Destination network |
| Cost | Cost to destination |

Table 80 Field descriptions of the display ospf routing command

| Field | Description |
|------------|--|
| Type | Route type: intra-area, transit, stub, inter-area, type1 external, type2 external. |
| NextHop | Next hop address |
| AdvRouter | Advertising router |
| Area | Area ID |
| Total Nets | Total networks |
| Intra Area | Total intra-area routes |
| Inter Area | Total inter-area routes |
| ASE | Total ASE routes |
| NSSA | Total NSSA routes |

display ospf vlink

Syntax `display ospf [process-id] vlink`

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf vlink** command to display OSPF virtual link information.

If no OSPF process is specified, the OSPF virtual link information of all OSPF processes is displayed.

Examples # Display OSPF virtual link information.

```
<Sysname> display ospf vlink
          OSPF Process 1 with Router ID 3.3.3.3
          Virtual Links

Virtual-link Neighbor-ID -> 2.2.2.2, Neighbor-State: Full
Interface: 10.1.2.1 (Vlan-interfacel)
Cost: 1 State: P-2-P Type: Virtual
Transit Area: 0.0.0.1
Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

Table 81 Field descriptions of the display ospf vlink command

| Field | Description |
|--------------------------|---|
| Virtual-link Neighbor-id | ID of the neighbor connected to the router via the virtual link |
| Neighbor-State | Neighbor State: Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, Full. |
| Interface | Local interface's IP address and name of the virtual link |
| Cost | Interface route cost |
| State | Interface state |
| Type | Type: virtual link |
| Transit Area | Transit area ID |

Table 81 Field descriptions of the display ospf vlink command

| Field | Description |
|--------|--|
| Timers | Values of timers: hello, dead, poll (NBMA), retransmit, and interface transmission delay |

enable log

Syntax `enable log [config | error | state]`

`undo enable log [config | error | state]`

View OSPF view

Parameters **config**: Enables configuration logging.

error: Enables error logging.

state: Enables state logging.

Description Use the **enable** command to enable specified OSPF logging.

Use the **undo enable** command to disable specified OSPF logging.

OSPF logging is disabled by default.

If no keyword is specified, all logging is enabled.

Examples # Enable OSPF logging.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] enable log
```

filter

Syntax `filter { acl-number | ip-prefix ip-prefix-name } { import | export }`

`undo filter { import | export }`

View OSPF area view

Parameters *acl-number*: ACL number, in the range 2000 to 3999.

ip-prefix-name: IP prefix list name, a string of up to 19 characters.

import: Filters incoming LSAs.

export: Filters outgoing LSAs.

Description Use the **filter** command to configure incoming/outgoing summary LSAs filtering on an ABR.

Use the **undo filter** command to disable summary LSA filtering.

By default, summary LSAs filtering is disabled.



This command is only available on an ABR.

Examples # Apply IP prefix list **my-prefix-list** to filter inbound Type-3 LSAs, and apply ACL 2000 to filter outbound Type-3 LSAs in OSPF Area 1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] filter ip-prefix my-prefix-list import
[Sysname-ospf-100-area-0.0.0.1] filter 2000 export
```

filter-policy export

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

View OSPF view

Parameters *acl-number*: Number of an ACL used to filter outgoing redistributed routes, in the range 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter outgoing redistributed routes, a string of up to 19 characters.

protocol: Specifies a protocol from which to filter redistributed routes. The protocol can be **direct**, **static**, **rip**, **ospf**, **isis** or **bgp**. If no protocol is specified, all redistributed routes are filtered.

process-id: Process ID, which is required when the *protocol* is **rip**, **ospf** or **isis**, in the range 1 to 65535.

Description Use the **filter-policy export** command to configure the filtering of outgoing redistributed routes.

Use the **undo filter-policy export** command to disable the filtering.

By default, the filtering of outgoing redistributed routes is not configured.

You can use this command to filter outgoing redistributed routes as needed.

Related commands: **import-route**.

Examples # Filter outgoing redistributed routes using ACL2000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 export
```

filter-policy import

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* }
import

undo filter-policy import

View OSPF view

Parameters *acl-number*: Number of an ACL used to filter incoming routes, in the range 2000 to 3999.

ip-prefix-name: Name of an IP address prefix list used to filter incoming routes, a string of up to 19 characters.

gateway *ip-prefix-name*: Name of an IP address prefix list used to filter routes from the specified neighbors, a string of up to 19 characters.

Description Use the **filter-policy import** command to configure the filtering of routes calculated from received LSAs.

Use the **undo filter-policy import** command to disable the filtering.

By default, the filtering is not configured.

Examples # Filter incoming routes using ACL2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 import
```

host-advertise

Syntax **host-advertise** *ip-address cost*

undo host-advertise *ip-address*

View OSPF area view

Parameters *ip-address*: IP address of a host

cost: Cost of the route, in the range 1 to 65535.

Description Use the **host-advertise** command to advertise a host route.

Use the **undo host-advertise** command to remove a host route.

No host route is advertised by default.

Examples # Advertise the host route 1.1.1.1 with a cost of 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] host-advertise 1.1.1.1 100
```

import-route

Syntax **import-route** *protocol* [*process-id* | **allow-ibgp**] [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*]*

undo import-route *protocol* [*process-id*]

View OSPF view

Parameters *protocol*: Redistributes routes from the protocol, which can be **direct**, **static**, **rip**, **ospf**, **isis** or **bgp**.

process-id: Process ID, which is optional when the *protocol* is **rip**, **ospf** or **isis**, in the range 1 to 65535.

allow-ibgp: Allows IBGP routes redistribution. It is optional only when the *protocol* is **bgp**.

cost *cost*: Specifies a route cost, in the range 0 to 16777214. The default is 1.

type *type*: Specifies a cost type, 1 or 2. The default is 2.

tag *tag*: Specifies a tag for external LSAs. The default is 1.

route-policy *route-policy-name*: Specifies a route policy to redistribute qualified routes only. A Route policy name is a string of up to 19 characters.

Description Use the **import-route** command to redistribute routes from another protocol.

Use the **undo import-route** command to disable route redistribution from a protocol.

Route redistribution from another protocol is not configured by default.

OSPF prioritize routes as follows:

- Intra-area route
- Inter-area route
- Type1 External route

- Type2 External route

An intra-area route is a route in an OSPF area. An inter-area route is between any two OSPF areas. Both of them are internal routes.

An external route is a route to a destination outside the OSPF AS.

A Type-1 external route is an IGP route, such as RIP or STATIC, which has high reliability and whose cost is comparable with the cost of OSPF internal routes. Therefore, the cost from an OSPF router to a Type-1 external route's destination equals the cost from the router to the corresponding ASBR plus the cost from the ASBR to the external route's destination.

A Type-2 external route is an EGP route, which has low credibility, so OSPF considers the cost from the ASBR to a Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. Therefore, the cost from an internal router to a Type-2 external route's destination equals the cost from the ASBR to the Type-2 external route's destination.

Related commands: **default-route-advertise.**



- The **import-route** command cannot redistribute **default** routes.
- Use the **import-route bgp allow-ibgp** command with care, because it redistributes both EBGP and IBGP routes that may cause routing loops.

Examples # Redistribute routes from RIP process 40 and specify the type, tag, and cost as 2, 33 and 50 for redistributed routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

log-peer-change

Syntax **log-peer-change**

undo log-peer-change

View OSPF view

Parameters None

Description Use the **log-peer-change** command to enable the logging of OSPF neighbor state changes.

Use the **undo log-peer-change** command to disable the logging.

The logging is enabled by default.

With this feature enabled, information about neighbor state changes is displayed on the terminal until the feature is disabled.

Examples # Disable the logging of neighbor state changes for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo log-peer-change
```

lsa-arrival-interval

Syntax **lsa-arrival-interval** *interval*

undo lsa-arrival-interval

View OSPF view

Parameters *interval*: Specifies the minimum LSA repeat arrival interval in milliseconds, in the range 0 to 60000.

Description Use the **lsa-arrival-interval** command to specify the minimum LSA repeat arrival interval.

Use the **undo lsa-arrival-interval** command to restore the default.

The interval defaults to 1000 milliseconds.

If an LSA that has the same LSA type, LS ID, originating router ID with the previous LSA is received within the interval, the LSA will be discarded. This feature helps protect routers and bandwidth from being over-consumed due to frequent network changes.

It is recommended the interval set with the **lsa-arrival-interval** command is smaller or equal to the initial interval set with the **lsa-generation-interval** command.

Related commands: **lsa-generation-interval**.

Examples # Set the LSA minimum repeat arrival interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-arrival-interval 200
```

lsa-generation-interval

Syntax **lsa-generation-interval** *maximum-interval* [*initial-interval* [*incremental-interval*]]

undo lsa-generation-interval

View OSPF view

Parameters *maximum-interval*: Maximum LSA generation interval in seconds, in the range 1 to 60.

initial-interval: Minimum LSA generation interval in milliseconds, in the range 10 to 60000. The default is 0.

incremental-interval: LSA generation incremental interval in milliseconds, in the range 10 to 60000. The default is 5000 milliseconds.

Description Use the **lsa-generation-interval** command to configure the OSPF LSA generation interval.

Use the **undo lsa-generation-interval** command to restore the default.

The LSA generation interval defaults to 5 seconds.

With this command configured, when network changes are not frequent, LSAs are generated at the *initial-interval*. If network changes become frequent, LSA generation interval is incremented by a specified value each time a generation happens, up to the *maximum-interval*.

Related commands: **lsa-arrival-interval**.

Examples # Configure the maximum LSA generation interval as 2 seconds, minimum interval as 100 milliseconds and incremental interval as 100 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-generation-interval 2 100 100
```

lsdb-overflow-limit

Syntax **lsdb-overflow-limit** *number*

undo lsdb-overflow-limit

View OSPF view

Parameters *number*: Specifies the upper limit of external LSAs in the LSDB, in the range 1 to 1000000.

Description Use the **lsdb-overflow-limit** command to specify the upper limit of external LSAs in the LSDB.

Use the **undo lsdb-overflow-limit** command to cancel the limitation.

External LSAs in the LSDB are unlimited by default.

Examples # Specify the upper limit of external LSAs as 400000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-limit 400000
```

maximum load-balancing

Syntax **maximum load-balancing** *maximum*
undo maximum load-balancing

View OSPF view

Parameters *maximum*: Maximum number of equal cost routes for load balancing, in the range 1 to 4. No load balancing is available when the number is set to 1.

Description Use the **maximum load-balancing** command to specify the maximum number of equal cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal cost routes is 4.

Examples # Specify the maximum number of equal cost routes as 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum load-balancing 2
```

maximum-routes

Syntax **maximum-routes** { **external** | **inter** | **intra** } *number*
undo maximum-routes { **external** | **inter** | **intra** }

View OSPF view

Parameters **external**: Specifies the maximum number of external routes.

inter: Specifies the maximum number of inter-area routes.

intra: Specifies the maximum number of intra-area routes.

number: Maximum route number, in the range 0 to 131072.

Description Use the **maximum-routes** command to specify the maximum route number of a specified type, inter-area, intra-area or external.

Use the **undo maximum-routes** command to restore the default route maximum value of a specified type.

By default, the maximum route number is 131072.

Examples # Specify the maximum number of intra-area routes as 500.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum-routes intra 500
```

network

Syntax **network** *ip-address wildcard-mask*

undo network *ip-address wildcard-mask*

View OSPF area view

Parameters *ip-address*: IP address of a network.

wildcard-mask: Wildcard mask of the IP address. For example, the wildcard mask of mask 255.0.0.0 is 0.255.255.255.

Description Use the **network** command to enable OSPF on the interface attached to the specified network in the area.

Use the **undo network** command to disable OSPF on an interface.

By default, an interface neither belongs to any area nor runs OSPF.

You can configure one or multiple interfaces in an area to run OSPF. Note that the interface's primary IP address must fall into the specified network segment to make the interface run OSPF. If only the interface's secondary IP address falls into the network segment, the interface cannot run OSPF.

Related commands: **ospf**.

Examples # Specify the interface whose primary IP address falls into 131.108.20.0/24 to run OSPF in Area 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

nssa

Syntax **nssa** [**default-route-advertise** | **no-import-route** | **no-summary**]*

undo nssa

View OSPF area view

- Parameters**
- default-route-advertise:** Usable on an NSSA ABR or an ASBR only. If it is configured on an NSSA ABR, the ABR generates a default route in a Type-7 LSA into the NSSA regardless of whether the default route is available. If it is configured on an ASBR, only a default route is available on the ASBR can it generates the default route in a Type-7 LSA into the attached area.
 - no-import-route:** Usable only on an NSSA ABR that is also the ASBR of the OSPF routing domain to disable redistributing routes in Type7 LSAs into the NSSA area, making sure that routes can be redistributed correctly.
 - no-summary:** Usable only on an NSSA ABR to advertise only a default route in a Type-3 summary LSA into the NSSA area. In this way, all the other summary LSAs are not advertised into the area. Such an area is known as an NSSA totally stub area.

- Description**
- Use the **nssa** command to configure the current area as an NSSA area.
- Use the **undo nssa** command to restore the default.
- By default, no NSSA area is configured.
- All routers attached to an NSSA area must be configured with the **nssa** command in area view.

Related commands: **default-cost.**

Examples # Configure Area 1 as an NSSA area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] nssa
```

ospf

- Syntax** **ospf** [*process-id* | **router-id** *router-id*]*
- undo ospf** [*process-id*]
- View** System view
- Parameters** *process-id*: OSPF process ID, in the range 1 to 65535.
- router-id*: OSPF Router ID, in dotted decimal format.
- Description** Use the **ospf** command to enable an OSPF process.
- Use the **undo ospf** command to disable an OSPF process.
- No OSPF process is enabled by default.

You can enable multiple OSPF processes on a router and specify different Router IDs for these processes.

Examples # Enable OSPF process 100 and specify Router ID 10.10.10.1.

```
<Sysname> system-view
[Sysname] ospf 100 router-id 10.10.10.1
[Sysname-ospf-100]
```

ospf authentication-mode

Syntax For MD5/HMAC-MD5 authentication:

```
ospf authentication-mode { md5 | hmac-md5 } key-id [ plain | cipher ]
password
```

```
undo ospf authentication-mode { md5 | hmac-md5 } key-id
```

For simple authentication:

```
ospf authentication-mode simple [ plain | cipher ] password
```

```
undo ospf authentication-mode simple
```

View Interface view

Parameters **md5**: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Authentication key ID, in the range 1 to 255.

plain | **cipher**: Plain or cipher password. If **plain** is specified, only plain password is supported and displayed upon displaying the configuration file. If **cipher** is specified, both plain and cipher are supported, but only cipher password is displayed when displaying the configuration file. If no keyword is specified, the cipher type is the default for the MD5/HMAC-MD5 authentication mode, and the plain type is the default for the simple authentication mode.

password: Password. Simple authentication: For plain type password, a plain password is a string of up to 8 characters; for cipher type password, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24 characters. MD5/HMAC-MD5 authentication: For plain type password, a plain password is a string of up to 16 characters; for cipher type password, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

Description Use the **ospf authentication-mode** command to set the authentication mode and key ID on an interface.

Use the **undo ospf authentication-mode** command to remove specified configuration.

By default, no authentication is available on an interface.

Interfaces attached to the same network segment must have the same authentication password and mode.

This configuration is not supported on the NULL interface.

Related commands: **authentication-mode.**

Examples # Configure the network 131.119.0.0/16 in Area 1 to support MD5 cipher authentication, and set the interface key ID to 15, authentication password to **abc**, and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode md5
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode md5 15 cipher abc
```

Configure the network 131.119.0.0/16 in Area 1 to support simple authentication, and set for the interface the authentication password to **abc**, and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode simple
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode simple cipher abc
```

ospf cost

Syntax **ospf cost** *value*

undo ospf cost

View Interface view

Parameters *value*: OSPF cost, in the range 1 to 65535.

Description Use the **ospf cost** command to set an OSPF cost for the interface.

Use the **undo ospf cost** command to restore the default OSPF cost for the interface.

By default, an OSPF interface calculates its cost with the formula: interface default OSPF cost=100 Mbps/interface bandwidth(Mbps). Default OSPF costs of some interfaces are:

- 1785 for the 56kbps serial interface
- 1562 for the 64kbps serial interface
- 48 for the E1 (2.048Mbps) interface
- 1 for the Ethernet interface

You can use the **ospf cost** command to set an OSPF cost for an interface manually.

This configuration is not supported on the NULL interface.

Examples # Set the OSPF cost for the interface to 65.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf cost 65
```

ospf dr-priority

Syntax **ospf dr-priority** *priority*

undo ospf dr-priority

View Interface view

Parameters *priority*: DR Priority of the interface, in the range 0 to 255.

Description Use the **ospf dr-priority** command to set the priority for DR/BDR election on an interface.

Use the **undo ospf dr-priority** command to restore the default value.

By default, the priority is 1.

The bigger the value, the higher the priority.

This configuration is not supported on the NULL interface and loopback interfaces.

Examples # Set the DR priority on the current interface to 8.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf dr-priority 8
```

ospf mib-binding

Syntax **ospf mib-binding** *process-id*

undo ospf mib-binding**View** System view**Parameters** *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **ospf mib-binding** command to bind an OSPF process to MIB operation.

Use the **undo ospf mib-binding** command to restore the default.

By default, MIB operation is bound to the first enabled OSPF process.

Examples # Bind OSPF process 100 to MIB operation.

```
<Sysname> system-view
[Sysname] ospf mib-binding 100
```

Bind the first enabled OSPF process to MIB operation.

```
<Sysname> system-view
[Sysname] undo ospf mib-binding
```

ospf mtu-enable

Syntax **ospf mtu-enable**

undo ospf mtu-enable

View Interface view**Parameters** None**Description** Use the **ospf mtu-enable** command to enable an interface to add the real MTU into DD packets.Use the **undo ospf mtu-enable** command to restore the default.

By default, an interface adds a MTU of 0 into DD packets, that is, no real MTU is added.

This configuration is not supported on the NULL interface.

Examples # Enable the interface to add the real MTU value into DD packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf mtu-enable
```

ospf network-type

Syntax `ospf network-type { broadcast | nbma | p2mp | p2p }`

`undo ospf network-type`

View Interface view

Parameters **broadcast**: Specifies the network type as Broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

p2p: Specifies the network type as P2P.

Description Use the **ospf network-type** command to set the network type for an interface.

Use the **undo ospf network-type** command to restore the default network type for an interface.

By default, the network type of an interface depends on its link layer protocol.

- For Ethernet, and FDDI, the default network type is broadcast.
- For ATM, FR, HDLC and X.25, the default network type is NBMA.
- For PPP, LAPB and POS, the default network type is P2P.

Note that:

- If a router on a broadcast network does not support multicast, you can configure the interface's network type as NBMA.
- If any two routers on an NBMA network are directly connected via a virtual link, that is, the network is fully meshed, you can configure the network type as NBMA; otherwise you need to configure it as P2MP for two routers having no direct link to exchange routing information via another router.
- When the network type of an interface is NBMA, you need to use the **peer** command to specify a neighbor.
- If only two routers run OSPF on a network segment, you can configure associated interfaces' network type as P2P.

Related commands: **ospf dr-priority**.



This command is not supported on the NULL interface.

Examples # Configure the interface's network type as NBMA.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf network-type nbma
```

ospf timer dead

Syntax **ospf timer dead** *seconds*

undo ospf timer dead

View Interface view

Parameters *seconds*: Dead interval in seconds, in the range 1 to 2147483647.

Description Use the **ospf timer dead** command to set the dead interval.

Use the **undo ospf timer dead** command to restore the default.

The dead interval defaults to 40s for Broadcast, P2P interfaces and defaults to 120s for P2MP and NBMA interfaces.

If an interface receives no hello packet from the neighbor within the dead interval, the interface considers the neighbor down. The dead interval on an interface is at least four times the hello interval. Any two routers attached to the same segment must have the same dead interval.

This configuration is not supported on the NULL interface.

Related commands: **ospf timer hello**.

Examples # Configure the dead interval on the current interface as 60 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer dead 60
```

ospf timer hello

Syntax **ospf timer hello** *seconds*

undo ospf timer hello

View Interface view

Parameters *seconds*: Hello interval in seconds, in the range 1 to 65535.

Description Use the **ospf timer hello** command to set the hello interval on an interface.

Use the **undo ospf timer hello** command to restore the default hello interval on an interface.

The hello interval defaults to 10s for P2P and Broadcast interfaces, and defaults to 30s for P2MP and NBMA interfaces.

The shorter the hello interval is, the faster the topology converges and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

This configuration is not supported on the NULL interface.

Related commands: **ospf timer dead.**

Examples # Configure the hello interval on the current interface as 20 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer hello 20
```

ospf timer poll

Syntax **ospf timer poll** *seconds*

undo ospf timer poll

View Interface view

Parameters *seconds*: Poll interval in seconds, in the range 1 to 2147483647.

Description Use the **ospf timer poll** command to set the poll interval on an NBMA interface.

Use the **undo ospf timer poll** command to restore the default value.

By default, the poll interval is 120s.

When an NBMA interface finds its neighbor is down, it will send hello packets at the poll interval. The poll interval is at least four times the hello interval.

This configuration is not supported on the NULL interface.

Related commands: **ospf timer hello.**

Examples # Set the poll timer interval on the current interface to 130 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer poll 130
```

ospf timer retransmit

Syntax **ospf timer retransmit** *interval*

undo ospf timer retransmit

View Interface view

- Parameters** *interval*: LSA retransmission interval in seconds, in the range 1 to 3600.
- Description** Use the **ospf timer retransmit** command to set the LSA retransmission interval on an interface.
- Use the **undo ospf timer retransmit** command to restore the default.
- The interval defaults to 5s.
- After sending an LSA, an interface waits for an acknowledgement packet. If the interface receives no acknowledgement within the retransmission interval, it will retransmit the LSA.
- The retransmission interval should not be so small to avoid unnecessary retransmissions.
- This configuration is not supported on the NULL interface.
- Examples** # Set the LSA retransmission interval to 8 seconds.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer retransmit 8
```

## ospf trans-delay

- Syntax** **ospf trans-delay** *seconds*
- undo ospf trans-delay**
- View** Interface view
- Parameters** *seconds*: LSA transmission delay in seconds, in the range 1 to 3600.
- Description** Use the **ospf trans-delay** command to set the LSA transmission delay on an interface.
- Use the **undo ospf trans-delay** command to restore the default.
- The delay defaults to 1s.
- Each LSA in the LSDB has an age that is incremented by 1 every second, but the age does not change during transmission. It is necessary to add a transmission delay into its age time, which is important for low speed networks.
- This configuration is not supported on the NULL interface.
- Examples** # Set the LSA transmission delay to 3 seconds on the current interface.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf trans-delay 3
```

peer

Syntax **peer** *ip-address* [**dr-priority** *dr-priority*]

undo peer *ip-address*

View OSPF view

Parameters *ip-address*: Neighbor IP address.

dr-priority: Neighbor DR priority, in the range 0 to 255.

Description Use the **peer** command to specify a neighbor, and the DR priority of the neighbor.

Use the **undo peer** command to remove the configuration.

On an X.25 or Frame Relay network, you can configure mappings to make the network fully meshed (any two routers have a direct link in between), so OSPF can handle DR/BDR election as it does on a broadcast network. However, since routers on the network cannot find neighbors via broadcasting hello packets, you need to specify neighbors and neighbor DR priorities on the routers.

After startup, a router sends a hello packet to neighbors with DR priorities higher than 0. When the DR and BDR are elected, the DR will send hello packets to all neighbors for adjacency establishment.

A router uses the priority set with the **peer** command to determine whether to send a hello packet to the neighbor rather than for DR election. The DR priority set with the **ospf dr-priority** command is used for DR election.

Related commands: **ospf dr-priority**.

Examples # Specify the neighbor 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] peer 1.1.1.1
```

preference

Syntax **preference** [**ase**] [**route-policy** *route-policy-name*] *value*

undo preference [**ase**]

View OSPF view

Parameters **ase**: Sets a priority for ASE routes. If the keyword is not specified, using the command sets a priority for OSPF internal routes.

route-policy: Applies a routing policy to set priorities for specified routes.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

value: Priority value, in the range 1 to 255. A smaller value represents a higher priority.

Description Use the **preference** command to set the priority of OSPF routes.

Use the **undo preference** command to restore the default.

The priority of OSPF internal routes defaults to 10, and the priority of OSPF external routes defaults to 150.

If a routing policy is specified, priorities defined by the routing policy will apply to matched routes, and the priorities set with the **preference** command apply to OSPF routes not matching the routing policy.

A router may run multiple routing protocols. When several routing protocols find routes to the same destination, the router uses the route found by the protocol with the highest priority.

Examples # Set a priority of 150 for OSPF internal routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] preference 150
```

reset ospf counters

Syntax **reset ospf** [*process-id*] **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]

View User view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

neighbor: Clears neighbor statistics.

interface-type interface-number: Interface type and interface number.

router-id: Neighbor Router ID.

Description Use the **reset ospf counters** command to reset OSPF counters. If no OSPF process is specified, counters of all OSPF processes are reset.

Examples # Reset OSPF counters.

```
<Sysname> reset ospf counters
```

reset ospf process

Syntax **reset ospf** [*process-id*] **process**

| | |
|--------------------|--|
| View | User view |
| Parameters | <i>process-id</i> : OSPF process ID, in the range 1 to 65535. |
| Description | Use the reset ospf process command to reset all OSPF processes or a specified process.

Using the reset ospf process command will: <ul style="list-style-type: none"> ■ Clear all invalid LSAs without waiting for their timeouts; ■ Make a newly configured Router ID take effect; ■ Start a new round of DR/BDR election; ■ Not remove any previous OSPF configurations. <p>The system prompts whether to reset OSPF process upon execution of this command.</p> |
| Examples | # Reset all OSPF processes.

<Sysname> reset ospf process |

reset ospf redistribution

| | |
|--------------------|--|
| Syntax | reset ospf [<i>process-id</i>] redistribution |
| View | User view |
| Parameters | <i>process-id</i> : OSPF process ID, in the range 1 to 65535. |
| Description | Use the reset ospf redistribution command to restart route redistribution. If no process ID is specified, using the command restarts route redistribution for all OSPF processes. |
| Examples | # Restart route redistribution.

<Sysname> reset ospf redistribution |

rfc1583 compatible

| | |
|-------------------|---|
| Syntax | rfc1583 compatible

undo rfc1583 compatible |
| View | OSPF view |
| Parameters | None |

- Description** Use the **rfc1583 compatible** command to make routing rules defined in RFC 1583 compatible.
- Use the **undo rfc1583 compatible** command to disable the function.
- By default, RFC 1583 routing rules are compatible.
- RFC 1583 and RFC 2328 have different routing rules on selecting the best route when multiple AS external LSAs describe routes to the same destination. Using this command can make them compatible.

Examples # Make RFC 1583 routing rules compatible.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] rfc1583 compatible
```

silent-interface

Syntax **silent-interface** { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

View OSPF view

Parameters **all**: Disables all interfaces from sending OSPF packets.

interface-type interface-number: Interface type and interface number.

Description Use the **silent-interface** command to disable an interface or all interfaces from sending OSPF packets.

Use the **undo silent-interface** command to restore the default.

By default, an interface sends OSPF packets.

A disabled interface is a passive interface, which cannot send any hello packet.

To make no routing information obtained by other routers on a network segment, you can use this command to disable the interface from sending OSPF packets.

Examples # Disable an interface from sending OSPF packets.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] silent-interface vlan-interface 10
```

snmp-agent trap enable ospf

Syntax **snmp-agent trap enable ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** |

lsdboverflow | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] *

undo snmp-agent trap enable ospf [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] *

View System view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

ifauthfail: Interface authentication failure information.

ifcfgerror: Interface configuration error information.

ifrxbadpkt: Information about error packets received.

ifstatechange: Interface state change information.

iftxretransmit: Packet receiving and forwarding information.

lsdbapproachoverflow: Information about cases approaching LSDB overflow.

lsdboverflow: LSDB overflow information.

maxagelsa: LSA max age information.

nbrstatechange: Neighbor state change information.

originatelsa: Information about LSAs originated locally.

vifauthfail: Virtual interface authentication failure information.

vifcfgerror: Virtual interface configuration error information.

virifauthfail: Virtual interface authentication failure information.

virifrxbadpkt: Information about error packets received by virtual interfaces.

virifstatechange: Virtual interface state change information.

viriftxretransmit: Virtual interface packet retransmission information.

virnbrstatechange: Virtual interface neighbor state change information.

Description Use the **snmp-agent trap enable ospf** command to enable the sending of SNMP traps for a specified OSPF process. If no process is specified, the feature is enabled for all processes.

Use the **undo snmp-agent trap enable ospf** command to disable the feature.

By default, this feature is enabled.

Refer to “SNMP Configuration Commands” on page 1023 for related information.

Examples # Enable the sending of SNMP traps for all OSPF processes.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ospf
```

spf-schedule-interval

Syntax **spf-schedule-interval** *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

View OSPF view

Parameters *maximum-interval*: Maximum SPF calculation interval in seconds, in the range 1 to 60.

minimum-interval: Minimum SPF calculation interval in milliseconds, in the range 10 to 60000, which defaults to 0.

incremental-interval: Incremental value in milliseconds, in the range 10 to 60000, which defaults to 5000.

Description Use the **spf-schedule-interval** command to set the OSPF SPF calculation interval.

Use the **undo spf-schedule-interval** command to restore the default.

The interval defaults to 5 seconds.

Based on its LSDB, an OSPF router calculates the shortest path tree with itself being the root, and uses it to determine the next hop to a destination. Through adjusting the SPF calculation interval, you can protect bandwidth and router resources from being over-consumed due to frequent network changes.

With this command configured, when network changes are not frequent, SPF calculation applies at the *minimum-interval*. If network changes become frequent, the SPF calculation interval is incremented by the *incremental-interval* each time a calculation happens, up to the *maximum-interval*.

Examples # Configure the SPF calculation maximum interval as 10 seconds, minimum interval as 500 milliseconds and incremental interval as 200 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] spf-schedule-interval 10 500 200
```

stub

Syntax **stub** [**no-summary**]

undo stub

View OSPF area view

Parameters **no-summary**: Usable only on a stub ABR. With it configured, the ABR advertises only a default route in a Summary LSA into the stub area (such a stub area is known as a totally stub area).

Description Use the **stub** command to configure an area as a stub area.

Use the **undo stub** command to remove the configuration.

No area is stub area by default. To configure an area as a stub area, all routers attached to it must be configured with this command.

Related commands: **default-cost.**

Examples # Configure Area1 as a stub area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
```

stub-router

Syntax **stub-router**

undo stub-router

View OSPF view

Parameters None

Description Use the **stub-router** command to configure the router as a stub router.

Use the **undo stub-router** command to restore the default.

By default, no router is configured as a stub router.

The router LSAs from the stub router may contain different link type values. A value of 3 means a link to the stub network, so the cost of the link remains unchanged. A value of 1, 2 or 4 means a point-to-point link, a link to a transit network or a virtual link; in such cases, a maximum cost value of 65535 is used. Thus, other neighbors find the links to the stub router have such big costs, they

will not send packets to the stub router for forwarding as long as there is a route with a smaller cost.

Examples # Configure a stub router.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] stub-router
```

vlink-peer

Syntax **vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** [**plain** | **cipher**] *password* | { **md5** | **hmac-md5** } *key-id* [**plain** | **cipher**] *password*]*

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead** | [**simple** | { **md5** | **hmac-md5** } *key-id*]]*

View OSPF area view

Parameters *router-id*: Router ID of the neighbor on the virtual link.

hello *seconds*: Hello interval in seconds, in the range 1 to 8192. The default is 10. It must be identical to the hello interval on its virtual link neighbor.

retransmit *seconds*: Retransmission interval in seconds, in the range 1 to 3600, which defaults to 5.

trans-delay *seconds*: Transmission delay interval in seconds, in the range 1 to 3600, which defaults to 1.

dead *seconds*: Dead interval in seconds, in the range 1 to 32768, which defaults to 40 and is identical to the value on its virtual link neighbor. The dead interval is at least four times the hello interval.

md5: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Key ID for MD5 or HMAC-MD5 authentication, in the range 1 to 255.

plain | **cipher**: Plain or cipher type. If plain is specified, only plain password is supported and displayed upon displaying the configuration file. If cipher is specified, both plain and cipher are supported, but only cipher password is displayed when displaying the configuration file. By default, MD5 and HMAC-MD5 support cipher password, and simple authentication supports plain password.

password: Plain or cipher password. Simple authentication: For plain type, a plain password is a string of up to 8 characters. For cipher type, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24

characters. MD5/HMAC-MD5 authentication: For plain type, a plain password is a string of up to 16 characters. For cipher type, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

Description Use the **vlink-peer** command to configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

As defined in RFC2328, all non-backbone areas must maintain connectivity to the backbone. You can use the **vlink-peer** command to configure a virtual link to connect an area to the backbone.

Considerations on parameters:

- The smaller the hello interval is, the faster the network converges and the more network resources are consumed.
- A so small retransmission interval will lead to unnecessary retransmissions. A big value is appropriate for a low speed link.
- You need to specify an appropriate transmission delay with the **trans-delay** keyword.

The authentication mode at the non-backbone virtual link end follows the one at the backbone virtual link end. The two authentication modes (MD5 or Simple) are independent, and you can specify neither of them.

Related commands: **authentication-mode, display ospf vlink.**

Examples # Configure a virtual link to the neighbor with router ID 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

25

IS-IS CONFIGURATION COMMANDS



The “router” in this document refers to a router in a generic sense or an Ethernet switch running routing protocols.

area-authentication-mode

Syntax `area-authentication-mode { simple | md5 } password [ip | osi]`

`undo area-authentication-mode`

View IS-IS view

Parameters **simple**: Specifies to send the password in plain text.

md5: Specifies to send the password encrypted with MD5.

password: Password to be set. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or ciphertext. A plaintext password can be a string of up to 16 characters, such as user918. A cipher password must be a ciphertext string of up to 24 characters, such as (TT8F]Y5SQ=^Q'MAF4<1!!.

ip: Specifies the system to check the configuration for the corresponding field of IP in LSP.

osi: Specifies the system to check the configuration for the corresponding field of OSI in LSP.



Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Description Use the **area-authentication-mode** command to specify the area authentication mode and a password. The password in the specified mode is inserted into all outgoing Level-1 packets (LSP, CSNP and PSNP) and is used for authenticating the incoming Level-1 packets.

Use the **undo area-authentication-mode** command to restore the default.

No area authentication mode is specified by default, that is, the system will neither authenticate incoming Level-1 packets nor set password for outgoing Level-1 packets.

With area authentication mode configured, the system will discard incoming routes from untrusted routers.

Related commands: **reset isis all, domain-authentication-mode, isis authentication-mode**

Examples # Set the area authentication password to hello, and the authentication mode to simple.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] area-authentication-mode simple hello
```

auto cost enable

Syntax **auto-cost enable**

undo auto-cost enable

View IS-IS view

Parameters None

Description Use the **auto-cost enable** command to enable interfaces of the current IS-IS process to calculate interface cost automatically.

Use the **undo auto-cost enable** command to disable the function.

This function is disabled by default.

The preference of interface cost set by the **auto-cost** command is lower than that set by the **circuit-cost** command. The preference from high to low is: the cost set by the **isis cost** command, the global cost set by the **circuit cost** command, the cost automatically calculated and the default cost.

When the **cost-style** is **wide** or **wide-compatible**, the cost value of an interface is calculated by using the following formula:

$$\text{cost} = (\text{reference value}/\text{bandwidth}) \times 10.$$

Related commands: **bandwidth-reference, cost-style.**

Examples # Enable interfaces of IS-IS process 1 to calculate interface cost automatically.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] auto-cost enable
```

bandwidth-reference

Syntax **bandwidth-reference** *value*

undo bandwidth-reference**View** IS-IS view**Parameters** **value**: Bandwidth reference value in Mbps, ranging from 1 to 2147483648.**Description** Use the **bandwidth-reference** command to set the bandwidth reference value for calculating link cost.Use the **undo bandwidth-reference** command to restore the default.

By default, the reference value is 100 Mbps.

In the case no interface cost is specified in interface view or system view and automatic cost calculation is enabled:

- When the cost style is **wide** or **wide-compatible**, IS-IS automatically calculates the interface cost based on the interface bandwidth, using the formula: interface cost = (reference value/bandwidth)×10, and the maximum calculated cost is 16777214.
- When the cost style is **narrow**, **narrow-compatible**, or **compatible**, if the interface is a loopback interface, the cost value is 0; otherwise, the cost value is automatically calculated as follows: if the interface bandwidth is in the range of 1 M to 10 M, the interface cost is 60; if the interface bandwidth is in the range of 11 M to 100 M, the interface cost is 50; if the interface bandwidth is in the range of 101 M to 155 M, the interface cost is 40; if the interface bandwidth is in the range of 156 M to 622 M, the interface cost is 30; if the interface bandwidth is in the range of 623 M to 2500 M, the interface cost is 20, and the default interface cost of 10 is used for any other bandwidths.

Related commands: **auto cost enable**.**Examples** # Configure the bandwidth reference of IS-IS process 1 as 200 Mbps.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] bandwidth-reference 200
```

circuit-cost**Syntax** **circuit-cost** *value* [**level-1** | **level-2**]**undo circuit-cost** [**level-1** | **level-2**]**View** IS-IS view**Parameters** *value*: Specifies the global link cost value. The value range varies with cost types.

- For types **narrow**, **narrow-compatible** and **compatible**: The cost value ranges from 0 to 63.

- For types **wide** and **wide-compatible**: The cost value ranges from 0 to 16777215.

level-1: Applies the link cost to Level-1.

level-2: Applies the link cost to Level-2.

Description Use the **circuit-cost** command to set a global link cost.

Use the **undo circuit-cost** command to restore the default.

By default, the global link cost is not configured.

If no keyword is specified, the specified cost applies to Level-1-2.

The preference of interface cost from high to low is: the cost set by the **isis cost** command, the global cost set by the **circuit-cost** command, the cost automatically calculated (**auto-cost**) and the default cost.

Related commands: **isis cost**, **cost-style**.

Examples # Set the global Level-1 link cost of IS-IS process 1 to 11.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] circuit-cost 11 level-1
```

cost-style

Syntax **cost-style** { **narrow** | **wide** | **wide-compatible** | { **compatible** | **narrow-compatible** } [**relax-spf-limit**] }

undo cost-style

View IS-IS view

Parameters **narrow**: Specifies to receive and send only packets of narrow cost style (The narrow cost ranges from 0 to 63).

wide: Specifies to receive and send only packets of wide cost style (The wide cost ranges from 0 to 16777215).

compatible: Specifies to receive and send both wide and narrow style packets.

narrow-compatible: Specifies to receive both narrow and wide style packets, but send only narrow style packets.

wide-compatible: Specifies to receive both narrow and wide style packets, but send only wide style packets.

relax-spf-limit: Specifies to allow receiving routes with cost bigger than 1023. If this keyword is not configured, any route with cost bigger than 1023 will be

discarded. This keyword is only available when keywords **compatible** and **narrow-compatible** are included.

Description Use the **cost-style** command to set the cost style of packets.
Use the **undo cost-style** command to restore the default.
Only packets of narrow cost style can be received and sent by default.

Related commands: **isis cost.**

Examples # Configure the router to send only packets of narrow cost style, but receive both narrow and wide cost style ones.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] cost-style narrow-compatible
```

default-route-advertise

Syntax **default-route-advertise** [**route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo default-route-advertise [**route-policy** *route-policy-name*]

View IS-IS view

Parameters *route-policy-name*: Specifies the name of a routing policy, a string of 1 to 19 characters.

level-1: Specifies the level of the default route as Level-1.

level-2: Specifies the level of the default route as Level-2.

level-1-2: Specifies the level of the default route as Level-1-2.



If no level is specified, a Level-2 default route is generated.

Description Use the **default-route-advertise** command to generate a Level-1 or Level-2 default route.

Use the **undo default-route-advertise** command to disable the function.

This function is disabled by default.

The Level-1 default route is advertised to other routers in the same area, while the Level-2 default route is advertised to all the Level-2 and Level-1-2 routers.

Using the **apply isis level-1** command in routing policy view will generate a default route in L1 LSP. Using the **apply isis level-2** command in routing policy view will generate a default route in L2 LSP. Using the **apply isis level-1-2**

command in routing policy view will generate a default route in L1 LSP and L2 LSP respectively.

Examples # Generate a default route in L2 LSP.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] default-route-advertise
```

display isis brief

Syntax display isis brief [*process-id*]

View Any view

Parameters *process-id*: IS-IS process ID, in the range of 1 to 65535.

Description Use the **display isis brief** command to view brief IS-IS configuration information.

Examples # Display brief IS-IS configuration information.

```
<Sysname> display isis brief
```

```
ISIS (1) Protocol Brief Information :
```

```
network-entity:
  10.0000.0000.0001.00
is-level :level-1-2
cost-style: narrow
preference : 15
Lsp-length receive : 1497
Lsp-length originate : level-1 1497
                      level-2 1497

Timers:
  spf-slice-size: 0
  lsp-max-age: 1200
  lsp-refresh: 900
  Interval between SPF's: 10
```

Table 82 Field descriptions of the display isis brief command

| Field | Description |
|----------------------|-----------------------------------|
| network-entity | Network entity name |
| is-level | IS-IS Routing level |
| cost-style | Cost style |
| preference | Preference |
| Lsp-length receive | Maximum LSP that can be received |
| Lsp-length originate | Maximum LSP that can be generated |
| Timers | Timers |

Table 82 Field descriptions of the display isis brief command

| Field | Description |
|-----------------------|---|
| spf-slice-size | Time of each SPF calculation slice (0 means SPF calculation time is not split.) |
| lsp-max-age | Maximum life period of LSP |
| lsp-refresh | Refresh period of LSP |
| Interval between SPFs | Interval between SPF calculations |

display isis interface

Syntax `display isis interface [verbose] [process-id]`

View Any view

Parameters **verbose**: Displays IS-IS interface detail information.

process-id: IS-IS process ID, in the range of 1 to 65535.

Description Use the **display isis interface** command to display IS-IS interface information.

The information displayed by this command includes interface name, interface IP address, interface link state and so on. Besides all the information displayed by **display isis interface**, using the **display isis interface verbose** command displays other interface related information, such as CSNP packets broadcast intervals, Hello packets broadcast intervals and the number of invalid Hello packets.

Examples # Display IS-IS enabled interface information.

```
<Sysname> display isis interface
                        Interface information for ISIS(1)
                        -----

Interface: Vlan-interface1
Id      IPV4.State      IPV6.State      MTU  Type  DIS
001      Up                Down            1497 L1/L2 No/No
```

Display detailed IS-IS enabled interface information.

```
<Sysname> display isis interface verbose
                        Interface information for ISIS(1)
                        -----

Interface: Vlan-interface1
Id      IPV4.State      IPV6.State      MTU  Type  DIS
001      Up                Down            1497 L1/L2 No/No
SNPA Address      : 000f-e200-2201
IP Address        : 192.168.0.136
Secondary IP Address(es) :
IPV6 Link Local Address :
IPV6 Global Address(es) :
```

```

Csnp Timer Value      : L1   10  L2   10
Hello Timer Value     : L1   10  L2   10
Hello Multiplier Value : L1    3  L2    3
Lsp Timer Value       : L12   33
Cost                  : L1   10  L2   10
Priority               : L1   64  L2   64
Retransmit Timer Value : L12    5

```

Table 83 Field descriptions of the display isis interface command

| Field | Description |
|--------------------------|--|
| Interface | Interface |
| Id | Circuit ID |
| IPV4.State | IPv4 state |
| IPV6.State | IPv6 state |
| MTU | Interface MTU |
| Type | Interface link type |
| DIS | Designated IS |
| SNPA Address | Subnet access point address |
| IP Address | Primary IP address |
| Secondary IP Address(es) | Secondary IP addresses |
| IPV6 Link Local Address | IPv6 link local address |
| IPV6 Global Address(es) | IPv6 global address |
| Csnp Timer Value | Interval for sending CSNP packets |
| Hello Timer Value | Interval for sending Hello packets |
| Hello Multiplier Value | Number of invalid Hello packets |
| Lsp Timer Value | Interval for sending LSP packets |
| Cost | Cost |
| Priority | Preference |
| Retransmit Timer Value | LSP retransmission interval over point-to-point link |

display isis license

Syntax `display isis license`

View Any view

Parameters None

Description Use the **display isis license** command to display the information of the IS-IS license.

Examples # Display the information of the IS-IS license.

```
<Sysname> display isis license
```

```
ISIS Shell License Values
```

| Feature Name | Active | Controllable |
|---------------|--------|--------------|
| ISIS Protocol | YES | YES |
| IPV6 | YES | YES |
| RESTART | YES | YES |
| TE | YES | NO |
| MI | YES | NO |

| Resource Name | MinVal | MaxVal | CurrVal | Controlla |
|------------------------|--------|--------|---------|-----------|
| Max Processes Resource | 1 | 1000 | 100 | 1 |
| Max Paths Resource | 1 | 4 | 4 | 1 |
| Max IPv4 Rt Resource | 8192 | 131072 | 131072 | 1 |
| Max IPv6 Rt Resource | 1 | 16384 | 16384 | 0 |

ISIS Core License Values

| Feature Name | Active |
|---------------|--------|
| ISIS Protocol | YES |
| IPV6 | YES |
| RESTART | YES |
| TE | YES |
| MI | YES |

| Resource Name | Current Value |
|------------------------|---------------|
| Max Processes Resource | 100 |
| Max Paths Resource | 4 |
| Max IPv4 Rt Resource | 131072 |
| Max IPv6 Rt Resource | 16384 |

Table 84 Field descriptions of the display isis license command

| Field | Description |
|---------------------------|---|
| ISIS Shell License Values | License values of ISIS shell |
| Feature Name | Feature name |
| Active | Whether the state is active. |
| Controllable | Whether support reading configuration through License file. |
| ISIS Protocol | IS-IS Protocol |
| IPV6 | Whether IPv6 is active or not. |
| RESTART | Graceful Restart (GR) |
| TE | Traffic Engineering |
| MI | Multi-instance |
| Resource Name | Resource name |
| MinVal | Minimum value |
| MaxVal | Maximum value |
| CurrVal | Current value |
| ISIS Core License Values | License values of ISIS Core |
| Max Processes Resource | Maximum number of processes supported |
| Max Paths Resource | Maximum equal cost paths |
| Max IPv4 Rt Resource | Maximum IPv4 routes supported |
| Max IPv6 Rt Resource | Maximum IPv6 routes supported |

display isis lsdb

Syntax **display isis lsdb** [[**I1** | **I2** | **level-1** | **level-2**]] [**lsp-id** *LSPID* | **lsp-name** *lspname*] | **local** | **verbose**] * [*process-id*]

View Any view

Parameters **I1, level-1**: Specifies level-1 LSDB.

I2, level-2: Specifies level-2 LSDB.

LSPID: LSP ID, in the form of sysid. Pseudo ID-fragment num.

lspname: LSP name, in the form of Symbolic name.[Pseudo ID]-fragment num.

local: Displays LSP information generated locally.

verbose: Displays LSDB detailed information.

process-id: IS-IS process ID, in the range of 1 to 65535.



If no level is specified, then both Level-1 and Level-2 (or Level-1-2) link state databases are displayed by default.

Description Use the **display isis lsdb** command to display IS-IS link state database.

Examples # Display Level-1 LSDB information.

```
<Sysname> dis isis lsdb level-1
```

```

Database information for ISIS(1)
-----
Level-1 Link State Database
LSPID                               Seq Num    Checksum    Holdtime    Length    ATT/P/OL
-----
bbbb.cccc.dddd.00-00* 0x0000001d 0x165      820         36       1/0/0
*--Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

```

Table 85 Field descriptions of the display isis lsdb command

| Field | Description |
|----------|--|
| LSPID | Link state packet ID |
| Seq Num | LSP sequence number |
| Checksum | LSP checksum |
| Holdtime | LSP holdtime |
| Length | LSP length |
| ATT/P/OL | Attach bit (ATT)
Partition bit (P)
Overload bit (OL) |

display isis mesh-group

Syntax **display isis mesh-group** [*process-id*]

View Any view

Parameters *process-id*: Specifies an IS-IS process ID, in the range of 1 to 65535.

Description Use the **display isis mesh-group** command to display IS-IS mesh-group.

Examples # Configure VLAN-interface 10 and VLAN-interface 20 on a switch to belong to mesh-group 100. (The process to establish VLAN-interface 10 and VLAN-interface 20 is omitted.)

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis mesh-group 100
[Sysname-Vlan-interface10] quit
[Sysname] interface vlan-interface 20
[Sysname-Vlan-interface20] isis mesh-group 100
```

Display the configuration information of IS-IS mesh-group.

```
[Sysname-Vlan-interface20] display isis mesh-group
```

```

                                Mesh Group information for ISIS(1)
                                -----
Interface          Status
Vlan10             100
Vlan20             100
```

Table 86 Field descriptions of the display isis mesh-group command

| Field | Description |
|-----------|------------------------------------|
| Interface | Interface name |
| Status | Mesh-group number of the interface |

display isis name-table

Syntax **display isis name-table** [*process-id*]

View Any view

Parameters *process-id*: IS-IS process ID, in the range of 1 to 65535.

Description Use the **display isis name-table** command to display the host name-to-system ID mapping table.

Examples # Configure a name for the local IS-IS system.

```

<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name RUTA

# Configure a static mapping for the remote IS-IS system (0000.0000.0041).

[Sysname-isis-1] is-name map 0000.0000.0041 RUTB

# Display the IS-IS host name-to-system ID mapping table.

[Sysname-isis-1] display isis name-table
                        Name table information for ISIS(1)
-----
System ID              Hostname                Type
6789.0000.0001        RUTA                    DYNAMIC
0000.0000.0041        RUTB                    STATIC

```

Table 87 Field descriptions of the display isis name-table command

| Field | Description |
|-----------|--|
| System ID | System ID |
| Hostname | Hostname name of the system ID |
| Type | Mapping type of system ID to host name (static or dynamic) |

display isis peer

Syntax `display isis peer [verbose] [process-id]`

View Any view

Parameters **verbose**: When this parameter is used, the area address advertised in a neighbor's Hello packet will be displayed. Otherwise the system displays only the summary information.

process-id: Specifies an IS-IS process ID, in the range of 1 to 65535.

Description Use the **display isis peer** command to display IS-IS neighbor information.

Besides all the information displayed using the **display isis peer** command, the **display isis peer verbose** command displays neighbor area address, hold time of Up state and direct interface's IP address.

Examples # Display detailed IS-IS neighbor information.

```

<Sysname> display isis peer verbose
                        Peer information for ISIS(1)
-----

System Id: 1010.1020.1031
Interface: Vlan-interface1          Circuit Id: 1010.1020.1031.01
State: Up      HoldTime: 7s         Type: L1(L1L2)      PRI: 64
Area Address(es): 10.0001
Peer IP Address(es): 192.168.0.156
Uptime: 00:05:45

```

```

Adj Protocol:  IPV4

System Id: 1010.1020.1031
Interface: Vlan-interface1          Circuit Id: 1010.1020.1031.01
State: Up      HoldTime: 7s        Type: L2(L1L2)      PRI: 64
Area Address(es):10.0001
Peer IP Address(es): 192.168.0.156
Uptime: 00:05:45
Adj Protocol:  IPV4

```

Table 88 Field descriptions of the display isis peer command

| Field | Description |
|---------------------|---|
| System Id | System ID |
| Interface | Interface connecting to the neighbor |
| Circuit Id | Circuit ID |
| State | State |
| HoldTime | Holdtime |
| Type | Type of the neighbor |
| PRI | DIS Priority |
| Area Address(es) | The neighbor's area address |
| Peer IP Address(es) | Interface IP address of the neighbor |
| Uptime | Time that elapsed since the neighbor relationship was formed. |
| Adj Protocol | Adjacency protocol |

display isis route

Syntax `display isis route [ipv4] [[level-1 | level-2] | verbose] * [process-id]`

View Any view

Parameters **ipv4**: Displays IS-IS IPv4 routing information (the default).

verbose: Displays IS-IS detailed IPv4 routing information.

process-id: Specifies an IS-IS process ID, in the range of 1 to 65535.

level-1: Displays Level-1 IS-IS routes.

level-2: Displays Level-2 IS-IS routes.



If no level is specified, then both Level-1 and Level-2 (Level-1-2) routing information will be displayed.

Description Use the **display isis route** command to display IS-IS IPv4 routing information.

Examples # Display IS-IS IPv4 routing information

```

<Sysname> display isis route 1
                        Route information for ISIS(1)
                        -----

```

| ISIS(1) IPv4 Level-1 Forwarding Table | | | | | |
|---------------------------------------|---------|---------|---------------|---------|-------|
| IPV4 Destination | IntCost | ExtCost | ExitInterface | NextHop | Flags |
| 192.168.0.0/24 | 10 | NULL | Vlan1 | Direct | D/L/- |

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

| ISIS(1) IPv4 Level-2 Forwarding Table | | | | | |
|---------------------------------------|---------|---------|---------------|---------|-------|
| IPV4 Destination | IntCost | ExtCost | ExitInterface | NextHop | Flags |
| 192.168.0.0/24 | 10 | NULL | Vlan1 | Direct | D/L/- |

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

Table 89 Field descriptions of the display isis route command

| Field | Description |
|------------------|---|
| IPV4 Destination | IPv4 destination address |
| IntCost | Interior routing cost |
| ExtCost | Exterior routing cost |
| ExitInterface | Exit interface |
| NextHop | Next hop |
| Flags | Routing state flag
D: Direct route.
R: The route has been added into the routing table.
L: The route has been advertised in an LSP.
U: A route's penetration flag. Setting it to UP can prevent an LSP sent from L2 to L1 from being sent back to L2. |

display isis spf-log

Syntax `display isis spf-log [process-id]`

View Any view

Parameters *process-id*: Specifies an IS-IS process ID, in the range of 1 to 65535.

Description Use the **display isis spf-log** command to display IS-IS SPF log record.

Examples # Display IS-IS SPF log record.

```
<Sysname> display isis spf-log
SPF Log information for ISIS(1)
-----
Level   Trig.Event                No.Nodes  Duration  StartTime
-----
L2      IS_SPFTRIG_PERIODIC      2          0         13:3:24
L1      IS_SPFTRIG_PERIODIC      2          0         13:18:8
L2      IS_SPFTRIG_PERIODIC      2          0         13:18:8
L1      IS_SPFTRIG_PERIODIC      2          0         13:32:28
L2      IS_SPFTRIG_PERIODIC      2          0         13:32:28
L1      IS_SPFTRIG_PERIODIC      2          0         13:44:0
L2      IS_SPFTRIG_PERIODIC      2          0         13:44:0
```

| | | | | |
|-------|---------------------|---|---|----------|
| L1 | IS_SPFTRIG_PERIODIC | 2 | 0 | 13:55:43 |
| -->L2 | IS_SPFTRIG_PERIODIC | 2 | 0 | 13:55:43 |
| L1 | IS_SPFTRIG_PERIODIC | 2 | 0 | 11:54:12 |
| L2 | IS_SPFTRIG_PERIODIC | 2 | 0 | 11:54:12 |
| L1 | IS_SPFTRIG_PERIODIC | 2 | 0 | 12:7:24 |
| L2 | IS_SPFTRIG_PERIODIC | 2 | 0 | 12:7:24 |
| L1 | IS_SPFTRIG_PERIODIC | 2 | 0 | 12:21:24 |
| L2 | IS_SPFTRIG_PERIODIC | 2 | 0 | 12:21:24 |
| L1 | IS_SPFTRIG_PERIODIC | 2 | 0 | 12:35:24 |
| L2 | IS_SPFTRIG_PERIODIC | 2 | 0 | 12:35:24 |
| L1 | IS_SPFTRIG_PERIODIC | 2 | 0 | 12:49:24 |
| L2 | IS_SPFTRIG_PERIODIC | 2 | 0 | 12:49:24 |
| L1 | IS_SPFTRIG_PERIODIC | 2 | 0 | 13:3:24 |

Table 90 Field descriptions of the display isis spf-log command

| Field | Description |
|------------|---------------------------------|
| Level | SPF calculation level |
| Trig.Event | SPF triggered event |
| No.Nodes | Number of SPF calculation nodes |
| Duration | SPF calculation duration |
| StartTime | SPF calculation start time |

display isis statistics

Syntax `display isis statistics [level-1 | level-2 | level-1-2]`

View Any view

Parameters **level-1:** IS-IS Level-1 statistic information.

level-2: IS-IS Level-2 statistic information.

level-1-2: IS-IS Level-1-2 statistic information.

process-id: Specifies an IS-IS process ID, in the range of 1 to 65535.

Description Use the **display isis statistics** command to display the statistic information of IS-IS process, including the number of routes learned from other IS-IS routers, the number of routes redistributed from other protocols and the number of LSP generated locally.

Examples # Display IS-IS statistics.

```
<Sysname> display isis statistics
```

```
Statistics information for ISIS(1)
```

```
-----
```

```
Level-1 Statistics
```

```
-----
```

```
Learnt routes information:
```

```
Total IPv4 Learnt Destinations: 4
```

```
Total IPv6 Learnt Destinations: 0
```

```

Imported routes information:
  IPv4 Imported Routes:
        Static: 0      Direct: 0
        ISIS:  0      BGP:  0
        RIP:   0      OSPF:  0
  IPv6 Imported Routes:
        Static: 0      Direct: 0
        ISISv6: 0     BGP4+: 0
        RIPng:  0     OSPFv3: 0

Lsp information:
        LSP Source ID:      No. of used LSPs
        0000.0000.0002      001
    
```

Table 91 Field descriptions of the display isis statistics command

| Field | | Description |
|---|----------------------|--|
| Statistics information for ISIS(<i>processid</i>) | | Statistics for the ISIS process |
| Level-1 Statistics | | Level-1 Statistics |
| Level-2 Statistics | | Level-2 Statistics |
| Learnt routes information | | Number of learnt IPv4 routes
Number of learnt IPv6 routes |
| Imported routes information | IPv4 Imported Routes | Redistributed IPv4 routes <ul style="list-style-type: none"> ■ Static ■ Direct ■ ISIS ■ BGP ■ RIP ■ OSPF |
| | IPv6 Imported Routes | Redistributed IPv6 routes <ul style="list-style-type: none"> ■ Static ■ Direct ■ ISISv6 ■ BGP4+ ■ RIPng ■ OSPFv3 |
| Lsp information | | LSP information <ul style="list-style-type: none"> ■ LSP Source ID: ID of the source system ■ No. of used LSPs: number of used LSPs |

domain-authentication-mode

Syntax `domain-authentication-mode { simple | md5 } password [ip | osi]`

undo domain-authentication-mode**View** IS-IS view**Parameters** **simple**: Specifies to send the password in plain text.**md5**: Specifies to send the password encrypted with MD5.

password: Specifies a password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or cipher text. A plain text password is a string of up to 16 characters, such as user918. A cipher password must be a string of 24 characters, such as `_(TT8F]Y5SQ=^Q'MAF4<1!!`.

ip: Checks IP related fields in LSPs and SNPs.**osi**: Checks OSI related fields in LSPs and SNPs.

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Description Use the **domain-authentication-mode** command to specify the routing domain authentication mode and a password. The password in the specified mode is inserted into all outgoing Level-2 packets (LSP, CSNP and PSNP) and is used for authenticating the incoming Level-2 packets.

Use the **undo domain-authentication-mode** command to disable the authentication.

No domain authentication mode is specified by default, that is, the system neither authenticates incoming Level-2 packets nor sets password for outgoing Level-2 packets.

Related commands: **area-authentication-mode, isis authentication-mode.****Examples** # Use the simple mode and password **123456** to authenticate level-2 routing packets.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] domain-authentication-mode simple 123456
```

filter-policy export

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **direct** | **static**]

undo filter-policy export [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **direct** | **static**]

View IS-IS view

Parameters *acl-number*: Specifies the number of an ACL that is used to filter outgoing redistributed routes, ranging from 2000 to 3999.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter outgoing redistributed routes, a string of 1 to 19 characters.

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter outgoing redistributed routes, a string of 1 to 19 characters.

isis *process-id*: Filters outgoing routes redistributed from an IS-IS process. The process ID is in the range of 1 to 65535.

ospf *process-id*: Filters outgoing routes redistributed from an OSPF process. The process ID is in the range of 1 to 65535.

rip *process-id*: Filters outgoing routes redistributed from a RIP process. The process ID is in the range of 1 to 65535.

bgp: Filters outgoing routes redistributed from BGP.

direct: Filters outgoing redistributed **direct** routes.

static: Filters outgoing redistributed **static** routes.

If no parameter is specified, the system will filter all outgoing redistributed routing information.

Description Use the **filter-policy export** command to configure IS-IS to filter outgoing redistributed routes.

Use the **undo filter-policy export** command to disable IS-IS from filtering outgoing redistributed routes.

IS-IS does not filter outgoing redistributed routes by default.

In some cases, only redistributed routing information satisfying certain conditions can be advertised. You can use the **filter-policy** command to reference filtering conditions.

Related commands: **filter-policy import.**

Examples # Reference ACL 2000 to filter outgoing redistributed routes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] filter-policy 2000 export
```

filter-policy import

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy import

View IS-IS view

Parameters *acl-number*: Specifies the number of an ACL that is used to filter incoming routes, ranging from 2000 to 3999.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter incoming routes, a string of 1 to 19 characters.

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter incoming routes, a string of 1 to 19 characters.

Description Use the **filter-policy import** command to configure IS-IS to filter incoming routing information.

Use the **undo filter-policy import** command to disable IS-IS from filtering incoming routing information.

IS-IS does not filter incoming routing information by default.

In some cases, only the routing information satisfying certain conditions can be received. You can reference filtering conditions using the **filter-policy** command.

Related commands: **filter-policy export**.

Examples # Reference ACL 2000 to filter incoming routing information.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] filter-policy 2000 import
```

flash-flood

Syntax **flash-flood** [**flood-count** *flooding-count* | **max-timer-interval** *flooding-interval* | [**level-1** | **level-2**]] *

undo flash-flood [**level-1** | **level-2**]

View IS-IS view

Parameters **flood-count** *flooding-count*: Specifies the maximum number of LSPs to be sent in the fast-flooding process, ranging from 1 to 15. The default is 5.

max-timer-interval *flooding-interval*: Specifies the delay interval (in milliseconds) between when it is enabled and when it begins, ranging from 10 to 50000. The default is 10.

level-1: Specifies to configure fast-flooding on **level-1** only.

level-2: Specifies to configure fast-flooding on **level-2** only. If no level is configured, the fast-flooding will be available on both **level-1** and **level-2** by default.

Description Use the **flash-flood** command to enable IS-IS LSP fast flooding and configure related parameters, including the maximum number of LSPs to be sent and the delay time before flooding.

Use the **undo flash-flood** command to disable fast-flooding.

Fast flooding is disabled by default.

Using this command can speed up LSP flooding that is triggered by topology changes, so as to reduce LSDB convergence time.

Examples # Enable fast flooding and configure the maximum LSPs be sent as 10 and the delay time as 100 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] flash-flood flood-count 10 max-timer-interval 100
```

import-route

Syntax **import-route** { **isis** [*process-id*] | **ospf** [*process-id*] | **rip** [*process-id*] | **bgp** [**allow-ibgp**] | **direct** | **static** } [**cost** *cost* | **cost-type** { **external** | **internal** }] [**level-1** | **level-1-2** | **level-2**] [**route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **isis** [*process-id*] | **ospf** [*process-id*] | **rip** [*process-id*] | **bgp** | **direct** | **static** }

View IS-IS view

Parameters **isis** [*process-id*]: Redistributes routes from a specified ISIS process. *process-id* is in the range of 1 to 65535.

ospf [*process-id*]: Redistributes routes from a specified OSPF process. *process-id* is in the range of 1 to 65535.

rip [*process-id*]: Redistributes routes from a specified RIP process. *process-id* is in the range of 1 to 65535.

bgp: Redistributes BGP routes.

allow-ibgp: Redistributes IBGP routes.

direct: Redistributes direct routes.

static: Redistributes static routes.

cost: Specifies a cost for redistributed routes.

The range of the cost depends on its type:

- For the types of narrow, narrow-compatible and compatible, the cost ranges from 0 to 63.
- For the types of wide, wide-compatible, the cost ranges from 0 to 16777215.

cost-type { external | internal }: Specifies a cost type. The **internal** type indicates the cost of routes within an area; the **external** type indicates the cost of routes between areas. The type is **external** by default. The keywords are valid only when the cost type is narrow, narrow-compatible or compatible.

level-1: Redistributes routes into the Level-1 routing table.

level-2: Redistributes routes into the Level-2 routing table. If no level is specified, the routes are redistributed into the Level-2 routing table by default.

level-1-2: Redistributes routes into both Level-1 and Level-2 routing tables.

route-policy route-policy-name: Redistributes only routes satisfying the matching conditions of a routing policy, the name of which is a string of 1 to 19 characters.

tag tag: Specifies a tag value for redistributed routes from 1 to 4294967295.

Description Use the **import-route** command to redistribute routes from other protocols.

Use the **undo import-route** command to disable route redistribution.

Route redistribution is not available by default.

IS-IS takes all the redistributed routes as external routes to destinations outside the IS-IS routing domain.

Related commands: **import-route isis level-2 into level-1.**



*Using the **import-route bgp** command redistributes only EBGP routes. Using the **import-route bgp allow-ibgp** command redistributes also IBGP routes, but this may cause routing loops. Be cautious with this command.*

Examples # Redistribute static routes and set the cost to 15.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] import-route static cost 15
```

import-route isis level-2 into level-1

Syntax **import-route isis level-2 into level-1** [**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo import-route isis level-2 into level-1

View IS-IS view

Parameters *acl-number*: Specifies the number of an ACL that is used to filter redistributed routes, ranging from 2000 to 3999.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter redistributed routes, a string of 1 to 19 characters.

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter redistributed routes, a string of 1 to 19 characters.

tag *tag*: Specifies a tag value from 1 to 4294967295 for redistributed routes.

Description Use the **import-route isis level-2 into level-1** command to redistribute routes from Level-2 to Level-1 area.

Use the **undo import-route isis level-2 into level-1** command to disable this redistribution.

The redistribution is not available by default.

Note that:

- You can specify a routing policy in the **import-route isis level-2 into level-1** command to filter routes from Level-2 to Level-1. Other routing policies specified for route reception and redistribution does not affect the route leaking.
- If a filter policy is configured, only routes passing it can be advertised into the Level-1 area.

Related commands: **import-route**.

Examples # Configure the router to redistribute routes from Level-2 to Level-1.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] import-route isis level-2 into level-1
```

isis

Syntax **isis** [*process-id*]

undo isis [*process-id*]

View System view

Parameters *process-id*: Process ID, ranging from 1 to 65535. The default is 1.

Description Use the **isis** command to enable an IS-IS process and enter IS-IS view.

Use the **undo isis** command to disable an IS-IS process.

To run IS-IS, you must first use the **isis** command to enable an IS-IS process, then use the **network-entity** command to configure a Network Entity Title (NET) for the router, and then use the **isis enable** command to enable IS-IS on each interface that needs to run the IS-IS process.

Related commands: **isis enable**, **network-entity**.

Examples # Enable IS-IS routing process 1, with the system ID being 0000.0000.0002, and area ID being 01.0001.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] network-entity 01.0001.0000.0000.0002.00
```

isis authentication-mode

Syntax **isis authentication-mode** { **simple** | **md5** } *password* [**level-1** | **level-2**] [**ip** | **osi**]

undo isis authentication-mode [**level-1** | **level-2**]

View Interface view

Parameters **simple**: Specifies to send the password in plain text.

md5: Specifies to send the password in ciphertext.

password: Specifies a password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or ciphertext. A plain text password can be a string of up to 16 characters, such as user918. A cipher password must be a string of 24 characters, such as _(TT8F)Y5SQ=^Q'MAF4<1!!.

level-1: Specifies to set the password for Level-1.

level-2: Specifies to set the password for Level-2.

ip: Specifies the system to check IP related fields in a LSP.

osi: Specifies the system to check OSI related fields in a LSP.

Whether a password should use **ip** or **osi** is not affected by the actual network environment.



This command is not available in loopback interface view.

Description Use the **isis authentication-mode** command to set the IS-IS authentication mode and password for an interface.

Use the **undo isis authentication-mode** command to disable the authentication and remove the password.

There is no password or authentication by default.

If you set a password without specifying any other parameter, the password applies to both Level-1 and Level-2, and the system checks the OSI related fields in a LSP.

Related commands: **area-authentication-mode**, **domain-authentication-mode**.



*The level-1 and level-2 keywords are available only on the VLAN interface of switches after IS-IS is enabled on the interface using the **isis enable** command.*

Examples # Set the plain text password tangshi for the VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis authentication-mode simple tangshi level-1
```

isis circuit-level

Syntax **isis circuit-level** [**level-1** | **level-1-2** | **level-2**]

undo isis circuit-level

View Interface view

Parameters **level-1**: Specifies to set up only level-1 adjacency on the interface.

level-1-2: Specifies to set up level-1-2 adjacency on the interface.

level-2: Specifies to set up only level-2 adjacency on the interface.

Description Use the **isis circuit-level** command to configure link adjacency level for an interface of a level-1-2 router.

Use the **undo isis circuit-level** command to restore the default.

An interface can establish level-1-2 adjacency by default.

This command is only available on a level-1-2 router. You can use it to configure an interface to establish the adjacency of a specified level (**level-1** or **level-2**) with the neighbor, making the interface handle only the specified level hello packets. An interface can receive and send only one level hello packet on a point-to-point

link. Using this command can reduce the router's processing time and save bandwidth.

Related commands: **is-level.**

Examples # Suppose VLAN-interface 10 is connected to a non backbone router in the same area. Configure the link adjacency level of VLAN-interface 10 as Level-1 to prevent sending and receiving Level-2 Hello packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable
[Sysname-Vlan-interface10] isis circuit-level level-1
```

isis circuit-type

Syntax **isis circuit-type p2p**
undo isis circuit-type

View Interface view

Parameters **p2p**: Specifies the interface's network type as P2P.

Description Use the **isis circuit-type** command to configure the network type for an interface.

Use the **undo isis circuit-type** command to restore the default.

By default, the network type of a switch's VLAN interface is broadcast.



This command is not available in the loopback interface view.

Examples # Configure the network type of VLAN-interface 10 as P2P.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable
[Sysname-Vlan-interface10] isis circuit-type p2p
```

isis cost

Syntax **isis cost** *value* [**level-1** | **level-2**]
undo isis cost [**level-1** | **level-2**]

View Interface view

Parameters *value*: Specifies a cost for SPF calculation on a specified level. The default is 10. The range of cost value differs according to different cost types.

- For types **narrow**, **narrow-compatible** and **compatible**: The cost value ranges from 1 to 63.
- For types **wide** and **wide-compatible**: The cost value ranges from 1 to 16777215.

level-1: Applies the cost to Level-1.

level-2: Applies the cost to Level-2.

Description Use the **isis cost** command to set the link cost of an interface for SPF calculation.

Use the **undo isis cost** command to restore the default.

No cost is configured by default.

If neither **level-1** nor **level-2** is included, the cost applies to both **level-1** and **level-2**.

You are recommended to configure a proper link cost for each interface for optimal route selection.

Relate command: **circuit-cost**.

Examples # Configure the Level-2 link cost as 5 for VLAN-interface10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis cost 5 level-2
```

isis dis-name

Syntax **isis dis-name** *symbolic-name*

undo isis dis-name

View Interface view

Parameters *symbolic-name*: Specifies a name for the local LAN, a string of 1 to 64 characters.

Description Use the **isis dis-name** command to configure a name for local LAN. If the local router is the DIS, the name will be advertised in a pseudonode LSP packet.

Use the **undo isis dis-name** command to disable this function.

No name is configured by default.

Note that this command takes effect only on a router with the dynamic hostname process enabled. This command is not supported on a Point-to-Point interface.



This command is not available in the loopback interface view.

Examples # Configure the name as **LOCALAREA** for the local LAN.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis dis-name LOCALAREA
```

isis dis-priority

Syntax **isis dis-priority** *value* [**level-1** | **level-2**]

undo isis dis-priority [**level-1** | **level-2**]

View Interface view

Parameters *value*: Specifies a priority for DIS selection, ranging from 0 to 127.

level-1: Applies the DIS selection priority to Level-1.

level-2: Applies the DIS selection priority to level-2.

If neither level-1 nor level-2 is specified in this command, the DIS priority applies to both Level-1 and Level-2.

Description Use the **isis dis-priority** command to specify a DIS selection priority on a specified level for an interface.

Use the **undo isis dis-priority** command to restore the default priority of 64.

There is no backup DIS in IS-IS and the router with the 0 priority can also participate in DIS selection.



This command is not available in the loopback interface view.

Examples # Configure the level-2 DIS priority as 127 for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis dis-priority 127 level-2
```

isis enable

Syntax **isis enable** [*process-id*]

undo isis enable

View Interface view

Parameters *process-id*: Specifies a IS-IS process ID, ranging from 1 to 65535. The default is 1.

Description Use the **isis enable** command to enable an IS-IS routing process on the interface.

Use the **undo isis enable** command to disable this configuration.

No IS-IS routing process is enabled on an interface by default.

To run IS-IS, you need to use the **isis** command to enable an IS-IS process, and use the **network-entity** command to configure a network entity title (NET) for the router, and then use the **isis enable** command to enable IS-IS on each interface that needs to run the IS-IS process.

Related commands: **isis**, **network-entity**.

Examples # Create IS-IS routing process 1, and enable the IS-IS routing process on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable 1
```

isis mesh-group

Syntax **isis mesh-group** { *mesh-group-number* | **mesh-blocked** }

undo isis mesh-group

View Interface view

Parameters *mesh-group-number*: Specifies a mesh group number, ranging from 1 to 4294967295.

mesh-blocked: Blocks the interface from flooding LSPs to make it send LSPs only after receiving requests.

Description Use the **isis mesh-group** command to add the interface into a specified mesh group.

Use the **undo isis mesh-group** command to delete the interface from a mesh group.

An interface is not in any mesh group by default.

For an interface not in a mesh group, it follows the normal process to flood the received LSPs to other interfaces. For the NBMA network with high connectivity and multiple point-to-point links, this will cause repeated LSP flooding and bandwidth waste.

After an interface is added to a mesh group, it will only flood a received LSP to interfaces not belonging to the same mesh group.

When you add an interface to a mesh group or block the interface, make sure to retain some redundancy so that a link failure will not affect the normal LSP packet flooding.



- *A mesh-group is only available for a point-to-point link interface.*
- *This command is not available in loopback interface view.*

Examples # Add IS-IS enabled VLAN-interface 10 to the mesh-group 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis mesh-group 3
```

isis silent

Syntax **isis silent**

undo isis silent

View Interface view

Parameters None

Description Use the **isis silent** command to disable the interface from sending and receiving IS-IS hello packets.

Use the **undo isis silent** command to restore the default.

By default, an interface is not disabled from sending and receiving hello packets.



The feature is not supported on the loopback interface.

Examples # Disable VLAN-interface 10 from sending and receiving hello packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface10
[Sysname-Vlan-interface10] isis silent
```

isis small-hello

Syntax **isis small-hello**

undo isis small-hello

View Interface view

Parameters None

Description Use the **isis small-hello** command to configure the interface to send small Hello packets without padding field.

Use the **undo isis small-hello** command to disable the feature.

An interface sends standard Hello packets by default.



This command is not available in loopback interface view.

Examples # Configure VLAN-interface 10 to send small Hello packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface10
[Sysname-Vlan-interface10] isis small-hello
```

isis timer csnp

Syntax **isis timer csnp** *seconds* [**level-1** | **level-2**]

undo isis timer csnp [**level-1** | **level-2**]

View Interface view

Parameters *seconds*: Specifies the interval in seconds for sending CSNP packets over broadcast network, ranging from 1 to 600.

level-1: Applies the interval to Level-1.

level-2: Applies the interval to Level-2.

Description Use the **isis timer csnp** command to specify the interval for sending CSNP packets over broadcast network.

Use the **undo isis timer csnp** command to restore the default.

The default CSNP interval is 10 seconds.



- *If no level is specified, the CSNP interval applies to both Level-1 and Level-2 of the current ISIS process. If a level is specified, the interval applies to the level.*
- *This command is not supported on the loopback interface.*
- *This command only applies to the DIS router, which sends CSNP packets periodically.*

Examples # Configure Level-2 CSNP packets to be sent every 15 seconds over VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer csnp 15 level-2
```

isis timer hello

Syntax **isis timer hello** *seconds* [**level-1** | **level-2**]

undo isis timer hello [**level-1** | **level-2**]

View Interface view

Parameters *seconds*: Specifies the interval in seconds for sending Hello packets, ranging from 3 to 255.

level-1: Specifies the interval for sending Level-1 Hello packets.

level-2: Specifies the time interval for sending Level-2 Hello packets.

Description Use the **isis timer hello** command to specify the interval for sending hello packets.

Use the **undo isis timer hello** command to restore the default.

The default hello interval is 10 seconds.



- *If no level is specified, the hello interval applies to both Level-1 and Level-2 of the current ISIS process. If a level is specified, the interval applies to the level.*
- *This command is not supported on the loopback interface.*
- *The broadcast link distinguishes between Level-1 and Level-2 packets, so you need specify intervals for the two levels respectively. The point-to-point link however does not distinguish, so you need not specify intervals respectively.*
- *As the shorter the interval is, the more system resources will be occupied, you should configure a proper interval as needed.*

Related commands: **isis timer holding-multiplier**.

Examples # Configure Level-2 Hello packets to be sent every 20 seconds over VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 10
[Sysname-Vlan-interface10] isis timer hello 20 level-2
```

isis timer holding-multiplier

Syntax **isis timer holding-multiplier** *value* [**level-1** | **level-2**]

undo isis timer holding-multiplier [**level-1** | **level-2**]

View Interface view

Parameters *value*: Number of hello intervals, in the range of 3 to 1000.

level-1: Applies the number to the Level-1 IS-IS neighbor.

level-2: Applies the number to the Level-2 IS-IS neighbor.



- *If neither level-1 nor level-2 is specified in the command, the number applies to the current level IS-IS process.*
- *This command is not available in loopback interface view.*

Description Use the **isis timer holding-multiplier** command to configure the number of hello intervals, within which if the interface receive no hello packets, its neighbor is considered dead.

Use the **undo isis timer holding-multiplier** command to restore the default.

On an interface, the default number of hello intervals is three.

You can specify the number of hello intervals for Level-1 and Level-2 neighbors respectively on a broadcast network. For a point-to-point link, there is only one kind of Hello packet, so you need not specify Level-1 or Level-2.

The specified number of hello intervals is used to configure the Holddown time. If a router receives no Hello packets from a neighbor within Holddown time, it will take the neighbor as dead. The Holddown time can be configured differently for different routers within an area. You can adjust the Holddown time by changing either the hello interval or the number of Hello intervals on an interface.

Related commands: **isis timer hello.**

Examples # Configure the number of Level-2 Hello intervals as 5 for interface VLAN-interface, that is, if no Hello packet is received from the interface within 5 hello intervals, the IS-IS neighbor is considered dead.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 10
[Sysname-Vlan-interface10] isis timer holding-multiplier 5
```

isis timer lsp

Syntax **isis timer lsp** *time* [**count** *count*]

undo isis timer lsp

View Interface view

Parameters *time*: Specifies the minimum interval in milliseconds for sending link-state packets, ranging from 1 to 1000.

count: Specifies the maximum number of link-state packets to be sent at one time, in the range of 1 to 1000. The default is 100 for the broadcast interface and 11 for point-to-point interface.

Description Use the **isis timer lsp** command to configure the interval for sending link-state packets on the interface.

Use the **undo isis timer lsp** command to restore the default of 33 ms.

Related commands: **isis timer retransmit**.



This command is not available in loopback interface view.

Examples # Configure the interval as 500 milliseconds for sending LSPs on interface VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer lsp 500
```

isis timer retransmit

Syntax **isis timer retransmit** *seconds*

undo isis timer retransmit

View Interface view

Parameters *seconds*: Specifies the interval in seconds for retransmitting LSP packets, ranging from 1 to 300.

Description Use the **isis timer retransmit** command to configure the interval for retransmitting LSP packets over point-to-point link.

Use the **undo isis timer retransmit** command to restore the default of 5s.

You need not use this command over a broadcast link where no LSP response is required.

Related commands: **isis timer lsp**.



- *This command is not available in loopback interface view.*
- *Configure a proper time to avoid unnecessary retransmissions.*

Examples # Configure the LSP retransmission interval as 10 seconds for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer retransmit 10
```

is-level

Syntax **is-level** { **level-1** | **level-1-2** | **level-2** }

undo is-level

View IS-IS view

Parameters **level-1**: Configures the router to work on Level-1, which means it only calculates routes within the area, and maintains the L1 LSDB.

level-1-2: Configures the router to work on Level-1-2, which means it calculates routes and maintains the LSDBs for both L1 and L2.

level-2: Configures the router to work on Level-2, which means it calculates routes and maintains the LSDB for L2 only.

Description Use the **is-level** command to configure IS-IS router type.

Use the **undo is-level** command to restore the default.

The default router type is **level-1-2**.

It is recommended to configure system level when you configure IS-IS.

You can configure all the routers as either Level-1 or Level-2 if there is only one area, because there is no need for all routers to maintain two identical databases at the same time. In this case, you are recommended to configure all the routers as Level-2 in the IP network for scalability consideration.

Related commands: **isis circuit-level**.

Examples # Configure the router to work in Level-1.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-level level-1
```

is-name

Syntax **is-name** *sys-name*

undo is-name

View IS-IS view

Parameters *symbolic-name*: Specifies a name for the local IS, a string of 1 to 64 characters.

Description Use the **is-name** command to enable the dynamic hostname process and configure a name for the router.

Use the **undo is-name** command to remove the configuration.

No IS name is configured by default.

Examples # Configure a name for the local IS.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name RUTA
```

is-name map

is-name map *sys-id map-sys-name*

undo is-name map *sys-id*

View IS-IS view

Parameters *sys-id*: System ID or a pseudonode ID of a remote IS.

map-sys-name: Specifies a name for the remote IS, a string of 1 to 64 characters.

Description Use the **is-name map** command to map a name to a remote IS. Each remote IS system ID corresponds to only one name.

Use the **undo is-name map** command to remove the configuration.

By default, no name is configured for a remote IS.

Examples # Map the name RUTB to the remote IS 0000.0000.0041.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

is-snmp-traps enable

Syntax **is-snmp-traps enable**

undo is-snmp-traps

View IS-IS view

Parameters None

Description Use the **is-snmp-traps enable** command to enable the SNMP Trap function of IS-IS.

Use the **undo is-snmp-traps** command to disable this function.

SNMP Trap is enabled by default.

Examples # Enable SNMP Trap.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-snmp-traps enable
```

log-peer-change

Syntax **log-peer-change**
undo log-peer-change

View IS-IS view

Parameters None

Description Use the **log-peer-change** command to enable logging on IS-IS adjacency state changes.

Use the **undo log-peer-change** command to disable the logging.

The feature is enabled by default.

After the feature is enabled, information about IS-IS adjacency state changes is sent to the configuration terminal.

Examples # Enable logging on the IS-IS adjacency state changes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] log-peer-change
```

lsp-fragments-extend

Syntax **lsp-fragments-extend** [[**level-1** | **level-2** | **level-1-2**]] [[**mode-1** | **mode-2**]] *

undo lsp-fragments-extend

View IS-IS view

Parameters **mode-1**: Fragment extension mode 1, used on a network where some routers do not support LSP fragment extension.

mode-2: Fragment extension mode 2, used on a network where all routers support LSP fragment extension.

level-1: Applies the fragment extension mode to Level-1 LSPs.

level-2: Applies the fragment extension mode to Level-2 LSPs.

level-1-2: Applies the fragment extension mode to both Level-1 and Level-2 LSPs.



The **mode-1** and **level-1-2** keywords are used by default.

Description Use the **lsp-fragments-extend** command to enable LSP fragment extension in a specified mode and level.

Use the **undo lsp-fragments-extend** command to disable this feature.

The feature is disabled by default.

Note the following:

- After LSP fragment extension is enabled in an IS-IS process, the MTUs of all the interfaces on which this IS-IS process is enabled must not be less than 512; otherwise, LSP fragment extension will not take effect.
- At least one virtual system needs to be configured for the router to generate extended LSP fragments. An IS-IS process allows 50 virtual systems at most.

Examples # Enable LSP fragment extension of **mode-1** and **Level-2**.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-fragments-extend mode-1 level-2
```

lsp-length originate

Syntax **lsp-length originate** *size* [**level-1** | **level-2**]

undo lsp-length originate [**level-1** | **level-2**]

View IS-IS view

Parameters *size*: Specifies the maximum size in bytes of a LSP packet, ranging from 512 to 16384.

level-1: Applies the size to Level-1 LSP packets.

level-2: Applies the size to Level-2 LSP packets.



If neither Level-1 nor Level-2 is specified in the command, the configured maximum size applies to the current IS-IS level.

Description Use the **lsp-length originate** command to configure the maximum size of generated Level-1 or Level-2 LSPs.

Use the **undo lsp-length originate** command to restore the default.

The maximum size of 1497 bytes is the default.

Examples # Configure the maximum size of the generated Level-2 LSPs as 1024 bytes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-length originate 1024 level-2
```

lsp-length receive

Syntax **lsp-length receive** *size*
undo lsp-length receive

View IS-IS view

Parameters *size*: Maximum size of received LSPs, in the range of 512 to 16384 bytes.

Description Use the **lsp-length receive** command to configure the maximum size of received LSPs.

Use the **undo lsp-length receive** command to restore the default.

By default, the maximum size of received LSPs is 1497 bytes.

Examples # Configure the maximum size of received LSPs.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-length receive 1024
```

maximum load-balancing

Syntax **maximum load-balancing** *number*
undo maximum load-balancing

View IS-IS view

Parameters *number*: Maximum number of equal-cost load balanced routes, in the range 1 to 4.

Description Use the **maximum load-balancing** command to configure the maximum number of equal-cost load balanced routes.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal-cost load balanced routes is 4.

Examples # Configure the maximum number of equal-cost load-balanced routes as 2.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] maximum load-balancing 2

# Restore the default.

[Sysname-isis-100] undo maximum load-balancing
```

network-entity

Syntax **network-entity** *net*
undo network-entity *net*

View IS-IS view

Parameters *net*: Network Entity Title (NET) in the format of X...X.XXXX....XXXX.00, with the first part X...X being the area address, the middle part XXXX....XXXX (a total of 12 "X") being the router's system ID and the last part 00 being SEL.

Description Use the **network-entity** command to configure the Network Entity Title for an IS-IS routing process.

Use the **undo network-entity** command to delete a NET.

No NET is configured by default.

A NET is a network service access point (NSAP), and it is in the range of 8 to 20 bytes for IS-IS.

A NET has three parts: The first part is area ID, which ranges from 1 to 13 bytes. Routers in the same area must have the same area ID. The second part is the router's 6-byte system ID, which is unique within the whole area and backbone area. The third part is the 1-byte SEL that must be 00. Generally, a router needs one NET. In the case of repartitioning an area, such as merging or splitting, you can configure multiple NETs beforehand for the router to ensure correct and continuous routing.

Related commands: **isis, isis enable.**

Examples # Specify the NET as 10.0001.1010.1020.1030.00, of which 10.0001 is the area ID and 1010.1020.1030 is the system ID.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
```

preference

Syntax **preference** { **route-policy** *route-policy-name* | *preference* } *

undo preference

View IS-IS view

Parameters *preference*: Specifies the preference for IS-IS protocol, ranging from 1 to 255.

route-policy-name: Routing policy name, a string of 1 to 19 characters. The preference applies to routes passing the routing policy.

Description Use the **preference** command to configure the preference for IS-IS protocol.

Use the **undo preference** command to restore the default.

By default, the IS-IS protocol preference is 15.

If a routing policy is specified in this command, the preference (if any) set by the routing policy applies to those matched routes. Other routes use the preference set by the **preference** command.

When a router runs multiple routing protocols at the same time, the system will set a preference to each routing protocol. If several protocols find routes to the same destination, the route of the routing protocol with the highest preference is selected.

Examples # Configure the preference of IS-IS protocol as 25.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] preference 25
```

reset isis all

Syntax **reset isis all** [*process-id*]

View User view

Parameters *process-id*: Clears the data structure information of an IS-IS process numbered from 1 to 65535.

Description Use the **reset isis all** command to clear all ISIS data structure information.

No data structure information is cleared by default.

This command is used when the LSP needs to be updated immediately. For example, after performing the **area-authentication-mode** and

domain-authentication-mode commands, you can use this command to clear old LSPs.

Related commands: **area-authentication-mode**, **domain-authentication-mode**.

Examples # Clear all IS-IS data structure information.
 <Sysname> reset isis all

reset isis peer

Syntax **reset isis peer** *system-id* [*process-id*]

View User view

Parameters *system-id*: Specifies the system ID of an IS-IS neighbor.
process-id: Specifies the ID of an IS-IS process, in the range of 1 to 65535.

Description Use the **reset isis peer** command to clear the data structure information of a specified IS-IS neighbor.

The command is disabled by default.

This command is used when you need to re-establish an IS-IS neighbor.

Examples # Clear the data structure information of the neighbor with system ID being 0000.0c11.1111.
 <Sysname> reset isis peer 0000.0c11.1111

set-overload

Syntax **set-overload** [**on-startup start-from-nbr** *system-id* [*timeout* [*nbr-timeout*]]]
 [**allow** { **interlevel** | **external** } *]

undo set-overload

View IS-IS view

Parameters **on-startup**: Specifies to start the overload tag timeout timer upon system startup.
start-from-nbr *system-id*: Specifies to start the overload tag timeout timer when the router begins to establish the connection with a neighbor.
timeout: Specifies the overload tag timeout timer, with an interval from 5 to 86400 seconds. The timer is started after system startup. The default is 600 seconds.

nbr-timeout: Specifies the overload tag timeout timer that is started when the router begins to establish the connection with a neighbor after system startup. The time has an interval from 5 to 86400 seconds. The default is 1200 seconds.

allow: Specifies to allow advertising address prefixes. By default, no address prefixes are allowed to be advertised when the system is in overload state.

interlevel: Allows advertising IP address prefixes learnt from different IS-IS levels with the **allow** keyword specified.

external: Allows advertising IP address prefixes learnt from other routing protocols with the **allow** keyword specified.

Description Use the **set-overload** command to set the overload tag for the current router.

Use the **undo set-overload** command to clear the overload tag.

No overload flag is set by default.

When the overload flag is set for a router, the routes calculated by the router will be ignored by other routers when they perform SPF calculations. (But the direct routes will not be ignored.)

When a router is set overload tag, other routers will not send packets to the router for forwarding.

Examples # Set overload flag on the current router.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] set-overload
```

spf-slice-size

Syntax **spf-slice-size** *duration-time*

undo spf-slice-size

View IS-IS view

Parameters *duration-time*: Specifies the duration in milliseconds of each sliced SPF calculation, ranging from 10 to 50000. Each sliced SPF calculation is ended when the duration time is reached. If the *duration-time* is set to 0, the entire SPF calculation will not be sliced.

Description Use the **spf-slice-size** command to specify the duration for each sliced SPF calculation.

Use the **undo spf-slice-size** command to restore the default.

By default, the duration of each sliced SPF calculation is 10 milliseconds.

To prevent the SPF calculation from occupying the system resources for a long time, you can use this command to slice the whole SPF calculation into pieces.

You are not recommended to change the default setting.

Examples # Set the duration of each sliced SPF calculation to 1 second.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] spf-slice-size 1000
```

summary

Syntax **summary** *ip-address* { *mask* | *mask-length* } [**avoid-feedback** | **generate_null0_route** | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] *
undo summary *ip-address* { *mask* | *mask-length* } [**level-1** | **level-1-2** | **level-2**]

View IS-IS view

Parameters *ip-address*: Destination IP address of a summary route.

mask: Mask of the destination IP address, in dotted decimal format.

mask-length: Mask length, in the range of 0 to 32.

avoid-feedback: Specifies to avoid learning aggregate routes by routing calculation.

generate_null0_route: Specifies to generate the Null 0 route to avoid routing loops.

tag *tag*: Specifies a management tag, in the range of 1 to 4294967295.

level-1: Specifies to summarize only the routes redistributed to Level-1 area.

level-1-2: Specifies to summarize all the routes redistributed to the Level-1 and Level-2 areas.

level-2: Specifies to summarize only the routes redistributed to the Level-2 area.

Description Use the **summary** command to configure a summary route.

Use the **undo summary** command to remove a summary route.

No summarization is configured by default.

If no level is specified, only the **level-2** routes will be summarized by default.

You can summarize multiple contiguous networks with a summary network to reduce the size of the routing table, as well as that of LSP and LSDB generated by the router. It is allowed to summarize native IS-IS routes and redistributed routes.

After summarization, the cost of the summary route is the smallest cost of those summarized routes.

Note that the router summarizes only routes in local LSPs.

Examples # Configure a summary route of 202.0.0.0/8.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] summary 202.0.0.0 255.0.0.0
```

timer isp-generation

Syntax **timer isp-generation** *maximum-interval* [*initial-interval* [*incremental-interval*]] [**level-1** | **level-2**]

undo timer isp-generation [**level-1** | **level-2**]

View IS-IS view

Parameters *maximum-interval*: Maximum interval in seconds for generating ISIS LSPs, in the range 1 to 120.

initial-interval: Initial interval in milliseconds for generating ISIS LSPs, in the range 10 to 60000. The default is 0.

incremental-interval: Incremental interval (in milliseconds), in the range 10 to 60000. The default is 0.

level-1: Applies the specified intervals to generating level-1 LSPs.

level-2: Applies the specified intervals to generating level-1 LSPs.

Description Use the **timer isp-generation** command to specify intervals for ISIS LSP generation.

Use the **undo timer isp-generation** command to restore the default.

By default, the LSP generation interval is 2 seconds.



- *If only the maximum interval is specified, this maximum interval is the LSP generation interval.*
- *If both the maximum and initial intervals are specified, the system can adjust the LSP generation interval upon topology changes. When the topology is stable, the initial interval applies as the LSP generation interval. When topology changes become frequent, the LSP generation interval is the maximum or initial interval.*
- *If all the maximum, initial and incremental intervals are specified, the system will adjust the LSP generation interval upon topology changes in this way: when the network changes are infrequent, the initial interval applies as the LSP generation interval. When the network changes become frequent, the*

generation interval changes between the initial and maximum intervals based on the specified incremental interval.

By using this command to adjust the LSP generation interval, you can save the bandwidth and router resources that may be wasted due to frequent network changes.

Examples # Set the maximum LSP generation interval to 10 seconds, initial interval to 100 milliseconds and the incremental interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer lsp-generation 10 100 200
```

Set the maximum LSP generation interval to 15 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer lsp-generation 15
```

timer lsp-max-age

Syntax **timer lsp-max-age** *seconds*

undo timer lsp-max-age

View IS-IS view

Parameters *seconds*: Specifies the LSP maximum aging time in seconds, ranging from 1 to 65535.

Description Use the **timer lsp-max-age** command to set the LSP maximum aging time for the current router.

Use the **undo timer lsp-max-age** command to restore the default.

The default is 1200 seconds.

A router puts the specified LSP maximum aging time into an LSP before advertisement. When the LSP is received by other routers, the aging time will decrease as the time goes by. If no update is received for the LSP after its aging time decreases to 0, the LSP will be deleted from the LSDB.

Related commands: **timer lsp-refresh.**

Examples # Set the maximum LSP aging time to 1500 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] timer lsp-max-age 1500
```

timer lsp-refresh

Syntax **timer lsp-refresh** *seconds*

undo timer lsp-refresh

View IS-IS view

Parameters *seconds*: Specifies the LSP refresh interval in seconds, ranging from 1 to 65534.

Description Use the **timer lsp-refresh** command to set the LSP refresh interval.

Use the **undo timer lsp-refresh** to restore the default.

The default is 900 seconds.

Using this feature, you can keep LSPs in synchronization for the whole area.

Related commands: **timer lsp-max-age**.



To refresh LSPs before they are aged out, the interval set by the **timer lsp-refresh** command must be smaller than that set by the **timer lsp-max-age** command.

Examples # Set the LSP refresh interval to 1500 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] timer lsp-refresh 1500
```

timer spf

Syntax **timer spf** *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo timer spf

View IS-IS view

Parameters *maximum-interval*: Specifies the maximum interval (in seconds) for SPF calculations, ranging from 1 to 120.

minimum-interval: Specifies the minimum interval (in milliseconds) for SPF calculations, ranging from 10 to 60000.

incremental-interval: Specifies the incremental interval (in milliseconds) for SPF calculations, ranging from 10 to 60000.

Description Use the **timer spf** command to set the time intervals for ISIS routing calculation.

Use the **undo timer spf** command to restore the default.

The default IS-IS SPF calculation interval is 10 seconds.

When the network changes are infrequent, the SPF calculation interval decreases to the minimum interval. When the network changes become frequent, the calculation interval is increased by $inc_interval * (2^{n-2})$, (n is the number of network changes that triggered SPF calculations) until the maximum interval is reached.

With this feature, you can prevent the router from over consumption due to frequent network changes.

Examples # Set the maximum SPF calculation interval to 10 seconds, minimum interval to 100 milliseconds and the incremental interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer spf 10 100 200
```

Set the maximum SPF calculation interval to 15 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer spf 15
```

virtual-system

Syntax **virtual-system** *virtual-system-id*

undo virtual-system *virtual-system-id*

View IS-IS view

Parameters *virtual-system-id*: Virtual system ID of the IS-IS process.

Description Use the **virtual-system** command to configure a virtual system ID for the IS-IS process. No extended LSPs are generated without the virtual system ID.

Use the **undo virtual-system** command to remove the virtual system ID.

By default, no virtual system ID is configured for the IS-IS process.

Examples # Set a virtual system ID of 2222.2222.2222 for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] virtual-system 2222.2222.2222
```


26

BGP CONFIGURATION COMMANDS



The term “router” in this document refers to a generic router or an Ethernet switch running routing protocols.



For routing policy configuration commands, refer to “Routing Policy Common Configuration Commands” on page 447 and “IPv4 Routing Policy Configuration Commands” on page 467.

aggregate

Syntax **aggregate** *ip-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate *ip-address* { *mask* | *mask-length* }

View BGP view

Parameters *ip-address*: Summary address.

mask: Summary mask, in dotted decimal notation.

mask-length: Summary mask length, in the range 0 to 32.

as-set: Creates a summary with AS set.

attribute-policy *route-policy-name*: Sets the attributes of the summary route according to the routing policy, the name of which is a string of 1 to 19 characters.

detail-suppressed: Only advertises the summary route.

suppress-policy *route-policy-name*: Suppresses specific routes defined in the routing policy, the name of which is a string of 1 to 19 characters.

origin-policy *route-policy-name*: References the routing policy to specify routes for summarization. The policy name is a string of 1 to 19 characters.

The keywords of the command are described as follows:

Table 92 Functions of the keywords

| Keywords | Function |
|--------------------------|--|
| as-set | Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of routes may lead to route oscillation. |
| detail-suppressed | This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the peer filter-policy command. |
| suppress-policy | Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the if-match clause of the route-policy command. |
| origin-policy | Selects only routes satisfying the routing policy for route summarization |
| attribute-policy | Sets attributes except the AS-PATH attribute for the summary route. The same work can be done by using the peer route-policy command. |

Description Use the **aggregate** command to create a summary route in the BGP routing table.

Use the **undo aggregate** command to remove a summary route.

By default, no summary route is configured.

Examples # In BGP view, create a summary of 192.213.0.0/16 in the BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] aggregate 192.213.0.0 255.255.0.0
```

balance

Syntax **balance** *number*

undo balance

View BGP view

Parameters *number*: Number of BGP routes for load balancing. Its range varies with devices. When it is set to 1, load balancing is disabled.

Description Use the **balance** command to configure the number of BGP routes for load balancing.

Use the **undo balance** command to disable load balancing.

By default, no load balancing is configured.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing using route selection rules.

Related commands: **display bgp routing-table.**

Examples # In BGP view, set the number of routes participating in BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] balance 2
```

bestroute as-path-neglect

Syntax **bestroute as-path-neglect**
undo bestroute as-path-neglect

View BGP view

Parameters None

Description Use the **bestroute as-path-neglect** command to configure the BGP router to not evaluate the AS_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure the BGP router to take the AS_PATH as a factor during best route selection.

By default, the router takes AS_PATH as a factor when selecting the best route.

Examples # In BGP view, ignore AS_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute as-path-neglect
```

bestroute compare-med

Syntax **bestroute compare-med**
undo bestroute compare-med

View BGP view

Parameters None

Description Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.



CAUTION: After the **bestroute compare-med** command is executed, the **balance** command does not take effect.

Examples # In BGP view, enable the comparison of MEDs for paths from each AS when selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute compare-med
```

bestroute med-confederation

Syntax **bestroute med-confederation**

undo bestroute med-confederation

View BGP view

Parameters None

Description Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers to select the optimal route.

Use the **undo bestroute med-confederation** command to disable the comparison.

The comparison is not enabled by default.

The system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples # In BGP view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute med-confederation
```

bgp

Syntax **bgp** *as-number*

undo bgp [*as-number*]

View System view

Parameters *as-number*: Specifies the local AS number from 1 to 65535.

Description Use the **bgp** command to enable BGP and enter the BGP view.

Use the **undo bgp** command to disable BGP.

By default, BGP is not enabled.

Examples # Enable BGP and set local AS number to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]
```

compare-different-as-med

Syntax **compare-different-as-med**
undo compare-different-as-med

View BGP view

Parameters None

Description Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If there are several paths for one destination available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

Examples # In BGP view, enable to compare the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] compare-different-as-med
```

confederation id

Syntax **confederation id** *as-number*
undo confederation id

View BGP view

Parameters *as-number*: Number of the AS that contains multiple sub-ASs, in the range 1 to 65535.

Description Use the **confederation id** command to configure a confederation ID.

Use the **undo confederation id** command to remove a specified confederation.

By default, no confederation ID is configured.

Configuring a confederation can reduce IBGP connections in a large AS. You can split the AS into several sub-ASs, and each sub-AS remains fully meshed. These sub-ASs form a confederation. Key IGP attributes of a route, such as the next hop, MED, local preference, are not discarded when crossing each sub-AS. The sub-ASs still look like a whole from the perspective of other ASs. This can ensure the integrity of the former AS, and solve the problem of too many IBGP connections in the AS.

Related commands: **confederation nonstandard** and **confederation peer-as**.

Examples # Confederation 9 consists of four sub-ASs, namely, 38, 39, 40 and 41. The peer 10.1.1.1 is a member of the confederation while the peer 200.1.1.1 is outside of the confederation. Take sub AS 41 as an example.

```
<Sysname> system-view
[Sysname] bgp 41
[Sysname-bgp] confederation id 9
[Sysname-bgp] confederation peer-as 38 39 40
[Sysname-bgp] group Confed38 external
[Sysname-bgp] peer Confed38 as-number 38
[Sysname-bgp] peer 10.1.1.1 group Confed38
[Sysname-bgp] group Remote98 external
[Sysname-bgp] peer Remote98 as-number 98
[Sysname-bgp] peer 200.1.1.1 group Remote98
```

confederation nonstandard

Syntax **confederation nonstandard**

undo confederation nonstandard

View BGP view

Parameters None

Description Use the **confederation nonstandard** command to make the router compatible with routers not compliant with RFC3065 in the confederation.

Use the **undo confederation nonstandard** command to restore the default.

By default, all routers in the confederation comply with RFC3065.

All devices should be configured with this command to interact with those nonstandard devices in the confederation.

Related commands: **confederation id** and **confederation peer-as**.

Examples # AS100 contains routers not compliant with RFC3065 and comprises two sub-ASs, 64000 and 65000.

```
<Sysname> system-view
[Sysname] bgp 64000
[Sysname-bgp] confederation id 100
[Sysname-bgp] confederation peer-as 65000
[Sysname-bgp] confederation nonstandard
```

confederation peer-as

Syntax **confederation peer-as** *as-number-list*

undo confederation peer-as [*as-number-list*]

View BGP view

Parameters *as-number-list*: Sub-AS number list. Up to 32 sub-ASs can be configured in one command line. The expression is *as-number-list* = *as-number* &<1-32>, in which *as-number* specifies a sub-AS number, and &<1-32> indicates up to 32 numbers can be specified.

Description Use the **confederation peer-as** command to specify confederation peer sub-ASs.

Use the **undo confederation peer-as** command to remove specified confederation peer sub-ASs.

By default, no confederation peer sub-ASs are configured.

Before this configuration, the **confederation id** command must be used to specify the confederation for the sub-ASs.

If the **undo confederation peer-as** command without the *as-number-list* argument is used, all confederation peer sub-ASs are removed.

Related commands: **confederation nonstandard** and **confederation id**.

Examples # Specify confederation peer sub ASs 2000 and 2001.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] confederation id 10
[Sysname-bgp] confederation peer-as 2000 2001
```

dampening

Syntax **dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View BGP view

Parameters *half-life-reachable*: Specifies a half-life for active routes from 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies a half-life for suppressed routes from 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies a reuse threshold value for suppressed routes from 1 to 20000. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750.

suppress: Specifies a suppression threshold from 1 to 20000. The route with a penalty value higher than the threshold is suppressed. The default value is 2000.

ceiling: Specifies a ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

half-life-reachable, *half-life-unreachable*, *reuse*, *suppress* and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

Description Use the **dampening** command to enable BGP route dampening and/or configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

The command dampens only EBGp routes rather than IBGP routes.

Related commands: **reset bgp dampening**, **reset bgp flap-info**, **display bgp routing-table dampened**, **display bgp routing-table dampening parameter** and **display bgp routing-table flap-info**.

Examples # In BGP view, configure BGP route dampening.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] dampening 15 15 1000 2000 10000
```

default ipv4-unicast

Syntax **default ipv4-unicast**

undo default ipv4-unicast

View BGP view

| | |
|--------------------|--|
| Parameters | None |
| Description | <p>Use the default ipv4-unicast command to enable the use of IPv4 unicast address family for all peers.</p> <p>Use the undo default ipv4-unicast command to disable the use of IPv4 unicast address family for all peers.</p> <p>The use of IPv4 unicast address family is enabled by default.</p> |
| Examples | <pre># Enable IPv4 unicast address family for all neighbors. <Sysname> system-view [Sysname] bgp 100 [Sysname-bgp] default ipv4-unicast</pre> |

default local-preference

| | |
|--------------------|---|
| Syntax | <p>default local-preference <i>value</i></p> <p>undo default local-preference</p> |
| View | BGP view |
| Parameters | <i>value</i> : Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is. |
| Description | <p>Use the default local-preference command to configure the default local preference.</p> <p>Use the undo default local-preference command to restore the default value.</p> <p>By default, the default local preference is 100.</p> <p>Using this command can affect BGP route selection.</p> |
| Examples | <pre># In BGP view, set the default local preference to 180. <Sysname> system-view [Sysname] bgp 100 [Sysname-bgp] default local-preference 180</pre> |

default med

| | |
|---------------|---|
| Syntax | <p>default med <i>med-value</i></p> <p>undo default med</p> |
| View | BGP view |

Parameters *med-value*: Default MED value, in the range 0 to 4294967295.

Description Use the **default med** command to specify a default MED value.

Use the **undo default med** command to restore the default.

By default, the default *med-value* is 0.

Multi-exit discriminator (MED) is an external metric for routes. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with an identical destination but different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system first selects the route with the smallest MED as the best external route.

Examples # In BGP view, configure the default MED as 25.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default med 25
```

default-route imported

Syntax **default-route imported**

undo default-route imported

View BGP view

Parameters None

Description Use the **default-route imported** command to allow default route redistribution into the BGP routing table.

Use the **undo default-route imported** command to disallow the redistribution.

By default, default route redistribution is not allowed.

Using the **default-route imported** command cannot redistribute default routes. To do so, use the **import-route** command.

Related commands: **import-route**.

Examples # In BGP view, allow default route redistribution from OSPF into BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default-route imported
[Sysname-bgp] import-route ospf 1
```

display bgp group

Syntax **display bgp group** [*group-name*]

View Any view

Parameters *group-name*: Peer group name, a string of 1 to 47 characters.

Description Use the **display bgp group** command to display the information of the peer group.

Examples # Display the information of the peer group **aaa**.

```
<Sysname> display bgp group aaa
```

```
BGP peer-group is aaa
remote AS 200
Type : external
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Peer Preferred Value: 0
No routing policy is configured
Members:
Peer          V    AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
-----
2.2.2.1      4    200      0         0       0         0 00:00:35 Active
```

Table 93 Field descriptions of the display bgp group command

| Field | Description |
|---|---|
| BGP peer-group | Name of the BGP peer group |
| remote AS | AS number of peer group |
| type | Type of the BGP peer group: IBGP or EBGP |
| Maximum allowed prefix number | Maximum allowed prefix number |
| Threshold | Threshold value |
| Configured hold timer value | Holdtime interval |
| Keepalive timer value | Keepalive interval |
| Minimum time between advertisement runs | Minimum time between advertisement runs |
| Peer Preferred Value | Preferred value of the routes from the peer |
| No routing policy is configured | No routing policy is configured for the peer |
| Members | Detailed information of the members in the peer group |
| Peer | IPv4 address of the peer |
| V | BGP version running on peers |
| AS | AS number of the peers |
| MsgRcvd | Number of messages received |
| MsgSent | Number of messages sent |
| OutQ | Number of messages to be sent |
| PrefRcv | Number of prefixes received |

Table 93 Field descriptions of the display bgp group command

| Field | Description |
|---------|--|
| Up/Down | The lasting time of a session/the lasting time of present state (when no session is established) |
| State | State machine of peer |

display bgp network

Syntax **display bgp network**

View Any view

Parameters None

Description Use the **display bgp network** command to display routing information that has been advertised.

Examples # Display routing information that has been advertised.

```
<Sysname> display bgp network
```

```
BGP Local Router ID is 10.1.4.2.
```

```
Local AS Number is 400.
```

```
Network           Mask           Route-policy     Short-cut
```

```
100.1.1.2.0       255.255.255.0
```

```
100.1.1.1.0       255.255.255.0           Short-cut
```

Table 94 Field descriptions of the display bgp network command

| Field | Description |
|---------------------|---------------------|
| BGP Local Router ID | BGP Local Router ID |
| Local AS Number | Local AS Number |
| Network | Network address |
| Mask | Mask |
| Route-policy | Routing policy |
| Short-cut | Short-cut route |

display bgp paths

Syntax **display bgp paths** [*as-regular-expression*]

View Any view

Parameters *as-regular-expression*: AS path regular expression.

Description Use the **display bgp paths** command to display information about BGP paths.

Examples # Display information about BGP paths matching the AS path regular expression.
 <Sysname> display bgp paths ^200

```

      Address      Hash      Refcount  MED      Path/Origin
      0x5917100    11        1          200      300i
  
```

Table 95 Field descriptions of the display bgp paths command

| Field | Description |
|----------|---|
| Address | Route address in local database, in dotted hexadecimal notation |
| Hash | Hash index |
| Refcount | Count of routes that referenced the path |
| MED | MED of the path |
| Path | AS_PATH attribute of the path, recording the ASs it has passed, for avoiding routing loops |
| Origin | Origin attribute of the route: <ul style="list-style-type: none"> i Indicates the route is interior to the AS.
Summary routes and routes defined using the network command are considered IGP routes. e Indicates that a route is learned from the exterior gateway protocol (EGP). ? Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. |

display bgp peer

Syntax **display bgp peer** [*ip-address* { **log-info** | **verbose** }] *group-name* **log-info** | **verbose**]

View Any view

Parameters *ip-address*: IP address of an peer to be displayed, in dotted decimal notation.
group-name: Name of a peer group to be displayed, a string of 1 to 47 characters.
log-info: Displays the log information of the specified peer.
verbose: Displays the detailed information of the peer/peer group.

Description Use the **display bgp peer** command to display peer/peer group information.

Examples # Display the detailed information of the peer 10.110.25.20.

```
<Sysname> display bgp peer 10.110.25.20 verbose
```

```

Peer: 10.110.25.20 Local: 2.2.2.2
Type: EBGp link
BGP version 4, remote router ID 1.1.1.1
BGP current state: Established, Up for 00h01m51s
BGP current event: RecvKeepalive
BGP last state: OpenConfirm
Port: Local - 1029 Remote - 179
Configured: Active Hold Time: 180 sec Keepalive Time: 60 sec
Received : Active Hold Time: 180 sec
  
```

```

Negotiated: Active Hold Time: 180 sec
Peer optional capabilities:
Peer support bgp multi-protocol extended
Peer support bgp route refresh capability
Address family IPv4 Unicast: advertised and received

Received: Total 5 messages, Update messages 1
Sent: Total 4 messages, Update messages 0
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
Peer Preferred Value: 0

Routing policy configured:
No routing policy is configured

```

Table 96 Field descriptions of the display bgp peer command

| Field | Description |
|---|--|
| Peer | IP address of the peer |
| Local | Local router ID |
| Type | Peer type: Internal as IBGP peers and External as EBGP peers. |
| BGP version | BGP protocol version |
| remote router ID | Router ID of the peer |
| BGP current state | Current state of the peer |
| BGP current event | Current event of the peer |
| BGP last state | Last state of the peer |
| Port | Port number of local router and its peer |
| Configured: Active Hold Time | Local holdtime interval |
| Keepalive Time | Local keepalive interval |
| Received: Active Hold Time | Remote holdtime interval |
| Negotiated: Active Hold Time | Negotiated holdtime interval |
| Peer optional capabilities | Optional capabilities supported by the peer, including BGP multiple extension and routing refresh. |
| Address family IPv4 Unicast | Routes are advertised and received in the form of IPv4 unicast |
| Received | Total numbers of received packets and updates |
| Sent | Total numbers of sent packets and updates |
| Maximum allowed prefix number | Maximum allowed prefix number |
| Threshold | Threshold value |
| Minimum time between advertisement runs | Minimum time between route advertisements |
| Optional capabilities | Optional capabilities enabled by the peer |
| Peer Preferred Value | Preferred value specified for the routes from the peer |
| Routing policy configured | Local routing policy |

display bgp routing-table

Syntax **display bgp routing-table** [*ip-address* [{ *mask* | *mask-length* } [*longer-prefixes*]]]

View Any view

Parameters *ip-address*: Destination IP address.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

longer-prefixes: Matches the longest prefix.

Description Use the **display bgp routing-table** command to display specified BGP routing information in the BGP routing table.

Examples # Display BGP routing table information.

```
<Sysname> display bgp routing-table

Total Number of Routes: 1

BGP Local router ID is 10.10.10.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
      Network          NextHop          MED          LocPrf          PrefVal Path/Ogn
* > 40.40.40.0/24      20.20.20.1              0            200 300i
```

Table 97 Field descriptions of the display bgp routing command

| Field | Description |
|------------------------|---|
| Total Number of Routes | Total Number of Routes |
| BGP Local router ID | BGP Local router ID |
| Status codes | Status codes:
* - valid
> - best
d - damped
h - history
i - internal (IGP)
s - summary suppressed (suppressed)
S - Stale |
| Origin | i - IGP (originated in the AS)
e - EGP (learned through EGP)
? - incomplete (learned by other means) |
| Network | Destination network address |
| Next Hop | Next hop IP address |

Table 97 Field descriptions of the display bgp routing command

| Field | Description |
|---------|---|
| MED | MULTI_EXIT_DISC attribute |
| LocPrf | Local preference value |
| PrefVal | Preferred value of the route |
| Path | AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops |
| PrefVal | Preferred value |
| Ogn | Origin attribute of the route, one of the following values: <ul style="list-style-type: none"> i Indicates that the route is interior to the AS.
Summary routes and the routes configured using the network command are considered IGP routes. e Indicates that the route is learned via the exterior gateway protocol (EGP). ? Short for INCOMPLETE. It indicates that the origin of the route is unknown and the route is learned by other means. |

display bgp routing-table as-path-acl

Syntax `display bgp routing-table as-path-acl as-path-acl-number`

View Any view

Parameters *as-path-acl-number*: Displays routing information permitted by the AS path ACL, which is specifies with a number from 1 to 256.

Description Use the **display bgp routing as-path-acl** command to display BGP routes permitted by an as-path ACL.

Examples # Display BGP routes permitted by AS path ACL 1.

```
<Sysname> display bgp routing-table as-path-acl 1

BGP Local router ID is 20.20.20.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
      Network          NextHop          MED          LocPrf          PrefVa
1 Path/Ogn

*> 40.40.40.0/24      30.30.30.1      0              0              30
0i
```

Refer to Table 97 for description on the fields above.

display bgp routing-table cidr

Syntax `display bgp routing-table cidr`

| | |
|--------------------|---|
| View | Any view |
| Parameters | None |
| Description | Use the display bgp routing-table cidr command to display BGP CIDR (Classless Inter-Domain Routing) routing information. |
| Examples | <pre># Display BGP CIDR routing information. <Sysname> display bgp routing-table cidr BGP Local router ID is 20.20.20.1 Status codes: * - valid, > - best, d - damped, h - history, i - internal, s - suppressed, S - Stale Origin : i - IGP, e - EGP, ? - incomplete Network NextHop MED LocPrf PrefVal Path/Ogn *> 40.40.40.0/24 30.30.30.1 0 0 300i</pre> <p>Refer to Table 97 for description on the above fields.</p> |

display bgp routing-table community

| | |
|--------------------|--|
| Syntax | display bgp routing-table community [<i>aa:nn</i> &<1-13>] [no-advertise no-export no-export-subconfed] * [whole-match] |
| View | Any view |
| Parameters | <p><i>aa:nn</i>: Community number. Both aa and nn are in the range 0 to 65535.</p> <p>&<1-13>: Argument before it can be entered up to 13 times.</p> <p>no-advertise: Displays BGP routes that are not advertised to any peer.</p> <p>no-export: Displays routes that are not advertised outside the AS. With a confederation configured, it displays routes that are not advertised outside the confederation, but can be advertised to other sub ASs in the confederation.</p> <p>no-export-subconfed: Displays routes that are neither advertised outside the AS nor to other sub ASs in a configured confederation.</p> <p>whole-match: Displays the exactly matched routes.</p> |
| Description | Use the display bgp routing-table community command to display BGP routing information with the specified BGP community. |
| Examples | <pre># Display routing information with the specified BGP community. <Sysname> display bgp routing-table community 11:22 BGP Local router ID is 10.10.10.1 Status codes: * - valid, > - best, d - damped, h - history, i - internal, s - suppressed, S - Stale Origin : i - IGP, e - EGP, ? - incomplete Network NextHop MED LocPrf PrefVal Path/Ogn</pre> |

```
*> 10.10.10.0/24      0.0.0.0      0      0      i
*> 40.40.40.0/24      20.20.20.1    0      0      200 300i
```

Refer to Table 97 for description on the fields above.

display bgp routing-table community-list

Syntax **display bgp routing-table community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

View Any view

Parameters *basic-community-list-number*: Specifies a basic community-list number from 1 to 99.

adv-community-list-number: Specifies an advanced community-list number from 100 to 199.

whole-match: Displays routes exactly matching the specified *basic-community-list*.

&<1-16>: Specifies the argument before it can be entered up to 16 times.

Description Use the **display bgp routing-table community-list** command to display BGP routing information matching the specified BGP community list.

Examples # Display BGP routing information matching BGP community list 100.

```
<Sysname> display bgp routing-table community-list 100

BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
   Network          NextHop      MED          LocPrf      PrefVal Path/Ogn
*> 30.30.30.0/24    0.0.0.0        0            0           0      i
*> 40.40.40.0/24    0.0.0.0        0            0           0      i
```

Refer to Table 97 for description on the fields above.

display bgp routing-table dampened

Syntax **display bgp routing-table dampened**

View Any view

Parameters None

Description Use the **display bgp routing-table dampened** command to display dampened BGP routes.

Examples # Display dampened BGP routes.

```
<Sysname> display bgp routing-table dampened
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
      Network          From          Reuse      Path/Origin
*d  77.0.0.0          12.1.1.1      00:29:20  100?
```

Table 98 Field descriptions of the display bgp routing-table dampened command

| Field | Description |
|-------|--|
| From | IP address from which the route was received |
| Reuse | Reuse time of the route |

Refer to Table 97 for description on the other fields above.

display bgp routing-table dampening parameter

Syntax **display bgp routing-table dampening parameter**

View Any view

Parameters None

Description Use the **display bgp routing-table dampening parameter** command to display BGP route dampening parameters.

Related commands: **dampening.**

Examples # Display BGP route dampening parameters.

```
<Sysname> display bgp routing-table dampening parameter
Maximum Suppress Time(in second) : 3069
Ceiling Value                      : 16000
Reuse Value                        : 750
HalfLife Time(in second)           : 900
Suppress-Limit                     : 2000
```

Table 99 Field descriptions of the display bgp routing-table dampening parameter command

| Field | Description |
|-----------------------|--------------------------------------|
| Maximum Suppress Time | Maximum Suppress Time |
| Ceiling Value | Upper limit of penalty value |
| Reuse Value | Limit for a route to be desuppressed |
| HalfLife Time | Half-life time of active routes |
| Suppress-Limit | Limit for a route to be suppressed |

display bgp routing-table different-origin-as

- Syntax** **display bgp routing-table different-origin-as**
- View** Any view
- Parameters** None
- Description** Use the **display bgp routing-table different-origin-as** command to display BGP routes originating from different autonomous systems.
- Examples** # Display BGP routes originating from different ASs.

```
<Sysname> display bgp routing-table different-origin-as
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
      Network          NextHop          MED          LocPrf          PrefVal Path/Ogn
* > 55.0.0.0          12.1.1.1          0              0              100?
*          14.1.1.2          0              0              300?
```

Refer to Table 97 for description on the fields above.

display bgp routing-table flap-info

- Syntax** **display bgp routing-table flap-info** [**regular-expression** *as-regular-expression* | **as-path-acl** *as-path-acl-number* | *ip-address* [{ *mask* | *mask-length* }] [**longer-match**]]]
- View** Any view
- Parameters** *as-regular-expression*: Displays route flap information that matches the AS path regular expression.
- as-path-acl-number*: Displays route flap information matching the AS path ACL. The number is in the range 1 to 256.
- ip-address*: Destination IP address.
- mask*: Mask, in dotted decimal notation.
- mask-length*: Mask length, in the range 0 to 32.
- longer-match**: Matches the longest prefix.
- Description** Use the **display bgp routing-table flap-info** command to display BGP route flap statistics. If no parameter is specified, this command displays all BGP route flap statistics.

Examples # Display BGP route flap statistics.

```
<Sysname> display bgp routing-table flap-info
```

```
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
      Network      From          Flaps  Duration  Reuse      Path/Origin
* > 55.0.0.0       12.1.1.1    2      00:00:16
*d 77.0.0.0       12.1.1.1    5      00:34:02  00:27:08  100?
```

Table 100 Field descriptions of the display bgp routing flap-info command

| Field | Description |
|----------|---------------------------------|
| From | Source IP address of the route |
| Flaps | Number of routing flaps |
| Duration | Duration time of the flap route |
| Reuse | Reuse time of the flap route |

Refer to Table 97 for description on the other fields above.

display bgp routing-table peer

Syntax **display bgp routing-table peer** *ip-address* { **advertised-routes** | **received-routes** } [*network-address* [*mask* | *mask-length*]] | **statistic**]

View Any view

Parameters *ip-address*: IP address of a peer.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

network-address: IP address of the destination network.

mask: Mask of the destination network, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

statistic: Displays route statistics.

Description Use the **display bgp routing-table peer** command to display BGP routing information advertised to or received from the specified BGP peer.

Related commands: **display bgp peer**.

Examples # Display BGP routing information advertised to BGP peer 20.20.20.1.

```
<Sysname> display bgp routing-table peer 20.20.20.1 advertised-routes
```

```
Total Number of Routes: 2
```

```

BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
      Network          NextHop          MED          LocPrf          PrefVal Path/Ogn
*> 30.30.30.0/24      0.0.0.0          0              0              i
*> 40.40.40.0/24      0.0.0.0          0              0              i

```

Refer to Table 97 for description on the fields above.

display bgp routing-table regular-expression

Syntax `display bgp routing-table regular-expression as-regular-expression`

View Any view

Parameters *as-regular-expression*: AS regular expression.

Description Use the **display bgp routing-table regular-expression** command to display BGP routing information matching the specified AS regular expression.

Examples # Display BGP routing information matching AS regular expression 300\$.

```

<Sysname> display bgp routing-table regular-expression 300$

BGP Local router ID is 20.20.20.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
      Network          NextHop          MED          LocPrf          PrefVal Path/Ogn
*> 40.40.40.0/24      30.30.30.1      0              0              300i

```

Refer to Table 97 for description on the fields above.

display bgp routing-table statistic

Syntax `display bgp routing-table statistic`

View Any view

Parameters None

Description Use the **display bgp routing-table statistic** command to display BGP routing statistics.

Examples # Display BGP routing statistics.

```

<Sysname> display bgp routing-table statistic

Total Number of Routes: 4

```

Table 101 Field descriptions of the display bgp routing-table statistic command

| Field | Description |
|------------------------|------------------------|
| Total number of routes | Total number of routes |

ebgp-interface-sensitive

Syntax **ebgp-interface-sensitive**

undo ebgp-interface-sensitive

View BGP view

Parameters None

Description Use the **ebgp-interface-sensitive** command to enable the clearing of EBGp session on any interface that becomes down.

Use the undo **ebgp-interface-sensitive** command to disable the function.

This function is enabled by default.

Examples # In BGP view, enable the clearing of EBGp session on any interface that becomes down.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ebgp-interface-sensitive
```

filter-policy export

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

undo filter-policy export [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

View BGP view

Parameters *acl-number*: Number of an ACL used to filter outgoing redistributed routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter outgoing redistributed routing information, a string of 1 to 19 characters.

direct: Filters direct routes.

isis *process-id*: Filters outgoing routes redistributed from an ISIS process. The ID is in the range 1 to 65535.

ospf *process-id*: Filters outgoing routes redistributed from the OSPF process with an ID from 1 to 65535.

rip *process-id*: Filters outgoing routes redistributed from a RIP process. The ID is in the range 1 to 65535.

static: Filters static routes.

If no routing protocol is specified, all outgoing routes are filtered.

Description Use the **filter-policy export** command to filter outgoing redistributed routes and only the routes permitted by the specified filter can be advertised.

Use the **undo filter-policy export** command to remove the filtering.

If no routing protocol is specified, the filtering applies to all outgoing redistributed routes.

By default, the filtering is not configured.

Examples # In BGP view, reference ACL 2000 to filter all outgoing redistributed routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 export
```

filter-policy import

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy import

View BGP view

Parameters *acl-number*: Number of an ACL used to filter incoming routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter incoming routing information, a string of 1 to 19 characters.

Description Use the **filter-policy import** command to configure the filtering of incoming routing information.

Use the **undo filter-policy import** command to disable the filtering.

By default, incoming routing information is not filtered.

Examples # In BGP view, reference ACL 2000 to filter incoming routing information.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 import
```

group

Syntax `group group-name [external | internal]`

`undo group group-name`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

external: Creates an EBGP peer group, which can be the group of another sub AS in a confederation.

internal: Creates an IBGP peer group.

Description Use the **group** command to create a peer group.

Use the **undo group** command to delete a peer group.

An IBGP peer group is created if neither **internal** nor **external** is specified.

Examples # In BGP view, create an EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] peer 10.1.1.1 group test
[Sysname-bgp] peer 10.1.2.1 group test
```

import-route

Syntax `import-route protocol [process-id [med med-value | route-policy route-policy-name] *]`

`undo import-route protocol [process-id]`

View BGP view

Parameters *protocol*: Redistributes routes from the routing protocol, which can be **direct**, **isis**, **ospf**, **rip** and **static** at present.

process-id: Process ID, in the range 1 to 65535. It is available only when the protocol is **isis**, **ospf** or **rip**.

med-value: Specifies the MED value to be applied to redistributed routes, ranging from 0 to 4294967295. If the argument is not specified, the cost of the redistributed route is used as its MED in the BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes, a string of 1 to 19 characters.

Description Use the **import-route** command to configure BGP to redistribute routes from a specified routing protocol and advertise redistributed routes.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

By default, BGP does not redistribute routes from other protocols.

The ORIGIN attribute of routes redistributed with the **import-route** command is incomplete.

Examples # In BGP view, redistribute routes from RIP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] import-route rip
```

log-peer-change

Syntax **log-peer-change**

undo log-peer-change

View BGP view

Parameters None

Description Use the **log-peer-change** command to enable the global BGP logging on peers going up and down.

Use the **undo log-peer-change** command to disable the function.

By default, the function is enabled.

Examples # Enable BGP logging on peers going up and down.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] log-peer-change
```

network

Syntax **network** *ip-address* [*mask* | *mask-length*] [**short-cut** | **route-policy** *route-policy-name*]

undo network *ip-address* [*mask* | *mask-length*] [**short-cut**]

| | |
|--------------------|--|
| View | BGP view |
| Parameters | <p><i>ip-address</i>: Destination IP address.</p> <p><i>mask</i>: Mask of the network address, in dotted decimal notation.</p> <p><i>mask-length</i>: Mask length, in the range 0 to 32.</p> <p>short-cut: Specifies the route to use the local preference. If the route is an EBGP route whose preference is higher than the local one, using this keyword can configure the EBGP route to use the local preference, so the route is hard to become the optimal route.</p> <p><i>route-policy-name</i>: Routing policy applied to the route. The name is a string of 1 to 19 characters.</p> |
| Description | <p>Use the network command to advertise a network to the BGP routing table.</p> <p>Use the undo network command to remove a network from the routing table.</p> <p>By default, no network route is advertised.</p> <p>Note that:</p> <ul style="list-style-type: none"> ■ The network route must be in the local IP routing table, and using a routing policy makes route management more flexible. ■ The route advertised to the BGP routing table using the network command has the ORIGIN attribute as IGP. |
| Examples | <p># In BGP view, advertise the network segment 10.0.0.0/16.</p> <pre><Sysname> system-view [Sysname] bgp 100 [Sysname-bgp] network 10.0.0.0 255.255.0.0</pre> |

peer advertise-community

| | |
|--------------------|--|
| Syntax | <p>peer { <i>group-name</i> <i>ip-address</i> } advertise-community</p> <p>undo peer { <i>group-name</i> <i>ip-address</i> } advertise-community</p> |
| View | BGP view |
| Parameters | <p><i>group-name</i>: Name of a peer group, a string of 1 to 47 characters.</p> <p><i>ip-address</i>: IP address of a peer.</p> |
| Description | Use the peer advertise-community command to advertise the community attribute to a peer/peer group. |

Use the **undo peer advertise-community** command to disable the community attribute advertisement to a peer/peer group.

By default, no community attribute is advertised to any peer group/peer.

Related commands: **ip community-list, if-match community, apply community.**

Examples # In BGP view, advertise the community attribute to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-community
```

peer advertise-ext-community

Syntax **peer** { *group-name* | *ip-address* } **advertise-ext-community**

undo peer { *group-name* | *ip-address* } **advertise-ext-community**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to disable the advertisement.

By default, no extended community attribute is advertised to a peer/peer group.

Related commands: **ip extcommunity-list, if-match extcommunity, apply extcommunity.**

Examples # In BGP view, advertise the extended community attribute to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-ext-community
```

peer allow-as-loop

Syntax **peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ip-address* } **allow-as-loop**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

number: Specifies the repeating times of the local AS number, in the range 1 to 10. The default number is 1.

Description Use the **peer allow-as-loop** command to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the repeating times of the local AS number.

Use the **undo peer allow-as-loop** command to remove the configuration.

By default, the local AS number is not allowed.

Related commands: **display bgp routing-table peer**.

Examples # In BGP view, configure the repeating times of the local AS number as 2 for routes from peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 allow-as-loop 2
```

peer as-number

Syntax **peer** { *group-name* | *ip-address* } **as-number** *as-number*

undo peer *group-name* **as-number**

undo peer *ip-address*

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: AS number of the peer or peer group, in the range 1 to 65535.

Description Use the **peer as-number** command to specify the AS number for a peer/peer group.

Use the **undo peer as-number** command to delete the AS number of a peer group.

Use the **undo peer** command to delete a peer.

By default, no AS number is configured for a peer/peer group.

Examples # In BGP view, specify the AS number of the peer group **test** as 100.

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100

```

peer as-path-acl

Syntax `peer { group-name | ip-address } as-path-acl as-path-acl-number { export | import }`

`undo peer { group-name | ip-address } as-path-acl as-path-acl-number { export | import }`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-path-acl-number: AS path ACL number, in the range 1 to 256.

export: Filters outgoing routes.

import: Filters incoming routes.

Description Use the **peer as-path-acl** command to configure the filtering of routes incoming from or outgoing to a peer/peer group based on a specified AS path ACL.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path ACL filtering is configured.

Related commands: **peer as-path-acl**, **if-match as-path**, **apply as-path**.

Examples # In BGP view, reference the AS path ACL 1 to filter routes outgoing to the peer group **test**.

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-path-acl 1 export

```

peer capability-advertise conventional

Syntax `peer { group-name | ip-address } capability-advertise conventional`

`undo peer { group-name | ip-address } capability-advertise conventional`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

- Description** Use the **peer capability-advertise conventional** command to disable BGP multi-protocol extension and route refresh for a peer/peer group.
- Use the **undo peer capability-advertise conventional** command to enable BGP multi-protocol extension and route refresh for a peer/peer group.
- By default, BGP multi-protocol extension and route refresh are enabled.

Examples # In BGP view, disable multi-protocol extension and route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise conventional
```

peer capability-advertise route-refresh

Syntax **peer** { *group-name* | *ip-address* } **capability-advertise route-refresh**

undo peer { *group-name* | *ip-address* } **capability-advertise route-refresh**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer capability-advertise route-refresh** command to enable the BGP route refresh capability.

Use the **undo peer capability-advertise route-refresh** command to disable the capability.

The capability is enabled by default.

Examples # In BGP view, enable BGP route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise route-refresh
```

peer connect-interface

Syntax **peer** { *group-name* | *ip-address* } **connect-interface** *interface-type* *interface-number*

undo peer { *group-name* | *ip-address* } **connect-interface**

| | |
|--------------------|--|
| View | BGP view |
| Parameters | <p><i>group-name</i>: Name of a peer group, a string 1 to 47 characters.</p> <p><i>ip-address</i>: IP address of a peer.</p> <p><i>interface-type interface-number</i>: Specifies the type and number of the interface.</p> |
| Description | <p>Use the peer connect-interface command to specify the source interface for establishing TCP connections to a peer/peer group.</p> <p>Use the undo peer connect-interface command to restore the default.</p> <p>Note that:</p> <p>To establish multiple BGP connections to another BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router; otherwise, the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.</p> |
| Examples | <p># In BGP view, specify loopback 0 as the source interface for routing updates to the peer group test.</p> <pre><Sysname> system-view [Sysname] bgp 100 [Sysname-bgp] peer test connect-interface loopback 0</pre> |

peer default-route-advertise

| | |
|--------------------|--|
| Syntax | <pre>peer { group-name ip-address } default-route-advertise [route-policy route-policy-name]</pre> <pre>undo peer { group-name ip-address } default-route-advertise</pre> |
| View | BGP view |
| Parameters | <p><i>group-name</i>: Name of a peer group, a string of 1 to 47 characters.</p> <p><i>ip-address</i>: IP address of a peer.</p> <p><i>route-policy-name</i>: Routing policy name, a string of 1 to 19 characters.</p> |
| Description | <p>Use the peer default-route-advertise command to advertise a default route to a peer/peer group.</p> <p>Use the undo peer default-route-advertise command to disable default route advertisement to a peer/peer group.</p> <p>By default, no default route is advertised to a peer/peer group.</p> |

With this command used, the router unconditionally sends a default route with the next hop being itself to the peer/peer group regardless of whether the default route is available in the routing table.

Examples # In BGP view, advertise a default route to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test default-route-advertise
```

peer description

Syntax **peer** { *group-name* | *ip-address* } **description** *description-text*

undo peer { *group-name* | *ip-address* } **description**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

description-text: Description information for the peer/peer group, a string of 1 to 79 characters.

Description Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer/peer group.

Create a peer/peer group before configuring a description for it.

Related commands: **display bgp peer**.

Examples # In BGP view, configure the description information of the peer group test as ISP1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test description ISP1
```

peer ebgp-max-hop

Syntax **peer** { *group-name* | *ip-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *group-name* | *ip-address* } **ebgp-max-hop**

| | |
|--------------------|---|
| View | BGP view |
| Parameters | <p><i>group-name</i>: Name of a peer group, a string of 1 to 47 characters.</p> <p><i>ip-address</i>: IP address of a peer.</p> <p><i>hop-count</i>: Maximum hop count, in the range 1 to 255. The default is 64.</p> |
| Description | <p>Use the peer ebgp-max-hop command to allow establishing an EBGP connection with a peer/peer group that is on an indirectly connected network.</p> <p>Use the undo peer ebgp-max-hop command to restore the default.</p> <p>By default, this feature is disabled.</p> <p>You can use the argument <i>hop-count</i> to specify the maximum route hop count of the EBGP connection.</p> |
| Examples | <p># In BGP view, allow establishing the EBGP connection with the peer group test that is on an indirectly connected network.</p> <pre><Sysname> system-view [Sysname] bgp 100 [Sysname-bgp] peer test ebgp-max-hop</pre> |

peer enable

| | |
|--------------------|---|
| Syntax | <p>peer <i>ip-address</i> enable</p> <p>undo peer <i>ip-address</i> enable</p> |
| View | BGP view |
| Parameters | <i>ip-address</i> : IP address of a peer. |
| Description | <p>Use the peer enable command to enable the specified peer.</p> <p>Use the undo peer enable command to disable the specified peer.</p> <p>By default, the BGP peer is enabled.</p> <p>If a peer is disabled, the router will not exchange routing information with the peer.</p> |
| Examples | <p># Disable peer 18.10.0.9.</p> <pre><Sysname> system-view [Sysname] bgp 100 [Sysname-bgp] peer 18.10.0.9 group group1 [Sysname-bgp] undo peer 18.10.0.9 enable</pre> |

peer fake-as

Syntax `peer { group-name | ip-address } fake-as as-number`

`undo peer { group-name | ip-address } fake-as`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: Local autonomous system number, in the range 1 to 65535.

Description Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.



*The **peer fake-as** command is only applicable to an EBGP peer or peer group.*

Examples # In BGP view, configure a fake AS number of 200 for the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test fake-as 200
```

peer filter-policy

Syntax `peer { group-name | ip-address } filter-policy acl-number { export | import }`

`undo peer { group-name | ip-address } filter-policy [acl-number] { export | import }`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

acl-number: ACL number, in the range 2000 to 3999.

export: Applies the filter-policy to routes advertised to the peer/peer group.

import: Applies the filter-policy to routes received from the peer/peer group.

Description Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Related commands: **peer as-path-acl.**

Examples # In BGP view, apply the ACL 2000 to filter routes advertised to the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test filter-policy 2000 export
```

peer group

Syntax **peer** *ip-address* **group** *group-name* [**as-number** *as-number*]

undo peer *ip-address* **group** *group-name*

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: AS number of the peer, in the range 1 to 65535.

Description Use the **peer group** command to add a peer to a peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, no peer is added into a peer group.

Examples # In BGP view, add the peer 10.1.1.1 to the EBGp peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 2004
[Sysname-bgp] peer 10.1.1.1 group test
```

peer ignore

Syntax **peer** { *group-name* | *ip-address* } **ignore**

undo peer { *group-name* | *ip-address* } **ignore**

| | |
|--------------------|--|
| View | BGP view |
| Parameters | <p><i>group-name</i>: Name of a peer group, a string of 1 to 47 characters.</p> <p><i>ip-address</i>: IP address of a peer.</p> |
| Description | <p>Use the peer ignore command to disable session establishment with a peer or peer group.</p> <p>Use the undo peer ignore command to remove the configuration.</p> <p>By default, session establishment with a peer or peer group is allowed.</p> <p>After the peer ignore command is executed, the system disables the session with the specified peer or peer group and clears all the related routing information. For a peer group, this means all sessions with the peer group will be tore down.</p> |
| Examples | <pre># In BGP view, disable session establishment with peer 10.10.10.10. <Sysname> system-view [Sysname] bgp 100 [Sysname-bgp] peer 10.10.10.10 ignore</pre> |

peer ip-prefix

| | |
|--------------------|--|
| Syntax | <pre>peer { <i>group-name</i> <i>ip-address</i> } ip-prefix <i>ip-prefix-name</i> { export import } undo peer { <i>group-name</i> <i>ip-address</i> } ip-prefix { export import }</pre> |
| View | BGP view |
| Parameters | <p><i>group-name</i>: Name of a peer group, a string of 1 to 47 characters.</p> <p><i>ip-address</i>: IP address of a peer.</p> <p><i>ip-prefix-name</i>: IP prefix list name, a string of 1 to 19 characters.</p> <p>export: Applies the filter to routes advertised to the specified peer/peer group.</p> <p>import: Applies the filter to routes received from the specified peer/peer group.</p> |
| Description | <p>Use the peer ip-prefix command to reference an IP prefix list to filter routes received from or advertised to a peer or peer group.</p> <p>Use the undo peer ip-prefix command to remove the configuration.</p> <p>By default, no IP prefix list is specified.</p> |
| Examples | <pre># In BGP view, use the IP prefix list list 1 to filter routes advertised to the peer group test.</pre> |

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ip-prefix list1 export

```

peer keep-all-routes

Syntax `peer { group-name | ip-address } keep-all-routes`

`undo peer { group-name | ip-address } keep-all-routes`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer keep-all-routes** command to save original routing information from a peer or peer group, even routes that failed to pass the inbound policy (if configured).

Use the **undo peer keep-all-routes** command to disable this function.

By default, the function is not enabled.

Examples # In BGP view, save routing information from peer 131.100.1.1.

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.100.1.1 as-number 200
[Sysname-bgp] peer 131.100.1.1 keep-all-routes

```

peer log-change

Syntax `peer { group-name | ip-address } log-change`

`undo peer { group-name | ip-address } log-change`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer log-change** command to enable the logging of session state and event information for a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

Examples # In BGP view, enable the logging of session state and event information for peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test log-change
```

peer next-hop-local

Syntax **peer** { *group-name* | *ip-address* } **next-hop-local**
undo peer { *group-name* | *ip-address* } **next-hop-local**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer next-hop-local** command to specify the router as the next hop for routes to a peer/peer group.

Use the **undo peer next-hop-local** command to remove the configuration.

By default, routes advertised to an EBGP peer/peer group take the local router as the next hop, while routes to an IBGP peer/peer group do not take the local router as the next hop.

Examples # In BGP view, set the next hop of routes advertised to peer group **test** to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test next-hop-local
```

peer password

Syntax **peer** { *group-name* | *ip-address* } **password** { **cipher** | **simple** } *password*
undo peer { *group-name* | *ip-address* } **password**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

cipher: Displays the configured password in cipher text format.

simple: Displays the configured password in plain text format.

password: Password, a string of 1 to 80 characters when the **simple** keyword is used, or when the **cipher** keyword and plain text password are used; a string of 108 characters when the cipher text password and the **cipher** keyword are used.

Description Use the **peer password** command to configure BGP to perform MD5 authentication when a TCP connection is being established with a peer/peer group.

Use the **undo peer password** command to disable the function.

By default, no MD5 authentication is performed for TCP connection establishment.

Once MD5 authentication is enabled, both parties must be configured with the same authentication mode and password. Otherwise, the TCP connection will not be set up.

Examples # In BGP view, perform MD5 authentication on the TCP connection set up between the local router 10.1.100.1 and the peer router 10.1.100.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.2 password simple aabbcc
```

Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.1 password simple aabbcc
```

peer preferred-value

Syntax **peer** { *group-name* | *ip-address* } **preferred-value** *value*

undo peer { *group-name* | *ip-address* } **preferred-value**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

value: Preferred value, in the range 0 to 65535.

Description Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default value.

The default preferred value is 0.

Routes learned from a peer have an initial preferred value.

Among multiple routes that have the same destination/mask and are learned from different peers, the one with the biggest preferred value is selected as the route to the network.

Note that:

If you both reference a routing policy and use the **peer** { *group-name* | *ip-address* } **preferred-value** *value* command to set a preferred value for routes from a peer, the routing policy sets a specified non-zero preferred value for routes matching it. Other routes not matching the routing policy uses the value set with the command. If the preferred value specified in the routing policy is zero, the routes matching it will also use the value set with the command. For information about using a routing policy to set a preferred value, refer to the command **peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** } and **apply preferred-value** *preferred-value*.

Examples # In BGP view, configure the preferred value as 50 for routes from peer 131.108.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 preferred-value 50
```

peer public-as-only

Syntax **peer** { *group-name* | *ip-address* } **public-as-only**
undo peer { *group-name* | *ip-address* } **public-as-only**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.
ip-address: IP address of a peer.

Description Use the **peer public-as-only** command to not keep private AS numbers in BGP updates sent to a peer/peer group.

Use the **undo peer public-as-only** command to keep private AS numbers in BGP updates sent to a peer/peer group.

By default, BGP updates carry private AS numbers.

The command does not take effect if the BGP update has both public and private AS numbers. The range of private AS number is from 64512 to 65535.

Examples # In BGP view, carry no private AS number in BGP updates sent to the peer **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test public-as-only
```

peer reflect-client

Syntax `peer { group-name | ip-address } reflect-client`

`undo peer { group-name | ip-address } reflect-client`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients** and **reflector cluster-id**.

Examples # In BGP view, configure the local device as a route reflector and specify the IBGP peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test reflect-client
```

peer route-limit

Syntax `peer { group-name | ip-address } route-limit limit [percentage]`

`undo peer { group-name | ip-address } route-limit`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

limit: Upper limit of IP prefixes that can be received from the peer or peer group, in the range 1 to 131072.

percentage: If the number of received routes reaches the specified percentage of the upper limit, the system will generate alarm information. The percentage is in the range from 1 to 100. The default is 75.

Description Use the **peer route-limit** command to set the maximum number of routes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

The number is unlimited by default.

Examples # In BGP view, set the number of routes that can be received from peer 129.140.6.6 to 10000.

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] peer 129.140.6.6 as-number 110
[Sysname-bgp] peer 129.140.6.6 route-limit 10000
```

peer route-policy

Syntax **peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

export: Applies the routing policy to routes outgoing to the peer (or peer group).

import: Applies the routing policy to routes incoming from the peer (or peer group).

Description Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no inbound/outbound routing policy is configured for the peer/peer group.

The **peer route-policy** command does not apply the **if-match interface** clause in the referenced routing policy. Refer to "IPv4 Routing Policy Configuration Commands" on page 467.

Examples # In BGP view, apply routing policy **test-policy** to routes outgoing to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test route-policy test-policy export
```

peer route-update-interval

Syntax `peer { group-name | ip-address } route-update-interval seconds`

`undo peer { group-name | ip-address } route-update-interval`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

seconds: Minimum interval for sending the same update message. The range is 5 to 600 seconds.

Description Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default value.

By default, the interval is 5 seconds for IBGP peers, and 30 seconds for EBGP peers.

Examples # In BGP view, specify the interval for sending the same update to peer group **test** as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
[Sysname-bgp] peer test route-update-interval 10
```

peer substitute-as

Syntax `peer { group-name | ip-address } substitute-as`

`undo peer { group-name | ip-address } substitute-as`

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer substitute-as** command to replace the AS number of a peer/peer group in the AS_PATH attribute with the local AS number.

Use the **undo peer substitute-as** command to remove the configuration.

No AS number is replaced by default.

Examples # In BGP view, substitute local AS number for AS number of peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 substitute-as
```

peer timer

Syntax **peer** { *group-name* | *ip-address* } **timer** **keepalive** *keepalive* **hold** *holdtime*
undo peer { *group-name* | *ip-address* } **timer**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

keepalive: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description Use the **peer timer** command to configure the keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

By default, the *keepalive* and *holdtime* are 60s and 180s respectively.

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer**.

Examples # In BGP view, configure the keepalive interval and holdtime interval for peer group **test** as 40s and 120s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test timer keepalive 40 hold 120
```

preference

Syntax **preference** { *external-preference* *internal-preference* *local-preference* | **route-policy** *route-policy-name* }

undo preference

| | |
|--------------------|---|
| View | BGP view |
| Parameters | <p><i>external-preference</i>: Preference of EBGP routes, in the range 1 to 255.</p> <p><i>internal-preference</i>: Preference of IBGP routes, in the range 1 to 255.</p> <p><i>local-preference</i>: Preference of local routes, in the range 1 to 255.</p> <p><i>route-policy-name</i>: Routing policy name, a string of 1 to 19 characters. Using the routing policy can set a preference for routes passing through it. The default value applies to routes filtered out.</p> |
| Description | <p>Use the preference command to configure preferences for external, internal, and local routes.</p> <p>Use the undo preference command to restore the default.</p> <p>For <i>external-preference</i>, <i>internal-preference</i> and <i>local-preference</i>, the bigger the preference value is, the lower the preference is, and the default values are 255, 255, 130 respectively.</p> |
| Examples | <p># In BGP view, configure preferences for EBGP, IBGP and local routes as 20, 20 and 200.</p> <pre><Sysname> system-view [Sysname] bgp 100 [Sysname-bgp] preference 20 20 200</pre> |

reflect between-clients

| | |
|--------------------------|--|
| Syntax | <p>reflect between-clients</p> <p>undo reflect between-clients</p> |
| View | BGP view |
| Parameters | None |
| Description | <p>Use the reflect between-clients command to enable route reflection between clients.</p> <p>Use the undo reflect between-clients command to disable this function.</p> <p>By default, route reflection between clients is enabled.</p> <p>After a route reflector is configured, it reflects the routes of a client to other clients. If the clients of a route reflector are fully meshed, you need disable route reflection between clients to reduce routing costs.</p> |
| Related commands: | reflector cluster-id and peer reflect-client . |

Examples # Disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] undo reflect between-clients
```

reflector cluster-id

Syntax **reflector cluster-id** *cluster-id*

undo reflector cluster-id

View BGP view

Parameters *cluster-id*: Cluster ID of the route reflector, an integer from 1 to 4294967295 (the integer is translated into an IP address by the system) or an IP address.

Description Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster. The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve the stability of the network. In this case, using this command can configure the identical cluster ID for all the route reflectors to avoid routing loops.

Related commands: **reflect between-clients** and **peer reflect-client**.

Examples # Set the cluster ID to 80.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] reflector cluster-id 80
```

refresh bgp

Syntax **refresh bgp** { **all** | *ip-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

View User view

Parameters **all**: Soft-resets all BGP connections.

ip-address: Soft-resets the BGP connection to a peer.

group-name: Soft-resets connections to a peer group, name of which is a string of 1 to 47 characters.

external: EBGp connection.

internal: IBGP connection.

export: Outbound soft reset.

import: Inbound soft reset.

Description Use the **refresh bgp** command to perform soft reset on specified BGP connections. Using this function can refresh the BGP routing table without tearing down BGP connections and apply a newly configured routing policy.

To perform BGP soft reset, all routers in the network must support route-refresh. If a router not supporting route-refresh exists in the network, you need to configure the **peer keep-all-routes** command to save all routing updates before performing soft reset.

Examples # Perform inbound BGP soft reset.
 <Sysname> refresh bgp all import

reset bgp

Syntax **reset bgp** { **all** | *as-number* | *ip-address* [**flap-info**] | **group** *group-name* | **external** | **internal** }

View User view

Parameters **all**: Resets all BGP connections.

as-number: Resets BGP connections to peers in the AS.

ip-address: Specifies the IP address of a peer with which to reset the connection.

flap-info: Clears history information of routing flap.

group *group-name*: Specifies to reset connections with the specified BGP peer group.

external: Resets all the EBGp connections.

internal: Resets all the IBGP connections.

Description Use the **reset bgp** command to reset specified BGP connections.

Examples # Reset all the BGP connections.
 <Sysname> reset bgp all

reset bgp dampening

Syntax **reset bgp dampening** [*ip-address* [*mask* | *mask-length*]]

View User view

Parameters *ip-address*: Destination IP address of a route.

mask: Mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

Description Use the **reset bgp dampening** command to clear route dampening information and release suppressed routes.

Related commands: **dampening, display bgp routing-table dampened.**

Examples # Clear damping information of route 20.1.0.0/16 and release suppressed route.

```
<Sysname> reset bgp dampening 20.1.0.0 255.255.0.0
```

reset bgp flap-info

Syntax **reset bgp flap-info** [**regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number* | *ip-address* [*mask* | *mask-length*]]

View User view

Parameters *as-path-regexp*: Clears the flap statistics of routes matching the AS path regular expression.

as-path-acl-number: Clears the flap statistics of routes matching an AS path ACL, number of which is in the range 1 to 256.

ip-address: Clears the flap statistics of a route.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

Description Use the **reset bgp flap-info** command to clear the flap statistics of routes matching the specified filter.

The flap statistics of all the routes will be cleared if no parameter is specified.

Examples # Clear the flap statistics of all routes matching AS path ACL 10.

```
<Sysname> reset bgp flap-info as-path-acl 10
```

reset bgp ipv4 all

| | |
|--------------------|--|
| Syntax | reset bgp ipv4 all |
| View | User view |
| Parameters | None |
| Description | Use the reset bgp ipv4 all command to reset all the BGP connections of IPv4 unicast address family. |
| Examples | # Reset all the BGP connections of IPv4 unicast address family.
<Sysname> reset bgp ipv4 all |

router-id

| | |
|--------------------|---|
| Syntax | router-id <i>router-id</i>
undo router-id |
| View | BGP view |
| Parameters | <i>router-id</i> : Router ID in IP address format. |
| Description | Use the router-id command to specify a router ID.

Use the undo router-id command to remove the router ID.

To run BGP protocol, a router must have a router ID, which is an unsigned 32-bit integer, the unique ID of the router in the AS.

You can specify a router ID manually. If not, the system selects an IP address as the router ID. The selection sequence is the highest IP address among loopback interface addresses; if not available, then the highest IP address of interfaces. It is recommended to specify a loopback interface address as the router ID to enhance network reliability.

Only when the interface with the selected Router ID or the manual Router ID is deleted will the system select another ID for the router. |
| Examples | # Specifies the Router ID as 10.18.4.221.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] router-id 10.18.4.221 |

summary automatic

Syntax **summary automatic**

undo summary automatic

View BGP view

Parameters None

Description Use the **summary automatic** command to enable automatic summarization for redistributed subnets.

Use the **undo summary automatic** command to disable automatic summarization.

By default, automatic summarization is disabled.

Note that:

- Neither the default route nor the routes imported using the **network** command can be summarized automatically.
- With this feature enabled, BGP limits the subnets redistribution from IGP to reduce the size of routing table.

Examples # In BGP view, enable automatic summarization.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] summary automatic
```

synchronization

Syntax **synchronization**

undo synchronization

View BGP view

Parameters None

Description Use the **synchronization** command to enable the synchronization between the BGP and IGP routes.

Use the **undo synchronization** command to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, BGP speakers in the AS cannot advertise routing

information to other ASs unless all routers in the AS know the latest routing information.

When a BGP router receives an IBGP route, it checks only whether the next hop is reachable by default. If the synchronization is enabled, the IBGP route is synchronized and advertised to EBGP peers only when the route is also advertised by IGP. Otherwise, the IBGP route cannot be advertised to EBGP peers.

Examples # Enable the synchronization between BGP and IGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] synchronization
```

timer

Syntax **timer keepalive** *keepalive* **hold** *holdtime*

undo timer

View BGP view

Parameters *keepalive*: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description Use the **timer** command to configure BGP keepalive interval and holdtime interval.

Use the **undo timer** command to restore the default.

By default, BGP keepalive and holdtime intervals are 60s and 180s.

Note that:

- Timer configured using the **peer timer** command is preferred to the timer configured using this command.
- The holdtime interval must be at least three times the keepalive interval.
- The configured timer applies to all the BGP peers, while it becomes valid only after the corresponding BGP connections are reset.

Related commands: **peer timer**.

Examples # Configure keepalive interval and holdtime interval as 40s and 120s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] timer keepalive 60 hold 180
```

27

ROUTING POLICY COMMON CONFIGURATION COMMANDS



- The term “router” in this document refers to a generic router or a Layer 3 switch running routing protocols.
- Routing policy common configuration commands are applicable to both IPv4 and IPv6.

apply as-path

Syntax `apply as-path as-number&<1-10> [replace]`

`undo apply as-path`

View Routing policy view

Parameters *as-number*: Autonomous system number, in the range of 1 to 65535.

&<1-10>: Indicates you can enter *as-number* up to 10 times.

replace: Replaces the original AS number.

Description Use the **apply as-path** command to apply the specified AS numbers to BGP routes.

Use the **undo apply as-path** command to remove the clause configuration.

No AS_PATH attribute is set by default.

With the **replace** keyword, using the **apply as-path** command replaces the original AS_PATH attribute with specified AS numbers. Without the **replace** keyword, using this command adds the specified AS numbers before the original AS_PATH attribute.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If BGP routing information matches AS-path-ACL 1, add AS number 200 before the original AS_PATH attribute.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply as-path 200
```

apply comm-list delete

- Syntax** **apply comm-list** *comm-list-number* **delete**
- undo apply comm-list**
- View** Routing policy view
- Parameters** *comm-list-number*: Community list number. The basic community list number ranges from 1 to 99. The advanced community list number ranges from 100 to 199.
- Description** Use the **apply comm-list delete** command to remove community attributes in BGP routing information specified by the community list.
- Use the **undo apply comm-list** command to remove the clause configuration.
- No community attributes are removed by default.
- Examples** # Create routing policy **policy1** with node 10, matching mode as permit. If BGP routing information matches AS-path-ACL 1, remove community attributes specified in community list 1.
- ```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply comm-list 1 delete
```

---

## apply community

- Syntax** **apply community** { **none** | **additive** | { *community-number*&<1-16> | *aa:nn*&<1-16> | **internet** | **no-export-subconfed** | **no-export** | **no-advertise** } \*  
[ **additive** ] }
- undo apply community**
- View** Routing policy view
- Parameters** **none**: Removes community attributes of BGP routes.
- community-number*: Community sequence number, in the range 1 to 4294967295.
- aa:nn*: Community number; both *aa* and *nn* are in the range 0 to 65535.
- &<1-16>: Indicates the argument before it can be entered up to 16 times.
- internet**: Sets the **internet** community attribute for matched BGP routes. Routes with this attribute are advertised to all BGP peers.

**no-export-subconfed:** Sets the **no-export-subconfed** community attribute for matched BGP routes. Routes with this attribute are not advertised out the sub autonomous system.

**no-advertise:** Sets the **no-advertise** community attribute for matched BGP routes. Routes with this attribute are not advertised to any peers.

**no-export:** Sets the **no-export** community attribute for matched BGP routes. Routes with this attribute are not advertised out the autonomous system or confederation, but can be advertised to other sub ASs in the confederation.

**additive:** Adds the specified community attribute to the original community attribute of a matched BGP route.

**Description** Use the **apply community** command to set the specified community attribute for BGP routes.

Use the **undo apply community** command to remove the apply clause.

No community attribute is set by default.

**Related commands:** **ip community-list, if-match community, route-policy.**

**Examples** # Create routing policy **setcommunity** with node 16 and matching mode as **permit**. Set the no-export community attribute for BGP routes passing AS-path-ACL 8.

```
<Sysname> system-view
[Sysname] route-policy setcommunity permit node 16
[Sysname-route-policy] if-match as-path 8
[Sysname-route-policy] apply community no-export
```

---

## apply cost

**Syntax** **apply cost** [ + | - ] *value*

**undo apply cost**

**View** Routing policy view

**Parameters** +: Increases cost value.

+: Decreases cost value.

*cost*: Specifies a cost from 0 to 4294967295.

**Description** Use the **apply cost** command to set a cost for routing information.

Use the **undo apply cost** command to remove the clause configuration.

No cost is set for routing information by default.

**Related commands:** **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply origin**, **apply tag**.

**Examples** # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches the outbound interface VLAN-interface 10, set the cost for the route to 120.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface vlan-interface 10
[Sysname-route-policy] apply cost 120
```

---

## apply cost-type

**Syntax** **apply cost-type** { **external** | **internal** | **type-1** | **type-2** }

**undo apply cost-type**

**View** Routing policy view

**Parameters** **external**: IS-IS external route.

**internal**: IS-IS internal route.

**type-1**: Type-1 external route of OSPF.

**type-2**: Type-2 external route of OSPF.

**Description** Use the **apply cost-type** command to set a cost type for routing information.  
Use the **undo apply cost-type** command to remove the clause configuration.  
No cost type is set for routing information by default.

**Examples** # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches tag 8, set the cost type for the route to IS-IS internal route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply cost-type internal
```

---

## apply extcommunity

**Syntax** **apply extcommunity** { **rt route-target** }&<1-16> [ **additive** ]

**undo apply extcommunity**

**View** Routing policy view

- Parameters** **rt route-target**: Sets the route target extended community attribute, which is a string of 3 to 21 characters. *route-target* has two forms:
- 16-bit AS number: 32-bit self-defined number, for example, 101:3;
- 32-bit IP address: 16-bit self-defined number, for example, 192.168.122.15:1.
- <1-16>: Indicates the argument before it can be entered up to 16 times.
- additive**: Adds to the original community attribute of a route.
- Description** Use the **apply extcommunity** command to apply the specified extended community attribute to BGP routes.
- Use the **undo apply extcommunity** command to remove the clause configuration.
- No extended community attribute is set for routing information by default.
- Examples** # Create routing policy **policy1** with node 10, matching mode as permit. If a BGP route matches AS-path-ACL 1, add the RT extended community attribute 100:2 to the route.
- ```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply extcommunity rt 100:2 additive
```

apply isis

apply isis { level-1 | level-1-2 | level-2 }

undo apply isis

View Routing policy view

Parameters **level-1**: Redistributes routes into IS-IS level-1 area.

level-2: Redistributes routes into IS-IS level-2 area.

level-1-2: Redistributes routes into both IS-IS level-1 and level-2 areas.

Description Use the **apply isis** command to redistribute routes into a specified ISIS level.

Use the **undo apply isis** command to remove the clause configuration.

No level is set by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip**, **if-match cost**, **if-match tag**, **route-policy**, **apply cost**, **apply origin**, **apply tag**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches tag 8, redistribute the route to IS-IS level-2 area.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply isis level-2
```

apply local-preference

Syntax **apply local-preference** *preference*

undo apply local-preference

View Routing policy view

Parameters *preference*: BGP local preference, in the range 0 to 4294967295.

Description Use the **apply local-preference** command to apply the specified local preference to BGP routes.

Use the **undo apply local-preference** command to remove the clause configuration.

No local preference is set for BGP routing information by default.

Related commands: **route-policy**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches AS-path-ACL 1, set the local preference for the route to 130.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply local-preference 130
```

apply origin

Syntax **apply origin** { **igp** | **egp** *as-number* | **incomplete** }

undo apply origin

View Routing policy view

Parameters **igp**: Sets the origin of BGP routing information to IGP.

egp: Sets the origin of BGP routing information to EGP.

as-number: Autonomous system number for EGP routes, in the range of 1 to 65535.

incomplete: Sets the origin of BGP routing information to unknown.

Description Use the **apply origin** command to apply the specified origin attribute to BGP routes.

Use the **undo apply origin** command to remove the clause configuration.

No origin attribute is set for routing information by default.

Related commands: **if-match interface, if-match acl, if-match ip-prefix, if-match ip, if-match cost, if-match tag, route-policy, apply ip-address next-hop, apply local-preference, apply cost, apply tag.**

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches AS-path-ACL 1, set the origin for the route to IGP.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply origin igp
```

apply preference

Syntax **apply preference** *preference*

undo apply preference

View Routing policy view

Parameters *preference*: Routing preference, in the range of 1 to 255.

Description Use the **apply preference** command to set a preference for a routing protocol.

Use the **undo apply preference** command to remove the clause configuration.

No preference is set for a routing protocol by default.

If you set preferences for routing protocols with the **preference** command, using the **apply preference** command will set a new preference for a matched routing protocol. Other routing protocols not satisfying criteria still use the preferences set by the **preference** command.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches OSPF external route type, set the preference for the routing protocol to 90.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1or2
[Sysname-route-policy] apply preference 90
```

apply preferred-value

Syntax **apply preferred-value** *preferred-value*

undo apply preferred-value

View Routing policy view

Parameters *preferred-value*: Preferred value, in the range of 0 to 65535.

Description Use the **apply preferred-value** command to apply a preferred value to BGP routes.

Use the **undo apply preferred-value** command to remove the clause configuration.

No preferred value is set for BGP routes by default.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a BGP route matches AS-path-ACL 1, set the preferred value 66 for the BGP route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply preferred-value 66
```

apply tag

Syntax **apply tag** *value*

undo apply tag

View Routing policy view

Parameters *value*: Tag value, in the range 0 to 4294967295.

Description Use the **apply tag** command to set a specified tag value for RIP, OSPF or IS-IS routing information.

Use the **undo apply tag** command to remove the clause configuration.

No routing tag is set for RIP, OSPF or IS-IS routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply cost**, **apply origin**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches OSPF external route type 1, set the tag of the route to 100.

```

<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1
[Sysname-route-policy] apply tag 100

```

display ip as-path

Syntax **display ip as-path** [*as-path-number*]

View Any view

Parameters *as-path-number*: AS path ACL number, in the range of 1 to 256.

Description Use the **display ip as-path** command to display BGP AS path ACL information. Information about all BGP AS path lists will be displayed if no *as-path-number* is specified.

Related commands: **ip as-path, if-match as-path, apply as-path.**

Examples # Display the information of BGP AS path list 1.

```

<Sysname> display ip as-path 1
ListID    Mode      Expression
1         permit    2

```

Table 102 Field descriptions of the display ip as-path command

| Field | Description |
|------------|---------------------------------|
| ListID | AS path ACL ID |
| Mode | Matching mode: permit, deny |
| Expression | Regular expression for matching |

display ip community-list

Syntax **display ip community-list** [*basic-community-list-number* | *adv-community-list-number*]

View Any view

Parameters *basic-community-list-number*: Basic community list number, in the range of 1 to 99.

adv-community-list-number: Advanced community list number, in the range of 100 to 199.

Description Use the **display ip community-list** command to display BGP community list information.

All BGP community list information will be displayed if no *basic-community-list-number* or *adv-community-list-number* is specified.

Related commands: **ip community-list, if-match community, apply community.**

Examples # Display the information of the BGP community list 1.

```
<Sysname> display ip community-list 1
Community List Number 1
    permit 1:1 1:2 2:2
```

display ip extcommunity-list

Syntax **display ip extcommunity-list** [*ext-comm-list-number*]

View Any view

Parameters *ext-comm-list-number*: Extended community list number, in the range of 1 to 199.

Description Use the **display ip extcommunity-list** command to display BGP extended community list information.

All BGP extended community list information will be displayed if no *ext-comm-list-number* is specified.

Related commands: **ip extcommunity-list, if-match extcommunity, apply extcommunity.**

Examples # Display the information of BGP extended community list 1.

```
<Sysname> display ip extcommunity-list 1
Extended Community List Number 1
    permit rt : 9:6
```

display route-policy

Syntax **display route-policy** [*route-policy-name*]

View Any view

Parameters *route-policy-name*: Routing policy name, a string of 1 to 19 characters.

Description Use the **display route-policy** command to display routing policy information.

All routing policy information will be displayed if no *route-policy-name* is specified.

Related commands: **route-policy.**

Examples # Display the information of routing policy 1.

```

<Sysname> display route-policy policy1
Route-policy : policy1
  permit : 10
    if-match ip-prefix abc
    apply cost 120

```

Table 103 Field descriptions of the display route-policy command.

| Field | Description |
|------------------------|---|
| Route-policy | Routing policy name |
| Permit | permit mode: permit, deny |
| if-match ip-prefix abc | Match criterion |
| apply cost 120 | If the match criterion is satisfied, set the route cost to 120. |

if-match as-path

Syntax **if-match as-path** *as-path-number*&<1-16>

undo if-match as-path [*as-path-number*&<1-16>]

View Routing policy view

Parameters *as-path-number*: AS path list number, in the range of 1 to 256.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match as-path** command to specify AS path list (s) for matching against the AS path attribute of BGP routing information.

Use the **undo if-match as-path** command to remove the match criterion.

The match criterion is not configured by default.

This command is one of the if-match clauses of a route policy, used for filtering BGP routing information and specifying match criteria according to the AS path attribute of routing information.

Related commands: **route-policy**, **ip as-path**.

Examples # Define as-path list 2, allowing routing information containing AS 200 or 300 to pass. Define routing policy **test** with node 10, and set an if-match clause using the as-path list for matching.

```

<Sysname> system-view
[Sysname] ip as-path 2 permit _*200.*300
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match as-path 2

```

if-match community

Syntax **if-match community** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

undo if-match community [*basic-community-list-number* | *adv-community-list-number*]&<1-16>

View Routing policy view

Parameters *basic-community-list-number*: Basic community list number, in the range of 1 to 99.

adv-community-list-number: Advanced community list number, in the range of 100 to 199.

whole-match: Specifies the exact match. All and only the specified communities must be present.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match community** command to specify community list(s) for matching against the community attribute of BGP routing information.

Use the **undo if-match community** command to remove the match criterion.

The match criterion is not configured by default.

This command is one of the if-match clauses of route policy, used for filtering BGP routing information and specifying match criterion according to the community attribute of BGP routing information.

Related commands: **route-policy**, **ip community-list**.

Examples # Define community-list 1, allowing routing information with community number 100 or 200 to pass. Then define a routing policy named test, whose node 10 is defined with an if-match clause to reference the community-list for matching.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit 100 200
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match community 1
```

if-match cost

Syntax if-match cost *value*

undo if-match cost

View Routing policy view

- Parameters** *cost*: Specifies the cost to match, ranging from 0 to 4294967295.
- Description** Use the **if-match cost** command to specify a cost for matching against the cost of a route.
- Use the **undo if-match cost** command to remove the match criterion.
- The match criterion is not configured by default.
- This command is one of the if-match clauses of routing policy, used for matching routes with the specified route cost.
- Related commands:** **if-match interface, if-match acl, if-match ip-prefix, if-match ip, if-match tag, route-policy, apply ip-address next-hop, apply cost, apply local-preference, apply origin, apply tag.**
- Examples** # Create routing policy **policy1** with node 10, matching mode as permit. Define an if-match clause to permit routing information with a cost of 8.
- ```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match cost 8
```

---

## if-match extcommunity

- Syntax** **if-match extcommunity** *ext-comm-list-number*&<1-16>
- undo if-match extcommunity** [ *ext-comm-list-number*&<1-16> ]
- View** Routing policy view
- Parameters** *ext-comm-list-number*: Extended community list number, in the range of 1 to 199.
- &<1-16>: Indicates the argument before it can be entered up to 16 times.
- Description** Use the **if-match extcommunity** command to specify extended community list(s) for matching against the extended community attribute of routing information.
- Use the **undo if-match extcommunity** command to remove the match criterion.
- The match criterion is not configured by default.
- Examples** # Create a routing policy named policy1 with node 10, matching mode as permit. Match the extended community attribute of routes against extended community lists 100 and 150.
- ```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match extcommunity 100 150
```

if-match interface

Syntax **if-match interface** { *interface-type interface-number* }&<1-16>
undo if-match interface [*interface-type interface-number*]&<1-16>

View Routing policy view

Parameters *interface-type*: Interface type
interface-number: Interface number

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match interface** command to specify interface(s) for matching against the outbound interfaces of routing information.
 Use the **undo if-match interface** command to remove the match criterion.
 The match criterion is not configured by default.

Related commands: **if-match acl, if-match ip-prefix, if-match ip, if-match cost, if-match tag, route-policy, apply ip-address next-hop, apply cost, apply local-preference, apply origin, apply tag.**

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to permit the routing information with the outbound interface as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface vlan-interface 1
```

if-match route-type

Syntax **if-match route-type** { **internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2** } *
undo if-match route-type [**internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2**] *

View Routing policy view

Parameters **internal**: Internal routes (OSPF intra-area and inter-area routes).
external-type1: OSPF Type 1 external routes.
external-type2: OSPF Type 2 external routes.

external-type1or2: OSPF Type 1 or 2 external routes.

is-is-level-1: IS-IS Level-1 routes.

is-is-level-2: IS-IS Level-2 routes.

nssa-external-type1: OSPF NSSA Type 1 external routes.

nssa-external-type2: OSPF NSSA Type 2 external routes.

nssa-external-type1or2: OSPF NSSA Type 1 or 2 external routes.

Description Use the **if-match route-type** command to configure a route type match criterion.

Use the **undo if-match route-type** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to match internal routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type internal
```

if-match tag

Syntax **if-match tag** *value*

undo if-match tag

View Routing policy view

Parameters *value*: Specifies a tag value, ranging from 0 to 4294967295.

Description Use the **if-match tag** command to match routing information having the specified tag.

Use the **undo if-match tag** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match interface, if-match acl, if-match ip-prefix, if-match ip, if-match cost, route-policy, apply ip-address next-hop, apply cost, apply local-preference, apply origin, apply tag.**

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to permit RIP, OSPF and IS-IS routing information with the tag as 8.

```

<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8

```

ip as-path

Syntax `ip as-path as-path-number { deny | permit } regular-expression`

`undo ip as-path as-path-number`

View System view

Parameters *as-path-number*: AS path ACL number, in the range of 1 to 256.

deny: Specifies the matching mode for the AS path ACL as deny.

permit: Specifies the matching mode for the AS path ACL as permit.

regular-expression: Regular expression of AS path, a string of 1 to 50 characters.

BGP routing information contains the AS path attribute field that identifies the autonomous systems through which routing information has passed. Used to compare with the AS path attribute, a regular expression is a formula comprised of characters, for example, `^200.*100$`, which matches AS path attribute fields that start with AS200 and end with AS100.

The meanings of special characters used in regular expressions are shown below:

| Character | Meaning |
|-----------|--|
| . | Matches any single character, including blank space. |
| * | Matches 0 or more patterns. |
| + | Matches 1 or more patterns. |
| ^ | Matches the beginning of an input string. |
| \$ | Matches the end of an input string. |
| _ | Matches a comma, left brace, right brace, left parenthesis, right parenthesis, the beginning of an input string, the end of an input string, or a space. |
| [range] | Means the range of single-character patterns. |
| - | Separates the ending points of a range. |

Description Use the **ip as-path** command to create an AS path ACL.

Use the **undo ip as-path** command to remove an AS path ACL.

No AS path ACL is created by default.

Examples # Create an AS path ACL numbered 1, permitting routing information whose AS_PATH starts with 10.

```
<Sysname> system-view
[Sysname] ip as-path-acl 1 permit ^10
```

ip community-list

Syntax **ip community-list** *basic-comm-list-num* { **deny** | **permit** }
 [*community-number-list*] [**internet** | **no-advertise** | **no-export** |
no-export-subconfed] *

undo ip community-list *basic-comm-list-num* [*community-number-list*]
 [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

ip community-list *adv-comm-list-num* { **deny** | **permit** } *regular-expression*

undo ip community-list *adv-comm-list-num* [*regular-expression*]

View System view

Parameters *basic-comm-list-num*: Basic community list number, in the range 1 to 99.

adv-comm-list-num: Advanced community list number, in the range 100 to 199.

regular-expression: Regular expression of advanced community attribute, a string of 1 to 50 characters.

deny: Specifies the matching mode of the community list as deny.

permit: Specifies the matching mode of the community list as permit.

community-number-list: Community number list, in the *community number* or *aa:nn* format, with *community number* in the range 1 to 4294967295 and *aa* and *nn* in the range 0 to 65535. Each format can be entered up to 16 times.

internet: Routes with this attribute can be advertised to all the BGP peers. By default, all routes have this attribute.

no-advertise: Routes with this attribute will not be advertised to other BGP peers.

no-export: Routes with this attribute will not be advertised out the local AS, or the confederation but can be advertised to other ASs in the confederation.

no-export-subconfed: Routes with this attribute can not be advertised out the local AS, or to other sub ASs in the confederation.

Description Use the **ip community-list** to define a community list entry.

Use the **undo ip community-list** command to remove a community list or entry.

No community list is defined by default.

Examples # Define basic community list 1 to permit routing information with the **internet** community attribute.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit internet
```

Define advanced community list 100 to permit routing information with the community attribute starting with 10.

```
<Sysname> system-view
[Sysname] ip community-list 100 permit ^10
```

ip extcommunity-list

Syntax **ip extcommunity-list** *ext-comm-list-number* { **deny** | **permit** } { **rt** *route-target* } &<1-16>

undo ip extcommunity-list *ext-comm-list-number*

View System view

Parameters *ext-comm-list-number*: Extended community list number, in the range 1 to 199.

permit: Specifies the matching mode for the extended community list as permit.

deny: Specifies the matching mode for the extended community list as deny.

rt *route-target*: Specifies route target extended community attribute, which is a string of 3 to 21 characters. *route-target* has two forms:

A 16-bit AS number: a 32-bit self-defined number, for example, 101:3;

A 32-bit IP address: a 16-bit self-defined number, for example, 192.168.122.15:1.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **ip extcommunity-list** to define an extended community list entry.

Use the **undo ip extcommunity-list** command to remove an extended community list.

No extended community list is defined by default.

Examples # Define extended community list 1 to permit routing information with RT 200:200.

```
<Sysname> system-view
[Sysname] ip extcommunity-list 1 permit rt 200:200
```

route-policy

Syntax **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*

undo route-policy *route-policy-name* [**node** *node-number*]

View System view

Parameters *route-policy-name*: Routing policy name, a string of 1 to 19 characters.

permit: Specifies the matching mode of the routing policy node as permit. If a route satisfies all the if-match clauses of the node, it passes through the filtering of the node and then is executed with the apply clauses of the node. If not, it goes to the next node of the routing policy.

deny: Specifies the matching mode of the routing policy node as deny. If a route satisfies all the if-match clauses of the node, it does not pass the filtering of the node and will not go to the next node.

node node-number: Node number, in the range 0 to 65535. The node with a smaller *node-number* will be tested first when the routing policy is used for filtering routing information.

Description Use the **route-policy** command to create a routing policy and enter its view.

Use the **undo route-policy** command to remove a routing policy.

No routing policy is created by default.

A routing policy is used for routing information filtering or policy routing. It contains several nodes and each node comprises some if-match and apply clauses. The if-match clauses define the matching criteria of the node and the apply clauses define the actions performed after a packet passes the filtering of the node. The relation among the if-match clauses of a node is logic AND, namely all the if-match clauses must be satisfied. The filter relation among different route-policy nodes is logic OR, namely a packet passing a node passes the routing policy.

Related commands: **if-match interface, if-match acl, if-match ip-prefix, if-match ip, if-match cost, if-match tag, apply ip-address next-hop, apply local-preference, apply cost, apply origin, apply tag.**

Examples # Create routing policy 1 with node 10 and matching mode as permit, and then enter routing policy view.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy]
```


28

IPv4 ROUTING POLICY CONFIGURATION COMMANDS

apply ip-address next-hop

Syntax `apply ip-address next-hop ip-address`

`undo apply ip-address next-hop`

View Routing policy view

Parameters *ip-address*: IP address of the next hop.

Description Use the **apply ip-address next-hop** command to set a next hop for IPv4 routing information.

Use the **undo apply ip-address next-hop** command to remove the clause configuration.

No next hop address is set for IPv4 routing information by default.

It is invalid to use the **apply ip-address next-hop** command to set a next hop when redistributing routes.

Related commands: **if-match interface, if-match acl, if-match ip-prefix, if-match ip, if-match cost, if-match tag, route-policy, apply local-preference, apply cost, apply origin, apply tag.**

Examples # Create routing policy **policy1** with node 10, matching mode **permit**. If passing AS path ACL 1, a route's next hop is set to 193.1.1.8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ip-address next-hop 193.1.1.8
```

display ip ip-prefix

Syntax `display ip ip-prefix [ip-prefix-name]`

View Any view

Parameters *ip-prefix-name*: IP prefix list name, a string of 1 to 19 characters.

Description Use the **display ip ip-prefix** command to display the statistics of an IPv4 prefix list. If no ip-prefix-name is specified, statistics for all IPv4 prefix lists will be displayed.

Related commands: **ip ip-prefix.**

Examples # Display the statistics of IPv4 prefix list **abc**.

```
<Sysname> display ip ip-prefix abc
Prefix-list abc
Permitted 0
Denied 0
      index: 10          permit 1.0.0.0/11          ge 22 le 32
```

Table 104 Field descriptions of the display ip ip-prefix command.

| Field | Description |
|-------------|---|
| Prefix-list | Name of the IPv4 prefix list |
| Permitted | Number of routes satisfying the match criterion |
| Denied | Number of routes not satisfying the match criterion |
| index | Internal serial number of the IPv4 prefix list |
| permit | Matching mode: permit or deny |
| 1.0.0.0/11 | Match IP address and mask |
| ge | greater-equal, the lower limit mask |
| le | less-equal, the upper limit mask |

if-match acl

Syntax **if-match acl** *acl-number*

undo if-match acl

View Routing policy view

Parameters *acl-number*: ACL number from 2000 to 3999.

Description Use the **if-match acl** command to configure an ACL match criterion.

Use the **undo if-match acl** command to remove the match criterion.

No ACL match criterion is configured by default.

Related commands: **if-match interface, if-match ip, if-match cost, if-match tag, route-policy, apply ip-address next-hop, apply cost, apply local-preference, apply origin, apply tag.**

Examples # Create routing policy **policy1** with node 10, matching mode as permit. Define an if-match clause to permit routes matching ACL 2000.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match acl 2000
```

if-match ip

Syntax **if-match ip** { **next-hop** | **route-source** } { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }

undo if-match ip { **next-hop** | **route-source** } [**acl** | **ip-prefix**]

View Routing policy view

Parameters **next-hop**: Matches next hop.

route-source: Matches source address.

acl *acl-number*: Matches an ACL with a number from 2000 to 2999.

ip-prefix *ip-prefix-name*: Matches an IP prefix list with a name being a string of 1 to 19 characters.

Description Use the **if-match ip** command to configure a next hop or source address match criterion for IPv4 routes.

Use the **undo if-match ip** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **route-policy**.

Examples # Create routing policy **policy1** with node 10, matching mode permit. Define an if-match clause to permit routing information whose next hop address matches IP prefix list p1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ip next-hop ip-prefix p1
```

if-match ip-prefix

Syntax **if-match ip-prefix** *ip-prefix-name*

undo if-match ip-prefix

View Routing policy view

Parameters *ip-prefix-name*: Matches an IP prefix list with a name being a string of 1 to 19 characters.

Description Use the **if-match ip-prefix** command to configure an IP prefix list based match criterion.

Use the **undo if-match ip-prefix** command to remove the match criterion.

No IP prefix list based match criterion is configured by default.

Related commands: **if-match interface, if-match ip, if-match cost, if-match tag, route-policy, apply ip-address next-hop, apply cost, apply local-preference, apply origin, apply tag.**

Examples # Create routing policy **policy1** with node 10, matching mode as permit. Define an if-match clause to permit a route whose destination address matches IP prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ip-prefix p1
```

ip ip-prefix

Syntax **ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ip-address mask-length* [**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]

undo ip ip-prefix *ip-prefix-name* [**index** *index-number*]

View System view

Parameters *ip-prefix-name*: IPv4 prefix list name, a string of 1 to 19 characters.

index-number: Index number, in the range 1 to 65535, for uniquely specifying an item of the IPv4 prefix list. The index with a smaller number is tested first.

permit: Specifies the matching mode for the IPv4 prefix list as permit, that is, when a route to be filtered is in the range of the IPv4 prefix list, the route passes the IPv4 prefix list without needing to enter the next item for testing. If the route to be filtered is not in the prefix range, it will enter the next item test.

deny: Specifies the matching mode for the IPv4 prefix list as deny, that is, when a route to be filtered is in the IPv4 prefix list range, the route neither passes the filter nor enters the next node for testing. If not in the range, the route will enter the next item test.

ip-address mask-length: Specifies an IPv4 address prefix and mask length. The *mask-length* is in the range 0 to 32.

min-mask-length, max-mask-length: Specifies the range for prefix if the IPv4 address and prefix length are matched. **greater-equal** means "greater than or equal to" and **less-equal** means "less than or equal to". The range relation is $mask-length \leq min-mask-length \leq max-mask-length \leq 32$. If only *min-mask-length* is specified, the prefix length range is [*min-mask-length*, 32]. If only *max-mask-length* is specified, the prefix length range is [*mask-length*, *max-mask-length*]. If both *min-mask-length* and *max-mask-length* are specified, the prefix length range is [*min-mask-length*, *max-mask-length*].

Description Use the **ip ip-prefix** command to configure an IPv4 prefix list item.

Use the **undo ip ip-prefix** command to remove an IPv4 prefix list or an item.

No IPv4 prefix list is configured by default.

An IPv4 prefix list is used to filter IPv4 addresses. It may have multiple items, each of which specifies a range of IPv4 prefix. The filtering relation among items is logic OR, namely, passing any item means the IPv4 prefix list is passed. If no item is passed, the IP prefix list cannot be passed.

The IP prefix range is determined by *mask-length* and [*min-mask-length*, *max-mask-length*]. If both *mask-length* and [*min-mask-length*, *max-mask-length*] are specified, then the IP address to be filtered must satisfy both of them.

If *ip-address mask-length* is specified as 0.0.0.0 0, then only the default route is matched.

With the keyword and argument combination *ip-address mask-length less-equal* specified as 0.0.0.0 **less-equal** 32, the command matches all the routes.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an IP prefix list named p1 to permit only the routes in the network segment 10.0.192.0/8 and with mask length 17 or 18.

```
<Sysname> system-view
[Sysname] ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17 less-equal 18
```

reset ip ip-prefix

Syntax **reset ip ip-prefix** [*ip-prefix-name*]

View User view

Parameters *ip-prefix-name*: IP prefix list name, a string of 1 to 19 characters.

Description Use the **reset ip ip-prefix** command to clear the statistics of a specified IPv4 prefix list. If no *ip-prefix-name* is specified, the statistics of all the IPv4 prefix lists will be cleared.

Examples # Clear the statistics of IPv4 prefix list **abc**.

```
<Sysname> reset ip ip-prefix abc
```


29

IPv6 STATIC ROUTING CONFIGURATION COMMANDS



- Throughout this chapter, the term “router” refers to a Layer 3 switch running routing protocols
- At present, the 0231A92P modules in the S7900E do not support IPv6.

delete ipv6 static-routes all

Syntax `delete ipv6 static-routes all`

View System view

Parameters None

Description Use the **delete ipv6 static-routes all** command to delete all static routes including the default route.

When using this command, you will be prompted whether to continue the deletion and only after you confirm the deletion will the static routes be deleted.

Related commands: **display ipv6 routing-table, ipv6 route-static.**

Examples # Delete all IPv6 static routes.

```
<Sysname> system-view
[Sysname] delete ipv6 static-routes all
This will erase all ipv6 static routes and their configurations, you
must reconfigure all static routes
Are you sure?[Y/N]Y
```

ipv6 route-static

Syntax `ipv6 route-static ipv6-address prefix-length [interface-type interface-number]
nexthop-address [preference preference-value]`

`undo ipv6 route-static ipv6-address prefix-length [interface-type
interface-number] [nexthop-address] [preference preference-value]`

View System view

Parameters `ipv6-address prefix-length`: IPv6 address and prefix length.

interface-type interface-number: Interface type and interface number of the output interface.

nexthop-address: Next hop IPv6 address.

preference-value: Route preference value, in the range of 1 to 255. The default is 60.

Description Use the **ipv6 route-static** command to configure an IPv6 static route.

Use the **undo ipv6 route-static** command to remove an IPv6 static route.

An IPv6 static route that has the destination address configured as **::/0** (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route will be used to forward the packet.

Related commands: **display ipv6 routing-table**, **delete ipv6 static-routes all**.

Examples # Configure a static IPv6 route, with the destination address being 1:1:2::/24 and next hop being 1:1:3::1.

```
<Sysname> system-view
[Sysname] ipv6 route-static 1:1:2:: 24 1:1:3::1
```

30

IPv6 RIPNG CONFIGURATION COMMANDS



- Throughout this chapter, the term “router” refers to a Layer 3 switch running routing protocols.
- At present, the 0231A92P modules in the S7900E do not support IPv6.

checkzero

Syntax **checkzero**
undo checkzero

View RIPng view

Parameters None

Description Use the **checkzero** command to enable the zero field check on RIPng packets.
Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

Some fields in RIPng packet headers must be zero. These fields are called zero fields. You can enable the zero field check on RIPng packet headers. If any such field contains a non-zero value, the RIPng packet will be discarded.

Examples # Disable the zero field check on RIPng packet headers of RIPng 100.

```
<Sysname> system-view  
[Sysname] ripng 100  
[Sysname-ripng-100] undo checkzero
```

default cost

Syntax **default cost** *cost*
undo default cost

View RIPng view

Parameters *cost*: Default metric of redistributed routes, in the range of 0 to 16.

Description Use the **default cost** command to specify the default metric of redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default metric of redistributed routes is 0.

The specified default metric applies to routes redistributed by the **import-route** command that has no metric specified.

Related commands: **import-route**.

Examples # Set the default metric of redistributed routes to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

display ripng

Syntax **display ripng** [*process-id*]

View Any view

Parameters *process-id*: RIPng process ID, in the range of 1 to 65535.

Description Use the **display ripng** command to display the running status and configuration information of a RIPng process. If *process-id* is not specified, information of all RIPng processes will be displayed.

Examples # Display the running status and configuration information of all configured RIPng processes.

```
<Sysname> display ripng
  RIPng process : 1
    Preference : 100
    Checkzero : Enabled
    Default Cost : 0
    Maximum number of balanced paths : 3
    Update time : 30 sec(s) Timeout time : 180 sec(s)
    Suppress time : 120 sec(s) Garbage-Collect time : 240 sec(s)
    Number of periodic updates sent : 0
    Number of trigger updates sent : 0
```

Table 105 Field descriptions of the display ripng command

| Field | Description |
|----------------------------------|--|
| RIPng Process | RIPng process ID |
| Preference | RIPng route priority |
| Checkzero | Whether zero field check for RIPng packet headers is enabled |
| Default Cost | Default metric of redistributed routes |
| Maximum number of balanced paths | Maximum number of load balanced routes |

Table 105 Field descriptions of the display ripng command

| Field | Description |
|---------------------------------|---|
| Update time | RIPng updating interval, in seconds |
| Timeout time | RIPng timeout interval, in seconds |
| Suppress time | RIPng suppress interval, in seconds |
| Garbage-Collect time | RIPng garbage collection interval, in seconds |
| Number of periodic updates sent | Number of periodic updates sent |
| Number of trigger updates sent | Number of triggered updates sent |

display ripng database

Syntax `display ripng process-id database`

View Any view

Parameters *process-id*: RIPng process ID, in the range of 1 to 65535.

Description Use the **display ripng database** command to display all active routes in the RIPng advertising database, which are sent in normal RIPng update messages.

Examples # Display the active routes in the database of RIPng process 100.

```
<Sysname> display ripng 100 database
 2001:7B::2:2A1:5DE/64,
   cost 4, Imported
 1:13::/120,
   cost 4, Imported
 1:32::/120,
   cost 4, Imported
 1:33::/120,
   cost 4, Imported
 100::/32,
   via FE80::200:5EFF:FE04:3302, cost 2
 3FFE:C00:C18:1::/64,
   via FE80::200:5EFF:FE04:B602, cost 2
 3FFE:C00:C18:1::/64,
   via FE80::200:5EFF:FE04:B601, cost 2
 3FFE:C00:C18:2::/64,
   via FE80::200:5EFF:FE04:B602, cost 2
 3FFE:C00:C18:3::/64,
   via FE80::200:5EFF:FE04:B601, cost 2
 4000:1::/64,
   via FE80::200:5EFF:FE04:3302, cost 2
 4000:2::/64,
   via FE80::200:5EFF:FE04:3302, cost 2
```

Table 106 Description on fields of the display ripng database command

| Field | Description |
|-----------------------|--|
| 2001:7B::2:2A1:5DE/64 | IPv6 destination address/prefix length |
| via | Next hop IPv6 address |

Table 106 Description on fields of the display ripng database command

| Field | Description |
|----------|--|
| cost | Route metric value |
| Imported | Routes learnt from other routing protocols |

display ripng interface

Syntax `display ripng process-id interface [interface-type interface-number]`

View Any view

Parameters *process-id*: RIPng process ID, in the range of 1 to 65535.

interface-type interface-number: Specified an interface.

Description Use the **display ripng interface** command to display the interface information of the RIPng process.

If no interface is specified, information about all interfaces of the RIPng process will be displayed.

Examples # Display the interface information of RIPng process 1.

```
<Sysname> display ripng 1 interface
```

```
Interface-name: Vlan-interface 100
  Link Local Address: FE80::200:5EFF:FE19:3E00
  Split-horizon: on           Poison-reverse: off
  MetricIn: 0                 MetricOut: 1
  Default route: off
```

Table 107 Field descriptions of the display ripng interface command

| Field | Description |
|--------------------|--|
| Interface-name | Name of an interface running RIPng. |
| Link Local Address | Link-local address of an interface running RIPng |
| Split-horizon | Indicates whether the split horizon function is enabled (on: Enabled off: Disabled). |
| Poison-reverse | Indicates whether the poison reverse function is enabled (on: Enabled off: Disabled). |
| MetricIn/MetricOut | Additional metric to incoming and outgoing routes |
| Default route | <ul style="list-style-type: none"> ■ Only/Originate: Only means that the interface advertises only default route. Originate means that the default route and other RIPng routes are advertised. ■ Off, indicates that no default route is advertised or the garbage-collect time expires after the default route advertisement was disabled. ■ In garbage-collect status: With default route advertisement disabled, the interface advertises the default route with metric 16 during the garbage-collect time. |

display ripng route

Syntax `display ripng process-id route`

View Any view

Parameters *process-id*: RIPng process ID, in the range of 1 to 65535.

Description Use the **display ripng route** command to display all RIPng routes and timers associated to each route of a RIPng process.

Examples # Display the routing information of RIPng process 100.

```
<Sysname> display ripng 100 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
  -----

  Peer FE80::20F:E2FF:FE00:220A on Vlan-interface100
  Dest 4:3::/64,
    via FE80::20F:E2FF:FE00:220A, cost 1, tag 0, A, 34 Sec
```

Table 108 Field descriptions of the display ripng route command

| Field | Description |
|-------|---|
| Peer | Neighbor connected to the interface |
| Dest | IPv6 destination address |
| via | Next hop IPv6 address |
| cost | Routing metric value |
| tag | Route tag |
| Sec | Time that a route entry stays in a particular state |
| A" | The route is in the aging state |
| S" | The route is in the suppressed state |
| G" | The route is in the Garbage-collect state |

filter-policy export

Syntax `filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [protocol [process-id]]`

`undo filter-policy export [protocol [process-id]]`

View RIPng view

Parameters *acl6-number*: Specifies the number of an ACL to filter advertised routing information, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list used to filter routing information, a string of 1 to 19 characters.

protocol: Filter routes redistributed from a routing protocol, currently including **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, and **static**

process-id: Process number of the specified routing protocol, in the range of 1 to 65535. This argument is specified only when the routing protocol is **ripng**, **ospfv3**, or **isisv6**.

Description Use the **filter-policy export** command to define an outbound route filtering policy. Only routes passing the filter can be advertised in the update messages.

Use the **undo filter-policy export** command to restore the default.

By default, RIPng does not filter any outbound routing information.

With the *protocol* argument specified, only routing information redistributed from the specified routing protocol will be filtered. Otherwise, all outgoing routing information will be filtered.

Examples # Use IPv6 prefix list Filter 2 to filter advertised RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter2 export
```

filter-policy import

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View RIPng view

Parameters *acl6-number*: Specifies the number of an ACL to filter incoming routing information, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 Prefix list to filter incoming routes, in the range 1 to 19 characters.

Description Use the **filter-policy import** command to define an inbound route filtering policy. Only routes which match the filtering policy can be received.

Use the **undo filter-policy import** command to disable inbound route filtering.

By default, RIPng does not filter incoming routing information.

Examples # Reference IPv6 prefix list **Filter1** to filter incoming RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter1 import
```

import-route

Syntax **import-route** *protocol* [*process-id*] [**allow-ibgp**] [**cost** *cost* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

View RIPng view

Parameters *protocol*: Specifies a routing protocol from which to redistribute routes. Currently, it can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

process-id: Process number of the specified routing protocol, in the range of 1 to 65535, with the default as 1. This argument is available only when the routing protocol is **isisv6**, **ospfv3**, or **ripng**.

cost: Routing metric of redistributed routes, in the range of 0 to 16. If *cost value* is not specified, the metric is the default metric specified by the **default cost** command.

route-policy *route-policy-name*: Specifies a routing policy by its name with 1 to 19 characters.

allow-ibgp: Optional keyword when the specified *protocol* is **bgp4+**. The **import-route bgp4+** command redistributes only EBGp routes. The **import-route bgp4+ allow-ibgp** command redistributes additionally IBGP routes, thus be cautious when using it.

Description Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to disable redistributing routes from another routing protocol.

By default, RIPng does not redistribute routes from other routing protocols.

- You can configure a routing policy to redistribute only needed routes.
- You can specify a cost for redistributed routes using keyword **cost**.

Related commands: **default cost**.

Examples # Redistribute IPv6-IS-IS routes (process 7) and specify the metric as 7.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route isisv6 7 cost 7
```

maximum load-balancing

Syntax **maximum load-balancing** *number*

undo maximum load-balancing**View** RIPng view**Parameters** *number*: Maximum number of equal-cost load-balanced routes. Its value is in the range 1 to 4.**Description** Use the **maximum load-balancing** command to specify the maximum number of equal cost routes for load balancing.Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal cost routes for load balancing is 4.

*Configure the maximum number according to the memory size.***Examples** # Set the maximum number of load balanced routes with equal cost to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] maximum load-balancing 2
```

Restore the default.

```
[Sysname-ripng-100] undo maximum load-balancing
```

preference**Syntax** **preference** [**route-policy** *route-policy-name*] *preference***undo preference** [**route-policy**]**View** RIPng view**Parameters** *route-policy-name*: Name of a routing policy, in the range of 1 to 19 characters.*preference*: RIPng route priority, in the range of 1 to 255.**Description** Use the **preference** command to specify the RIPng route priority.Use the **undo preference route-policy** command to restore the default.

By default, the priority of a RIPng route is 100.

Using the **route-policy** keyword can set a priority for routes filtered in by the routing policy:

- If a priority is set in the routing policy, the priority applies to matched routes, and the priority set by the **preference** command applies to routes not matched.

- If no priority is set in the routing policy, the one set by the **preference** command applies to all routes.

Examples # Set the RIPng route priority to 120.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] preference 120
```

Restore the default RIPng route priority.

```
[Sysname-ripng-100] undo preference
```

ripng

Syntax **ripng** [*process-id*]
undo ripng [*process-id*]

View System view

Parameters *process-id*: RIPng process ID, in the range of 1 to 65535. The default value is 1.

Description Use the **ripng** command to create a RIPng process and enter RIPng view.
 Use the **undo ripng** command to disable a RIPng process.
 By default, no RIPng process is enabled.

Examples # Create RIPng process 100 and enter its view.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100]
```

Disable RIPng process 100.

```
[Sysname] undo ripng 100
```

ripng default-route

Syntax **ripng default-route** { **only** | **originate** } [**cost** *cost*]
undo ripng default-route

View Interface view

Parameters **only**: Indicates that only the IPv6 default route (::/0) is advertised via the interface.
originate: Indicates that the IPv6 default route (::/0) is advertised without suppressing other routes.

cost: Metric of the advertised default route, in the range of 1 to 15, with a default value of 1.

Description Use the **ripng default-route** command to advertise a default route with the specified routing metric to a RIPng neighbor.

Use the **undo ripng default-route** command to stop advertising and forwarding the default route.

By default, a RIP process does not advertise any default route.

After you execute this command, the generated RIPng default route is advertised in a route update over the specified interface. This IPv6 default route is advertised without considering whether it already exists in local IPv6 routing table.

Examples # Advertise only the default route via VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng default-route only
```

Advertise the default route together with other routes via VLAN-interface 101.

```
<Sysname> system-view
[Sysname] interface vlan-interface 101
[Sysname-Vlan-interface101] ripng default-route originate
```

ripng enable

Syntax **ripng** *process-id* **enable**

undo ripng enable

View Interface view

Parameters *process-id*: RIPng process ID, in the range of 1 to 65535.

Description Use the **ripng enable** command to enable RIPng on the specified interface.

Use the **undo ripng enable** command to disable RIPng on the specified interface.

By default, RIPng is disabled on an interface.

Examples # Enable RIPng100 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng 100 enable
```

ripng metricin

Syntax `ripng metricin value`

`undo ripng metricin`

View Interface view

Parameters *value*: Additional metric for received routes, in the range of 0 to 16.

Description Use the **ripng metricin** command to specify an additional metric for received RIPng routes.

Use the **undo ripng metricin** command to restore the default.

By default, the additional metric to received routes is 0.

Related commands: **ripng metricout.**

Examples # Specify the additional routing metric as 12 for RIPng routes received by VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricin 12
```

ripng metricout

Syntax `ripng metricout value`

`undo ripng metricout`

View Interface view

Parameters *value*: Additional metric to advertised routes, in the range of 1 to 16.

Description Use the **ripng metricout** command to configure an additional metric for RIPng routes advertised by an interface.

Use the **undo rip metricout** command to restore the default.

The default additional routing metric is 1.

Related commands: **ripng metricin.**

Examples # Set the additional metric to 12 for routes advertised by VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ripng metricout 12
```

ripng poison-reverse

| | |
|--------------------|--|
| Syntax | ripng poison-reverse
undo ripng poison-reverse |
| View | Interface view |
| Parameters | None |
| Description | Use the rip poison-reverse command to enable the poison reverse function.

Use the undo rip poison-reverse command to disable the poison reverse function.

By default, the poison reverse function is disabled. |
| Examples | Enable the poison reverse function for RIPng update messages on VLAN-interface 100.

<pre><Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng poison-reverse</pre> |

ripng split-horizon

| | |
|--------------------|--|
| Syntax | ripng split-horizon
undo ripng split-horizon |
| View | Interface view |
| Parameters | None |
| Description | Use the rip split-horizon command to enable the split horizon function.

Use the undo rip split-horizon command to disable the split horizon function.

By default, the split horizon function is enabled.

Note that: <ul style="list-style-type: none">■ The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.■ In special cases, make sure that it is necessary to disable the split horizon function before doing so. |



If both the poison reverse and split horizon functions are enabled, only the poison reverse function takes effect.

Examples Enable the split horizon function on Vlan-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng split-horizon
```

ripng summary-address

Syntax **ripng summary-address** *ipv6-address prefix-length*

undo ripng summary-address *ipv6-address prefix-length*

View Interface view

Parameters *ipv6-address*: Destination IPv6 address prefix of the summary route.

prefix-length: Destination IPv6 address prefix length of the summary route, in the range 0 to 128.

Description Use the **ripng summary-address** command to configure a summary advertised through the interface.

Use the **undo ripng summary-address** command to remove the summary.

If the prefix and the prefix length of a route match the IPv6 prefix, the IPv6 prefix will be advertised instead. Thus, one route can be advertised on behalf of many routes. After summarization, the summary route cost is the lowest cost among summarized routes.

Examples # Assign an IPv6 address with the 64-bit prefix to VLAN-interface 100 and configure a summary with the 35-bit prefix length.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001:200::3EFF:FE11:6770/64
[Sysname-Vlan-interface100] ripng summary-address 2001:200:: 35
```

timers

Syntax **timers** { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* }*

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** }*

View RIPng view

- Parameters**
- garbage-collect-value*: Interval of the garbage-collect timer in seconds, in the range of 1 to 86400.
 - suppress-value*: Interval of the suppress timer in seconds, in the range of 0 to 86400.
 - timeout-value*: Interval of the timeout timer in seconds, in the range of 1 to 86400.
 - update-value*: Interval of the update timer in seconds, in the range of 1 to 86400.

Description Use the **timers** command to configure RIPng timers.

Use the **undo timers** command to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIPng is controlled by the above four timers.

- The update timer defines the interval between update messages.
- The timeout timer defines the route aging time. If no update message related to a route is received within the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines how long a RIPng route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIPng advertises the route with the routing metric set to 16. If no update message is announced for that route before the garbage-collect timer expires, the route will completely be deleted from the routing table.

Note that:

- You are not recommended to change the default values of these timers under normal circumstances.
- The lengths of these timers must be kept consistent on all routers and access servers in the network

Examples # Configure the update, timeout, suppress, and garbage-collect timers as 5s, 15s, 15s and 30s.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] timers update 5
[Sysname-ripng-100] timers timeout 15
[Sysname-ripng-100] timers suppress 15
[Sysname-ripng-100] timers garbage-collect 30
```

31

IPv6 OSPFv3 CONFIGURATION COMMANDS



At present, the 0231A92P modules in the S7900E do not support IPv6.

abr-summary

Syntax `abr-summary ipv6-address prefix-length [not-advertise]`

`undo abr-summary ipv6-address prefix-length`

View OSPFv3 area view

Parameters *ipv6-address*: Destination IPv6 address of the summary route.

prefix-length: Prefix length of the destination IPv6 address, in the range 0 to 128. This argument specifies the number of consecutive 1s of the prefix, which defines the network ID.

not-advertise: Specifies not to advertise the summary IPv6 route.

Description Use the **abr-summary** command to configure an IPv6 summary route on an area border router.

Use the **undo abr-summary** command to remove an IPv6 summary route. Then the summarized routes are advertised.

By default, no route summarization is available on an ABR.

You can use this command only on an ABR to configure a summary route for the area. The ABR advertises only the summary route to other areas. Multiple contiguous networks may be available in an area, where you can summarize them with one route for advertisement.

Examples # Summarize networks 2000:1:1:1::/64 and 2000:1:1:2::/64 in Area 1 with 2000:1:1::/48.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

area

Syntax `area area-id`

View OSPFv3 view

Parameters *area-id*: ID of an area, a decimal integer (in the range of 0 to 4294967295 and changed to IPv4 address format by the system) or an IPv4 address.

Description Use the **area** command to enter OSPFv3 area view.



The undo form of the command is not available. An area is removed automatically if there is no configuration and no interface is up in the area.

Examples # Enter OSPFv3 Area 0 view.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0]
```

default cost

Syntax `default cost value`

`undo default cost`

View OSPFv3 view

Parameters *value*: Specifies a default cost for redistributed routes, in the range of 1 to 16777214.

Description Use the **default cost** command to configure a default cost for redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default cost is 1.

You need to configure the default cost value for redistributed routes to advertise them throughout the whole AS.

If multiple OSPFv3 processes are available, use of this command takes effect for the current process only.

Examples # Specify the default cost for redistributed routes as 10.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default cost 10
```

default-cost

Syntax **default-cost** *value*

undo default-cost

View OSPFv3 area view

Parameters *value*: Specifies a cost for the default route advertised to the stub area, in the range of 0 to 65535. The default is 1.

Description Use the **default-cost** command to specify the cost of the default route to be advertised to the stub area.

Use the **undo-default-cost** command to restore the default value.

Use of this command is only available on the ABR that is connected to a stub area.

You have two commands to configure a stub area: **stub**, **defaulted-cost**. You need to use the **stub** command on routers connected to a stub area to configure the area as stub.

If multiple OSPFv3 processes are running, use of this command takes effect only for the current process.

Related commands: **stub**.

Examples # Configure Area1 as a stub area, and specify the cost of the default route advertised to the stub area as 60.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
[Sysname-ospfv3-1-area-0.0.0.1] default-cost 60
```

display ospfv3

Syntax **display ospfv3** [*process-id*]

View Any view

Parameters *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

Description Use the **display ospfv3** command to display the brief information of an OSPFv3 process. If no process ID is specified, OSPFv3 brief information about all processes will be displayed.

Examples # Display brief information about all OSPFv3 processes.

```

<Sysname> display ospfv3
Routing Process "OSPFv3 (1)" with ID 0.0.0.0
  SPF schedule delay 5 secs, Hold time between SPFs 10 secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
  Number of external LSA 0. These external LSAs' checksum Sum 0x0000
  Number of AS-Scoped Unknown LSA 0
  Number of LSA originated 0
  Number of LSA received 0
  Number of areas in this router is 2
    Area BACKBONE(0)
      Number of interfaces in this area is 1
      SPF algorithm executed 1 times
      Number of LSA 0. These LSAs' checksum Sum 0x0000
      Number of Unknown LSA 0
    Area 0.0.0.1
      Number of interfaces in this area is 0
      SPF algorithm executed 1 times
      Number of LSA 0. These LSAs' checksum Sum 0x0000
      Number of Unknown LSA 0
Routing Process "OSPFv3 (3)" with ID 0.0.0.0
  SPF schedule delay 2 secs, Hold time between SPFs 2 secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
  Number of external LSA 0. These external LSAs' checksum Sum 0x0000
  Number of AS-Scoped Unknown LSA 0
  Number of LSA originated 0
  Number of LSA received 0
  Number of areas in this router is 0

```

Table 109 Field descriptions of the display ospfv3 command

| Field | Description |
|--|--|
| Routing Process "OSPFv3 (1)" with ID 0.0.0.0 | OSPFv3 process is 1, and router ID is 0.0.0.0. |
| SPF schedule delay | Delay interval of SPF calculation |
| Hold time between SPFs | Hold time between SPF calculations |
| Minimum LSA interval | Minimum interval for generating LSAs |
| Minimum LSA arrival | Minimum LSA repeat arrival interval |
| Number of external LSA | Number of ASE LSAs |
| These external LSAs' checksum Sum | Sum of all the ASE LSAs' checksum |
| Number of AS-Scoped Unknown LSA | Number of LSAs with unknown flooding scope |
| Number of LSA originated | Number of LSAs originated |
| Number of LSA received | Number of LSAs received |
| Number of areas in this router | Number of areas this router is attached to |
| Area | Area ID |
| Number of interfaces in this area | Number of interfaces attached to this area |
| SPF algorithm executed 1 times | SPF algorithm is executed 1 time |
| Number of LSA | Number of LSAs |
| These LSAs' checksum Sum | Sum of all LSAs' checksum |
| Number of Unknown LSA | Number of unknown LSAs |

display ospfv3 interface

Syntax `display ospfv3 interface [interface-type interface-number | statistic]`

View Any view

Parameters `interface-type interface-number`: Interface type and interface number.

statistic: Displays the interface statistics.

Description Use the **display ospfv3 interface** command to display OSPFv3 interface information.

Examples # Display OSPFv3 interface information of VLAN-interface 200.

```
<Sysname >display ospfv3 interface Vlan-interface 200
Vlan-interface200 is up, line protocol is up
  Interface ID 11665607
  IPv6 Prefixes
    FE80::20F:E2FF:FE00:5 (Link-Local Address)
    2001:1::2
  OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0
  Router ID: 1.1.1.1, Network Type: BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State: DR, Priority: 1
  Designated Router (ID) 1.1.1.1
    Interface Address: FE80::20F:E2FF:FE00:5
  Backup Designated Router (ID): 2.2.2.2
    Interface Address: FE80::20F:E2FF:FE00:2205
  Timer interval configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
  Hello due in 00:00:08
  Neighbor Count is 1, Adjacent neighbor count is 1
```

Table 110 Field descriptions of the display ospfv3 interface command

| Field | Description |
|---|---|
| Interface ID | Interface ID |
| IPv6 Prefixes | IPv6 Prefix |
| OSPFv3 Process | OSPFv3 Process |
| Area | Area ID |
| Instance ID | Instance ID |
| Router ID | Router ID |
| Network Type | Network type of the interface |
| Cost | Cost value of the interface |
| Transmit Delay | Transmission delay of the interface |
| State | Interface state |
| Priority | DR priority of the interface |
| Designated Router (ID) | ID of the designated router on this link |
| Backup Designated Router (ID) | ID of the backup designated router on this link |
| Interface Address | Interface address |
| Timer interval configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5 | Time intervals in seconds configured on the interface, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5 |
| Hello due in 00:00:08 | Hello packet will be sent in 8 seconds |


```

Link State ID  Origin Router  Age  Seq#  CkSum
0.15.0.9      6.6.6.6      0264 0x80000001 0x3498
                Intra-Area-Prefix-LSA (Area 0.0.0.0)
-----
Link State ID  Origin Router  Age  Seq#  CkSum  Prefix  Reference
0.0.0.2      6.6.6.6      0263 0x80000001 0x95c4  1  Network-LSA

```

Table 111 Field descriptions of the display ospfv3 lsdb command

| Field | Description |
|-----------------------|------------------------|
| Link-LSA | Type 8 LSA |
| Link State ID | Link State ID |
| Origin Router | Originating Router |
| Age | Age of LSAs |
| Seq# | LSA sequence number |
| CkSum | LSA Checksum |
| Prefix | Number of Prefixes |
| Router-LSA | Router-LSA |
| Link | Number of links |
| Network-LSA | Network-LSA |
| Intra-Area-Prefix-LSA | Type 9 LSA |
| Reference | Type of referenced LSA |

Display Link-local LSA information in the LSDB.

```
<Sysname> display ospfv3 lsdb link
```

```
OSPFv3 Router with ID (4.4.4.4) (Process 1)
```

```
Link-LSA (Interface Vlan-interface400)
```

```

-----
LS age          : 1536
LS Type        : Link-LSA
Link State ID   : 0.178.1.143
Originating Router: 3.3.3.3
LS Seq Number   : 0x80000003
Checksum       : 0x22A7
Length         : 56
Priority        : 1
Options        : 0x000011 (-|R|-|-|V6)
Link-Local Address: FE80::2E0:FCFF:FE00:242A
Number of Prefixes: 1
    Prefix      : 2001:2::/64
    Prefix Options: 0 (-|-|-|-)
LS age          : 1558
LS Type        : Link-LSA
Link State ID   : 0.178.1.143
Originating Router: 4.4.4.4
LS Seq Number   : 0x80000003
Checksum       : 0x4A6A
Length         : 56
Priority        : 1
Options        : 0x000011 (-|R|-|-|V6)
Link-Local Address: FE80::2E0:FCFF:FE00:550A

```

```

Number of Prefixes: 1
Prefix           : 2001:2::/64
Prefix Options: 0 (-|-|-|-)

```

Table 112 Field descriptions of the display ospfv3 lsdb command

| Field | Description |
|--------------------|---------------------|
| LS age | Age of LSA |
| LS Type | Type of LSA |
| Originating Router | Originating Router |
| LS Seq Number | LSA Sequence Number |
| Checksum | LSA Checksum |
| Length | LSA Length |
| Priority | Router Priority |
| Options | Options |
| Link-Local Address | Link-Local Address |
| Number of Prefixes | Number of Prefixes |
| Prefix | Address prefix |
| Prefix Options | Prefix options |

display ospfv3 lsdb statistic

Syntax `display ospfv3 lsdb statistic`

View Any view

Parameters None

Description Use the **display ospfv3 lsdb statistic** command to display LSA statistics in the OSPFv3 LSDB.

Examples # Display OSPFv3 LSDB statistics.

```
<System> display ospfv3 lsdb statistic
```

```

                OSPFv3 Router with ID (1.1.1.1) (Process 1)
                  LSA Statistics
-----
Area ID          Router   Network  InterPre  InterRou  IntraPre  Link   ASE
0.0.0.0          2         1         1          0          1         0
0.0.0.1          1         0         1          0          1         0
Total            3         1         2          0          2         3      0

```

Table 113 Descriptions on the fields of the display ospfv3 lsdb statistic command

| Field | Description |
|----------|------------------------------|
| Area ID | Area ID |
| Router | Router-LSA number |
| Network | Network-LSA number |
| InterPre | Inter-Area-Prefix-LSA number |
| InterRou | Inter-Area-Router-LSA number |

Table 113 Descriptions on the fields of the display ospfv3 lsdb statistic command

| Field | Description |
|----------|------------------------------|
| IntraPre | Intra-Area-Prefix-LSA number |
| Link | Link-LSA number |
| ASE | AS-external-LSA number |
| Total | Total LSA number |

display ospfv3 next-hop

Syntax **display ospfv3** [*process-id*] **next-hop**

View Any view

Parameters *process-id*: Specifies ID of an OSPFv3 process, ranging from 1 to 65535.

Description Use the **display ospfv3 next-hop** command to display OSPFv3 next hop information.

If no process is specified, next hop information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 next hop information.

```
<Sysname> display ospfv3 next-hop
```

```

                OSPFv3 Router with ID (2.2.2.2) (Process 1)
Neighbor-Id      Next-Hop                Interface      RefCount
1.1.1.1          FE80::20F:E2FF:FE00:1          Vlan100       1

```

Table 114 Field descriptions of the display ospfv3 next-hop command

| Field | Description |
|-------------|-----------------------|
| Neighbor-Id | Neighboring router ID |
| Next-hop | Next-hop address |
| Interface | Outbound interface |
| RefCount | Reference count |

display ospfv3 peer

Syntax **display ospfv3** [*process-id*] [**area** *area-id*] **peer** [[*interface-type* *interface-number*] [**verbose**]] [*peer-router-id*]

View Any view

Parameters *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

area: Specifies to display neighbor information of the specified area.

area-id: The ID of an area, a decimal integer that is translated into IPv4 address format by the system (in the range of 0 to 4294967295) or an IPv4 address.

interface-type interface-number: interface type and number.

verbose: Display detailed neighbor information.

peer-router-id: Router-ID of the specified neighbor.

Description Use the **display ospfv3 peer** command to display OSPFv3 neighbor information.

- If no *area-id* is specified, the neighbor information of all areas is displayed.
- If no *process-id* is specified, the information of all processes is displayed.
- If no interface or neighbor Router-ID is specified, the neighbor information of all interfaces is displayed.

Examples # Display the neighbor information of OSPFv3 process 1 on an interface.

```
<Sysname> display ospfv3 1 peer Vlan-interface 400
```

```
OSPFv3 Process (1)
```

```
OSPFv3 Area (0.0.0.2)
```

| Neighbor ID | Pri | State | Dead Time | Interface | Instance ID |
|-------------|-----|-------------|-----------|-----------|-------------|
| 3.3.3.3 | 1 | Full/Backup | 00:00:38 | Vlan400 | 0 |

Table 115 Field descriptions of the display ospfv3 peer command

| Field | Description |
|-------------|-------------------------------------|
| Neighbor ID | Neighbor ID |
| Pri | Priority of neighbor router |
| State | Neighbor state |
| Dead Time | Dead time remained |
| Interface | Interface connected to the neighbor |
| Instance ID | Instance ID |

Display detailed neighbor information of OSPFv3 process 1 of an interface.

```
<Sysname> display ospfv3 1 peer Vlan-interface 400 verbose
```

```
OSPFv3 Process (1)
```

```
Neighbor: 3.3.3.3, interface address: FE80::2E0:FCFF:FE00:242A
In the area 0.0.0.2 via interface Vlan-interface400
DR is 4.4.4.4 BDR is 3.3.3.3
Options is 0x000011 (-|R|-|-|V6)
Dead timer due in 00:00:35
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
```

Table 116 Field descriptions of the display ospfv3 peer verbose command

| Field | Description |
|-------------------|-------------------|
| Neighbor | Neighbor ID |
| interface address | Interface address |

Table 116 Field descriptions of the display ospfv3 peer verbose command

| Field | Description |
|---|--|
| In the area 0.0.0.2 via interface
vlan-interface 400 | Interface VLAN-interface 400 belongs to area 1. |
| DR is 4.4.4.4 BDR is 3.3.3.3 | DR is 4.4.4.4. BDR is 3.3.3.3 |
| Options is 0x000011 (- R - V6) | The option is 0x000011 (- R - V6). |
| Dead timer due in 00:00:35 | Dead timer due in 35 seconds |
| Database Summary List | Number of LSAs sent in DD packet |
| Link State Request List | Number of LSAs in the link state request list |
| Link State Retransmission List | Number of LSAs in the link state retransmission list |

display ospfv3 peer statistic

Syntax `display ospfv3 peer statistic`

View Any view

Parameters None

Description Use the **display ospfv3 peer statistic** command to display information about all OSPFv3 neighbors on the router, that is, numbers of neighbors in different states.

Examples # Display information about all OSPFv3 neighbors.

```
<Sysname> display ospfv3 peer statistic
```

```

                                OSPFv3 Router with ID (1.1.1.1) (Process 1)
                                Neighbor Statistics
-----
Area ID          Down      Init      2-way     ExStar    Exchange Loading  Full
0.0.0.0          0         0         0         0         0         0         1
Total            0         0         0         0         0         0         1

```

Table 117 Field descriptions of the display ospfv3 peer statistic command

| Field | Description |
|----------|--|
| Area ID | Area ID |
| Down | In this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time. |
| Init | In this state, the device received a Hello packet from the neighbor but the packet contains no Router ID of the neighbor. Mutual communication is not setup. |
| 2-Way | Indicates mutual communication between the router and its neighbor is available. DR/BDR election is finished under this state (or higher). |
| ExStar | In this state, the router decides on the initial DD sequence number and master/slave relationship of the two parties. |
| Exchange | In this state, the router exchanges DD packets with the neighbor. |
| Loading | In this state, the router sends LSRs to request the neighbor for needed LSAs. |

Table 117 Field descriptions of the display ospfv3 peer statistic command

| Field | Description |
|-------|---|
| Full | Indicates LSDB synchronization has been accomplished between neighbors. |
| Total | Total number of neighbors under the same state |

display ospfv3 request-list

Syntax **display ospfv3** [*process-id*] **request-list** [{ **external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **router** } [*link-state-id*] [**originate-router** *ip-address*] | **statistics**]

View Any view

Parameters *process-id*: OSPFv3 process ID, in the range 1 to 65535.

external: Displays the AS-external LSA information of the OSPFv3 link state request list.

inter-prefix: Displays the Inter-area-prefix LSA information of the OSPFv3 link state request list.

inter-router: Displays the Inter-area-router LSA information of the OSPFv3 link state request list.

intra-prefix: Displays the Intra-area-prefix LSA information of the OSPFv3 link state request list.

link: Displays the Link LSA information of the OSPFv3 link state request list.

network: Displays the Network-LSA information of the OSPFv3 link state request list.

router: Displays the Router-LSA information of the OSPFv3 link state request list.

link-state-id: Link state ID, in the format of an IPv4 address.

originate-router *ip-address*: Specifies the router ID of an advertising router.

statistics: Displays the LSA statistics of the OSPFv3 link state request list.

Description Use the **display ospfv3 request-list** command to display OSPFv3 link state request list information.

If no process is specified, link state request list information of all OSPFv3 processes is displayed.

Examples # Display the information of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list
```

```
OSPFv3 Router with ID (11.1.1.1) (Process 1)
```



```

                Interface Vlan100      Area-ID 0.0.0.0
-----
                Nbr-ID 12.1.1.1
LS-Type          LS-ID          AdvRouter      SeqNum      Age  CkSum
Router-LSA      0.0.0.0          12.1.1.1      0x80000014  774  0xe5b0

```

Table 118 Field descriptions of the display ospfv3 request-list command

| Field | Description |
|-----------|---------------------|
| Interface | Interface name |
| Area-ID | Area ID |
| Nbr-ID | Neighbor router ID |
| LS-Type | Type of LSA |
| LS-ID | Link state ID |
| AdvRouter | Advertising router |
| SeqNum | LSA sequence number |
| Age | Age of LSA |
| CkSum | Checksum |

Display the statistics of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list statistics
```

```

                OSPFv3 Router with ID (1.1.1.1) (Process 1)
Interface      Neighbor      LSA-Count
Vlan100        2.2.2.2      0

```

Table 119 Field descriptions of the display ospfv3 request-list statistics command

| Field | Description |
|-----------|------------------------------------|
| Interface | Interface name |
| Neighbor | Neighbor router ID |
| LSA-Count | Number of LSAs in the request list |

display ospfv3 retrans-list

Syntax `display ospfv3 [process-id] retrans-list [{ external | inter-prefix | inter-router | intra-prefix | link | network | router } [link-state-id] [originate-router ip-address] | statistics]`

View Any view

Parameters *process-id*: OSPFv3 process ID, in the range 1 to 65535.

external: Displays the AS-external LSA information of the OSPFv3 link state retransmission list.

inter-prefix: Displays the Inter-area-prefix LSA information of the OSPFv3 link state retransmission list.

inter-router: Displays the Inter-area-router LSA information of the OSPFv3 link state retransmission list.

intra-prefix: Displays the Intra-area-prefix LSA information of the OSPFv3 link state retransmission list.

link: Displays the Link LSA information of the OSPFv3 link state retransmission list.

network: Displays the Network-LSA information of the OSPFv3 link state retransmission list.

router: Displays the Router-LSA information of the OSPFv3 link state retransmission list.

link-state-id: Link state ID, in the format of an IPv4 address.

originate-router ip-address: Specifies the router ID of an advertising router.

statistics: Displays the LSA statistics of the OSPFv3 link state retransmission list.

Description Use the **display ospfv3 retrans-list** command to display OSPFv3 link state retransmission list.

If no process is specified, link state retransmission list information of all OSPFv3 processes is displayed.

Examples # Display the information of OSPFv3 link state retransmission list.

```
<Sysname> display ospfv3 retrans-list
```

```

                OSPFv3 Router with ID (11.1.1.1) (Process 1)
                Interface Vlan100      Area-ID 0.0.0.0
                -----
                Nbr-ID      12.1.1.1
LS-Type      LS-ID      AdvRouter      SeqNum      Age  CkSum
Link-LSA     0.15.0.24      12.1.1.1      0x80000003  519  0x7823
Router-LSA   0.0.0.0        12.1.1.1      0x80000014  774  0xe5b0

```

Table 120 Field descriptions of the display ospfv3 retrans-list command

| Field | Description |
|-----------|---------------------|
| Interface | Interface name |
| Area-ID | Area ID |
| Nbr-ID | Neighbor router ID |
| LS-Type | Type of LSA |
| LS-ID | Link state ID |
| AdvRouter | Advertising Router |
| SeqNum | LSA sequence Number |
| Age | Age of LSA |
| CkSum | Checksum |

Display the statistics of OSPFv3 link state retransmission list.

```
<Sysname> display ospfv3 retrans-list statistics
```

```

                OSPFv3 Router with ID (3.3.3.3) (Process 1)
Interface Neighbor      LSA-Count
Vlan100   1.1.1.1      0

```

Table 121 Field descriptions of the display ospfv3 retrans-list statistics command

| Field | Description |
|-----------|---|
| Interface | Interface name |
| Neighbor | Neighbor ID |
| LSA-Count | Number of LSAs in the retransmission request list |

display ospfv3 routing

Syntax **display ospfv3** [*process-id*] **routing** [*ipv6-address prefix-length* | *ipv6-address/prefix-length* | **abr-routes** | **asbr-routes** | **all** | **statistics**]

View Any view

Parameters *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

ipv6-address: IPv6 address prefix.

prefix-length: Prefix length, in the range 0 to 128.

abr-routes: Displays routes to ABR.

asbr-routes: Displays routes to ASBR.

all: Displays all routes.

statistics: Displays the OSPFv3 routing table statistics.

Description Use the **display ospfv3 routing** command to display OSPFv3 routing table information.

If no process is specified, routing table information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 routing table information.

```
<Sysname> display ospfv3 routing

E1 - Type 1 external route,   IA - Inter area route,   I - Intra area route
E2 - Type 2 external route,   * - Seleted route

          OSPFv3 Router with ID (1.1.1.1) (Process 1)
-----
*Destination: 2001::/64
  Type       : I                               Cost       : 1
  NextHop    : directly-connected              Interface: Vlan100
```

Table 122 Field descriptions of the display ospfv3 routing command

| Field | Description |
|-------------|-----------------------------|
| Destination | Destination network segment |
| Type | Route type |
| Cost | Route cost value |
| Next-hop | Next hop address |

Table 122 Field descriptions of the display ospfv3 routing command

| Field | Description |
|-----------|--------------------|
| Interface | Outbound interface |

Display the statistics of OSPFv3 routing table.

```
<Sysname> display ospfv3 routing statistics
```

```

                OSPFv3 Router with ID (3.3.3.3) (Process 1)
                OSPFv3 Routing Statistics
Intra-area-routes : 1
Inter-area-routes : 1
External-routes   : 0

```

Table 123 Field descriptions of the display ospfv3 routing statistics command

| Field | Description |
|-------------------|-----------------------------|
| Intra-area-routes | Number of Intra-area-routes |
| Inter-area-routes | Number of inter-area routes |
| External-routes | Number of external routes |

display ospfv3 statistic

Syntax `display ospfv3 statistic`

View Any view

Parameters None

Description Use the **display ospfv3 statistic** command to display outbound/inbound OSPFv3 packet statistics on associated interface(s).

Examples # Display outbound/inbound OSPFv3 packet statistics on associated interfaces.

```
<Sysname> display ospfv3 statistic
```

```

                OSPFv3 Statistics
Interface Vlan-interface100 Instance 0
Type      Input      Output
Hello     189                63
DB Description 10                8
Ls Req    2                  1
Ls Upd    16                6
Ls Ack    10                6

```

Table 124 Field descriptions of the display ospfv3 statistics command

| Field | Description |
|-----------|---|
| Interface | Interface name |
| Instance | Instance number |
| Type | Type of packet |
| Input | Number of packets received by the interface |

Table 124 Field descriptions of the display ospfv3 statistics command

| Field | Description |
|----------------|---|
| Output | Number of packets sent by the interface |
| Hello | Hello packet |
| DB Description | Database description packet |
| Ls Req | Link state request packet |
| Ls Upd | Link state update packet |
| Ls Ack | Link state acknowledgement packet |

display ospfv3 topology

Syntax `display ospfv3 [process-id] topology [area area-id]`

View Any view

Parameters *process-id*: Displays the topology information of an OSPFv3 process; The process ID ranges from 1 to 65535.

area: Displays the topology information of the specified area.

area-id: ID of an area, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

Description Use the **display ospfv3 topology** command to display OSPFv3 topology information. If no process is specified, topology information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 area 1 topology information.

```
<Sysname> display ospfv3 topology area 1
```

```

                                OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1) topology
Type  ID(If-Index)      Bits      Metric  Next-Hop      Interface
Rtr   1.1.1.1            --        --
Rtr   2.2.2.2            1         2.2.2.2      Vlan100

```

Table 125 Field descriptions of the display ospfv3 topology command

| Field | Description |
|--------------|--------------------|
| Type | Type of node |
| ID(If-Index) | Router ID |
| Bits | Flag bit |
| Metric | Cost value |
| Next-Hop | Next hop |
| Interface | Outbound interface |

display ospfv3 vlink

- Syntax** `display ospfv3 [process-id] vlink`
- View** Any view
- Parameters** *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.
- Description** Use the **display ospfv3 vlink** command to display OSPFv3 virtual link information. If no process is specified, virtual link information of all OSPFv3 processes is displayed.
- Examples** # Display OSPFv3 virtual link information.

```
<Sysname> display ospfv3 vlink

Virtual Link VLINK1 to router 1.1.1.1 is up
  Transit area :0.0.0.1 via interface Vlan-interface100, instance ID: 0
  Local address: 2000:1::1
  Remote address: 2001:1:1::1
  Transmit Delay is 1 sec, State: P-To-P,
  Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
  Hello due in 00:00:02
  Adjacency state :Full
```

Table 126 Field descriptions of the display ospfv3 vlink command

| Field | Description |
|--|--|
| Virtual Link VLINK1 to router 1.1.1.1 is up | The virtual link VLINK1 to router 1.1.1.1 is up |
| Transit area 0.0.0.1 via interface Vlan-interface100 | Interface VLAN-interface 100 in transit area 0.0.0.1. |
| instance ID | Instance ID |
| Local address | Local IPv6 address |
| Remote address | Remote IPv6 address |
| Transmit Delay | Transmit delay of sending LSAs |
| State | Interface state |
| Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5 | Timer intervals in seconds, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5 |
| Hello due in 00:00:02 | Send hello packets in 2 seconds. |
| Adjacency state | Adjacency state |

filter-policy export

- Syntax** `filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [isisv6 process-id | ospfv3 process-id | ripng process-id | bgp4+ | direct | static]`
- `undo filter-policy export [isisv6 process-id | ospfv3 process-id | ripng process-id | bgp4+ | direct | static]`
- View** OSPFv3 view

- Parameters**
- acl6-number*: Specifies the ACL6 number, ranging from 2000 to 3999.
 - ipv6-prefix** *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.
 - isisv6** *process-id*: Specifies to filter the routes of an IPv6-IS-IS process, which is in the range of 1 to 65535.
 - ospfv3** *process-id*: Specifies to filter the routes of an OSPFv3 process, which is in the range of 1 to 65535.
 - ripng** *process-id*: Specifies to filter the routes of a RIPng process, which in the range of 1 to 65535.
 - bgp4+**: Specifies to filter BGP4+ routes.
 - direct**: Specifies to filter direct routes.
 - static**: Specifies to filter static routes.

- Description**
- Use the **filter-policy export** command to filter redistributed routes.
- Use the **undo filter-policy export** command to remove the configuration.
- If no protocol is specified, all redistributed routes will be filtered.
- By default, IPv6 OSPFv3 does not filter redistributed routes.



*Using the **filter-policy export** command filters only routes redistributed by the **import-route** command. If the **import-route** command is not configured to redistribute routes from other protocols and other OSPFv3 processes, use of the **filter-policy export** command does not take effect.*

- Examples**
- ```
Filter all redistributed routes using IPv6 ACL 2001.
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2002:1:: 64
[Sysname-acl6-basic-2001] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 2001 export
```

---

## filter-policy import

- Syntax** **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**  
**undo filter-policy import**

- View** OSPFv3 view

- Parameters** *acl6-number*: Specifies an ACL number, ranging from 2000 to 3999.

**ipv6-prefix** *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.

**Description** Use the **filter-policy import** command to filter received routes.

Use the **undo filter-policy import** command to remove the configuration.

No received routes are filtered by default.



*Using the **filter-policy import** command only filters routes computed by OSPFv3. The routes that fail to pass are not added to the routing table.*

**Examples** # Filter received routes using the IPv6 prefix list abc.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc permit 2002:1:: 64
[Sysname] ospfv3 1
[Sysname-ospfv3-1] filter-policy ipv6-prefix abc import
```

---

## import-route

**Syntax** **import-route** { **isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** [ **allow-ibgp** ] | **direct** | **static** } [ **cost** *value* | **type** *type* | **route-policy** *route-policy-name* ]\*

**undo import-route** { **isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static** }

**View** OSPFv3 view

**Parameters** **isisv6** *process-id*: Redistributes IPv6 ISIS routes from an IPv6 IS-IS process. The process ID is in the range 1 to 65535.

**ospfv3** *process-id*: Redistributes OSPFv3 routes from an OSPFv3 process. The process ID is in the range 1 to 65535.

**ripng** *process-id*: Redistributes RIPng routes from a RIPng process. The process ID is in the range 1 to 65535.

**bgp4+**: Redistributes BGP4+ routes.

**allow-ibgp**: Allows redistributing IBGP routes.

**direct**: Redistributes direct routes.

**static**: Redistributes static routes.

**cost** *value*: Cost for redistributed routes, ranging from 1 to 16777214. The default is 1.

**type** *type*: Specifies the type for redistributed routes, 1 or 2. It defaults to 2.



**route-policy** *route-policy-name*: Specifies to redistribute only the routes that match the specified route-policy. *route-policy-name* is a string of up to 19 characters.



**CAUTION:** Using the **import-route bgp4+** command redistributes only EBGP routes, while using the **import-route bgp4+ allow-ibgp** command redistributes both EBGP and IBGP routes.

**Description** Use the **import-route** command to redistribute routes.  
Use the **undo import-route** command to disable routes redistribution.  
IPv6 OSPFv3 does not redistribute routes from other protocols by default.

**Examples** # Configure to redistribute routes from RIPng and specify the type as type 2 and cost as 50.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50
```

# Configure OSPFv3 process 100 to redistribute the routes found by OSPFv3 process 160.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] import-route ospfv3 160
```

---

## log-peer-change

**Syntax** **log-peer-change**  
**undo log-peer-change**

**View** OSPFv3 view

**Parameters** None

**Description** Use the **log-peer-change** command to enable the logging on neighbor state changes.

Use the **undo maximum load-balancing** command to disable the logging.

With this feature enabled, information about neighbor state changes of the current OSPFv3 process will display on the configuration terminal.

**Examples** # Disable the logging on neighbor state changes of OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] undo log-peer-change
```

---

**maximum load-balancing**

**Syntax** **maximum load-balancing** *maximum*

**undo maximum load-balancing**

**View** OSPFv3 view

**Parameters** *maximum*: Maximum number of equal-cost routes for load-balancing. The argument being set to 1 means no load balancing is available. Its value is in the range 1 to 4.

**Description** Use the **maximum load-balancing** command to configure the maximum number of equal-cost routes for load-balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal-cost routes for load-balancing in OSPFv3 is 4.

**Examples** # Configure the maximum number of equal-cost routes for load-balancing as 2.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] maximum load-balancing 2
```

---

**ospfv3**

**Syntax** **ospfv3** [ *process-id* ]

**undo ospfv3** [ *process-id* ]

**View** System view

**Parameters** *process-id*: OSPFv3 process ID, ranging from 1 to 65535. The process ID defaults to 1.

**Description** Use the **ospfv3** command to enable an OSPFv3 process and enter OSPFv3 view.

Use the **undo ospfv3** command to disable an OSPFv3 process.

The system runs no OSPFv3 process by default.

**Related commands:** **router-id.**



*An OSPFv3 process can run normally only when Router ID is configured in OSPFv3 view. Otherwise, you can find the process, but which cannot generate any LSA.*

**Examples** # Enable the OSPFv3 process with process ID as 120 and configure the Router ID as 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] router-id 1.1.1.1
```

## ospfv3 area

**Syntax** **ospfv3** *process-id* **area** *area-id* [ **instance** *instance-id* ]

**undo ospfv3** *process-id* **area** *area-id* [ **instance** *instance-id* ]

**View** Interface view

**Parameters** *process-id*: OSPFv3 process ID, in the range 1 to 65535.

*area-id*: Area ID, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

*instance-id*: Instance ID of an interface, in the range 0 to 255. The default is 0.

**Description** Use the **ospfv3 area** command to enable an OSPFv3 process on the interface and specify the area for the process.

Use the **undo ospfv3 area** command to disable an OSPFv3 process.

OSPFv3 is not enabled on an interface by default.

**Examples** # Enable OSPFv3 process 1 on an interface that belongs to instance 1 and specify area 1 for the process.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 1 area 1 instance 1
```

## ospfv3 cost

**Syntax** **ospfv3 cost** *value* [ **instance** *instance-id* ]

**undo ospfv3 cost** [ **instance** *instance-id* ]

**View** Interface view

**Parameters** *value*: OSPFv3 cost of the interface, in the range 1 to 65535.

*instance-id*: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

**Description** Use the **ospfv3 cost** command to configure the OSPFv3 cost of the interface in an instance.

Use the **undo ospfv3 cost** command to restore the default OSPFv3 cost of the interface in an instance.

By default, the OSPFv3 cost of the interface in an instance is 1.

**Examples** # Specifies the OSPFv3 cost of the interface in instance 1 as 33.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 cost 33 instance 1
```

## ospfv3 dr-priority

**Syntax** **ospfv3 dr-priority** *priority* [ **instance** *instance-id* ]

**undo ospfv3 dr-priority** [ **instance** *instance-id* ]

**View** Interface view

**Parameters** *priority*: DR priority, in the range 0 to 255.

*instance-id*: ID of the instance an interface belongs to, in the range 0 to 255, which defaults to 0.

**Description** Use the **ospfv3 dr-priority** command to set the DR priority for an interface in an instance.

Use the **undo ospfv3 dr-priority** command to restore the default value.

The DR priority on an interface defaults to 1.

An interface's DR priority determines its privilege in DR/BDR selection, and the interface with the highest priority is preferred.

**Examples** # Set the DR priority for an interface in instance 1 to 8.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 dr-priority 8 instance 1
```

## ospfv3 mtu-ignore

**Syntax** **ospfv3 mtu-ignore** [ **instance** *instance-id* ]

**undo ospfv3 mtu-ignore** [ **instance** *instance-id* ]

**View** Interface view

- Parameters** *instance-id*: Instance ID, in the range 0 to 255, which defaults to 0.
- Description** Use the **ospfv3 mtu-ignore** command to configure an interface to ignore MTU when sending DD packets.
- Use the **undo ospfv3 mtu-ignore** command to restore the default configuration.
- MTU is not ignored by default.
- Examples** # Configure VLAN-interface 10 that belongs to instance 1 to ignore MTU.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 mtu-ignore instance 1
```

ospfv3 timer dead

Syntax **ospfv3 timer dead** *seconds* [**instance** *instance-id*]
undo ospfv3 timer dead [**instance** *instance-id*]

View Interface view

Parameters *seconds*: Dead time in seconds, ranging from 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description Use the **ospfv3 timer dead** command to configure the OSPFv3 neighbor dead time for an interface that belongs to a specified instance.

Use the **undo ospfv3 timer dead** command to restore the default.

By default, the OSPFv3 neighbor dead time is 40 seconds.

OSPFv3 neighbor dead time: if an interface receives no hello packet from a neighbor after dead time elapses, the interface will consider the neighbor dead.

The **dead seconds** value is at least four times the **Hello seconds** value and must be identical on interfaces attached to the same network segment.

Related commands: **ospfv3 timer hello**.

Examples # Configure the OSPFv3 neighbor dead time as 80 seconds for VLAN-interface 10 in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer dead 80 instance 1
```

ospfv3 timer hello

Syntax **ospfv3 timer hello** *seconds* [**instance** *instance-id*]

undo ospfv3 timer hello [**instance** *instance-id*]

View Interface view

Parameters *seconds*: Interval between hello packets, ranging from 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description Use the **ospfv3 timer hello** command to configure the hello interval for an interface that belongs to an instance.

Use the **undo ospfv3 timer hello** command to restore the default.

By default, the hello interval is 10 seconds.

Related commands: **ospfv3 timer dead**.

Examples # Configure the hello interval as 20 seconds for VLAN-interface 10 in instance 1.

```
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] ospfv3 timer hello 20 instance 1
```

ospfv3 timer retransmit

Syntax **ospfv3 timer retransmit** *interval* [**instance** *instance-id*]

undo ospfv3 timer retransmit [**instance** *instance-id*]

View Interface view

Parameters *interval*: LSA retransmission interval in seconds, ranging from 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description Use the **ospfv3 timer retransmit** command to configure the LSA retransmission interval for an interface in an instance.

Use the **undo ospfv3 timer retransmit** command to restore the default.

The interval defaults to 5 seconds.

After sending a LSA to its neighbor, the device waits for an acknowledgement. If receiving no acknowledgement after the LSA retransmission interval elapses, it will retransmit the LSA.

The LSA retransmission interval should not be too small for avoidance of unnecessary retransmissions.

Examples # Configure the LSA retransmission interval on VLAN-interface 10 in instance 1 as 12 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer retransmit 12 instance 1
```

ospfv3 trans-delay

Syntax **ospfv3 trans-delay** *seconds* [**instance** *instance-id*]

undo ospfv3 trans-delay [**instance** *instance-id*]

View Interface view

Parameters *seconds*: Transmission delay in seconds, ranging from 1 to 3600.

instance-id: Instance ID of an interface, in the range of 0 to 255, with the default as 0.

Description Use the **ospfv3 trans-delay** command to configure the transmission delay for an interface with an instance ID.

Use the **undo ospfv3 trans-delay** command to restore the default.

The transmission delay defaults to 1s.

As LSAs are aged in the LSDB (incremented by 1 every second) but not aged on transmission, it is necessary to add a delay time to the age time before sending a LSA. This configuration is important for low-speed networks.

Examples # Configure the transmission delay as 3 seconds for VLAN-interface 10 in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 trans-delay 3 instance 1
```

preference

Syntax **preference** [**ase**] [**route-policy** *route-policy-name*] *preference*

undo preference [**ase**]

View OSPFv3 view

Parameters **ase**: Applies the preference to OSPFv3 external routes. If the keyword is not specified, the preference applies to OSPFv3 internal routes.

route-policy *route-policy-name*: References a routing policy to set preference for specific routes. The name is a string of 1 to 19 characters.

Preference: Preference of OSPFv3, in the range 1 to 255.

Description Use the **preference** command to specify a preference for OSPFv3 routes.

Use the **undo preference** command to restore the default.

By default, the preference for OSPFv3 internal routes is 10, and that for OSPFv3 external routes is 150.

The smaller the value is, the higher the preference is.

A router may run multiple routing protocols. Each protocol has a preference. When several routing protocols find multiple routes to the same destination, the route found by the protocol with the highest preference is selected.

Examples # Set a preference of 150 for OSPFv3 routes.

```
<Sysname> system-view
[Sysname] OSPFv3
[Sysname-OSPFv3-1] preference 150
```

router-id

Syntax **router-id** *router-id*

undo router-id

View OSPFv3 view

Parameters *router-id*: 32-bit router ID, in IPv4 address format.

Description Use the **router-id** command to configure the OSPFv3 router ID.

Use the **undo router-id** command to remove a configured router ID.

Router ID is the unique identifier of a device running an OSPFv3 process in the autonomous system. The OSPFv3 process cannot run without a Router ID.

Make sure that different processes have different Router IDs.

Related commands: **ospfv3**.



By configuring different router IDs for different processes, you can run multiple OSPFv3 processes on a router.

Examples # Configure the Router ID as 10.1.1.3 for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] router-id 10.1.1.3
```

silent-interface

Syntax **silent-interface** { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

View OSPFv3 view

Parameters *interface-type interface-number*: Interface type and number

all: Specifies all interfaces.

Description Use the **silent-interface** command to disable the specified interface from sending OSPFv3 packets.

Use the **undo silent-interface** command to restore the default.

An interface is able to send OSPFv3 packets by default.

Multiple processes can disable the same interface from sending OSPFv3 packets, but use of the **silent-interface** command takes effect only on interfaces enabled with the current process.

Examples # Disable VLAN-interface 10 from sending OSPFv3 packets in OSPFv3 processes 100 and 200.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] router-id 10.110.1.9
[Sysname-ospfv3-100] silent-interface vlan-interface 10
[Sysname-ospfv3-100] quit
[Sysname] ospfv3 200
[Sysname-ospfv3-200] router-id 20.18.0.7
[Sysname-ospfv3-200] silent-interface vlan-interface 10
```

spf timers

Syntax **spf timers** *delay-interval hold-interval*

undo spf timers

View OSPFv3 view

- Parameters** *delay-interval*: Interval in seconds between when OSPFv3 receives a topology change and when it starts SPF calculation. in the range 1 to 65535.
- hold-interval*: Hold interval in seconds between two consecutive SPF calculations, in the range 1 to 65535.
- Description** Use the **spf timers** command to configure the delay interval and hold interval for OSPFv3 SPF calculation.
- Use the **undo spf timers** command to restore the default.
- The delay interval and hold interval default to 5s and 10s.
- An OSPFv3 router works out a shortest path tree with itself as root based on the LSDB, and decides on the next hop to a destination network according the tree. Adjusting the SPF calculation interval can restrain bandwidth and router resource from over consumption due to frequent network changes.
- Examples** # Configure the delay interval and hold interval as 6 seconds for SPF calculation.
- ```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] spf timers 6 6
```

## stub

- Syntax** **stub** [ **no-summary** ]
- undo stub**
- View** OSPFv3 area view
- Parameters** **no-summary**: This argument is only applicable to the ABR of a stub area. With it configured, the ABR advertises only a default route in a Summary-LSA to the stub area (such an area is called a totally stub area).
- Description** Use the **stub** command to configure an area as a stub area.
- Use the **undo stub** command to remove the configuration.
- By default, an area is not configured as a stub area.
- When an area is configured as a stub area, all the routers attached to the area must be configured with the **stub** command.
- Related commands:** **default-cost.**
- Examples** # Configure OSPFv3 area 1 as a stub area.
- ```
<Sysname> system-view
[Sysname] ospfv3 1
```

```
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
```

vlink-peer

Syntax **vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **instance** *instance-id*] *

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead**]*

View OSPFv3 area view

Parameters *router-id*: Router ID for a virtual link neighbor.

hello *seconds*: Specifies the interval in seconds for sending Hello packets, ranging from 1 to 8192, with the default as 10. This value must be equal to the **hello** *seconds* configured on the virtual link peer.

retransmit *seconds*: Specifies the interval in seconds for retransmitting LSA packets, ranging from 1 to 3600, with the default as 5.

trans-delay *seconds*: Specifies the delay interval in seconds for sending LSA packets, ranging from 1 to 3600, with the default as 1.

dead *seconds*: Specifies the neighbor dead time in seconds, ranging from 1 to 32768, with the default as 40. This value must be equal to the **dead** *seconds* configured on the virtual link peer, and at least four times the value of **hello** *seconds*.

instance *Instance-id*: Instance ID of an virtual link, in the range of 0 to 255, with the default as 0.

Description Use the **vlink-peer** command to create and configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

For a non-backbone area without a direct connection to the backbone area or for a backbone area that cannot maintain connectivity, you can use the **vlink-peer** command to create logical links. A virtual link can be considered as an interface with OSPFv3 enabled, because parameters such as **hello**, **dead**, **retransmit** and **trans-delay** are configured in the similar way.

Both ends of a virtual link are ABRs that are configured with the **vlink-peer** command.

Examples # Create a virtual link to 10.110.0.3.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 10.0.0.0
[Sysname-ospfv3-1-area-10.0.0.0] vlink-peer 10.110.0.3
```


32

IPv6 IS-IS CONFIGURATION COMMANDS



- IPv6 IS-IS supports all the features of IPv4 IS-IS except that it advertises IPv6 routing information instead. This document describes only IPv6 IS-IS exclusive commands. Refer to “IS-IS Configuration Commands” on page 347.
- At present, the 0231A92P modules in the S7900E do not support IPv6.

display isis route ipv6

Syntax `display isis route ipv6 [[level-1 | level-2] | verbose]* [process-id]`

View Any view

Parameters **verbose**: Displays detailed IPv6 IS-IS routing information.

process-id: IS-IS process ID, in the range 1 to 65535.

level-1: Display Level-1 IPv6 IS-IS routes only.

level-2: Displays Level-2 IPv6 IS-IS routes only.



If no level is specified, both Level-1 and Level-2 (namely Level-1-2) routing information will be displayed.

Description Use the **display isis route ipv6** command to display IPv6 IS-IS routing information.

Examples # Display IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6
```

```
                Route information for ISIS(1)
                -----
                ISIS(1) IPv6 Level-1 Forwarding Table
                -----
Destination: 2001::                                PrefixLen: 64
Flag        : R/L/-                                Cost       : 10
Next Hop    : Direct                               Interface: Vlan100
Destination: 2002::                                PrefixLen: 64
Flag        : R/L/-                                Cost       : 20
Next Hop    : FE80::20F:E2FF:FE1D:A65B            Interface: Vlan100
                Flags: R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 127 Field descriptions of the display isis route ipv6 command

| Field | Description |
|-------------|--|
| Destination | IPv6 destination address prefix |
| PrefixLen | Length of the prefix |
| Flag/Flags | Flag of routing information status
D: This is a direct route.
R: The route has been added into the routing table.
L: The route has been advertised in an LSP.
U: Route leaking flag, indicating the Level-1 route is from Level-2. "UP" means the route will not be returned to Level-2. |
| Cost | Value of cost |
| Next Hop | Next hop |
| Interface | Outbound interface |

Display detailed IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6 verbose
                    Route information for ISIS(1)
                    -----
                    ISIS(1) IPv6 Level-1 Forwarding Table
                    -----
IPV6 Dest : 2001:1::/64          Cost : 10      Flag : R/L/-
Preference : 15                  Admin Tag : -
Interface : Vlan100             Next Hop : Direct
IPV6 Dest : 2001:2::/64          Cost : 20      Flag : R/-/-
Preference : 15                  Admin Tag : -
Interface : Vlan100             Next Hop : FE80::2E0:FCFF:FE00:242A
IPV6 Dest : 2001:3::/64          Cost : 20      Flag : R/-/-
Preference : 15                  Admin Tag : -
Interface : Vlan100             Next Hop : FE80::2E0:FCFF:FE00:242A
IPV6 Dest : ::/0                 Cost : 10      Flag : R/-/-
Preference : 15                  Admin Tag : -
Interface : Vlan100             Next Hop : FE80::2E0:FCFF:FE00:242A
Flags: R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 128 Field descriptions of the display isis route ipv6 verbose command

| Field | Description |
|------------|--|
| IPV6 Dest | IPv6 destination address |
| Cost | Value of cost |
| Flag/Flags | Flag of routing information status
D: This is a direct route.
R: The route has been added into the routing table.
L: The route has been advertised in an LSP.
U: Route leaking flag, indicating the Level-1 route is from Level-2. "UP" means the route will not be returned to Level-2. |
| Admin Tag | Administrative tag |
| Src Count | Number of advertisement sources |
| Next Hop | Next hop |
| Interface | Outbound interface |

ipv6 default-route-advertise

Syntax **ipv6 default-route-advertise** [[**level-1** | **level-2** | **level-1-2**] | **route-policy** *route-policy-name*]*

undo ipv6 default-route-advertise [**route-policy** *route-policy-name*]

View IS-IS view

Parameters *route-policy-name*: Specifies the name of a routing policy with a string of 1 to 19 characters.

level-1: Specifies the default route as Level-1.

level-2: Specifies the default route as Level-2.

level-1-2: Specifies the default route as Level-1-2.



If no level is specified, the default route belongs to Level-2.

Description Use the **ipv6 default-route-advertise** command to generate a Level-1 or Level-2 IPv6 IS-IS default route.

Use the **undo ipv6 default-route-advertise** command to disable generating a default route.

No IPv6 IS-IS default route is generated by default.

With a routing policy, you can configure IPv6 IS-IS to generate the default route that must match the routing policy. You can use the **apply isis level-1** command in routing policy view to generate a default route in L1 LSPs, or use the **apply isis level-2** command in routing policy view to generate a default route in L2 LSPs, and use the **apply isis level-1-2** in routing policy view to generate a default route in L1 and L2 LSPs respectively.

Examples # Configure the router to generate a default route in Level-2 LSPs.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 default-route-advertise
```

ipv6 enable

Syntax **ipv6 enable**

undo ipv6 enable

View IS-IS view

Parameters None

Description Use the **ipv6 enable** command to enable IPv6 for the IPv6 IS-IS process.

Use the **undo ipv6 enable** command to disable IPv6.

IPv6 is disabled by default.

Examples # Create IS-IS routing process 1, and enable IPv6 for the process.

```
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] ipv6 enable
```

ipv6 filter-policy export

Syntax **ipv6 filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* *process-id*]

undo ipv6 filter-policy export [*protocol* [*process-id*]]

View IS-IS view

Parameters *acl6-number*: Number of a basic or advanced IPv6 ACL used to filter redistributed routes before advertisement, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter the redistributed routes before advertisement, a string of 1 to 19 characters.

route-policy-name: Name of a routing policy used to filter the redistributed routes before advertisement, a string of 1 to 19 characters.

protocol: Filter routes redistributed from the specified routing protocol before advertisement. The routing protocol can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng** or **static** at present. If no protocol is specified, routes redistributed from all protocols are filtered before advertisement.

process-id: Process ID of the routing protocol, ranging from 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3** or **ripng**.

Description Use the **ipv6 filter-policy export** command to configure IPv6 IS-IS to filter redistributed routes before advertisement.

Use the **undo ipv6 filter-policy export** command to disable the filtering.

The filtering is disabled by default.

In some cases, only routes satisfying certain conditions will be advertised. You can configure the filtering conditions using the **ipv6 filter-policy** command.

You can use the **ipv6 filter-policy export** command, which filters redistributed routes only when they are advertised to other routers, in combination with the **ipv6 import-route** command.

- If no protocol is specified, routes redistributed from all protocols are filtered before advertisement.
- If a protocol is specified, only routes redistributed from the protocol are filtered before advertisement.

Related commands: **ipv6 filter-policy import.**

Examples # Reference the ACL6 2006 to filter all the redistributed routes before advertisement.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 filter-policy 2006 export
```

ipv6 filter-policy import

Syntax **ipv6 filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo ipv6 filter-policy import

View IS-IS view

Parameters *acl6-number*: Number of a basic or advanced IPv6 ACL used to filter incoming routes, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter incoming routes, a string of 1 to 19 characters.

route-policy-name: Name of a routing policy used to filter incoming routes, a string of 1 to 19 characters.

Description Use the **ipv6 filter-policy import** command to configure IPv6 IS-IS to filter the received routes.

Use the **undo ipv6 filter-policy import** command to disable the filtering.

The filtering is disabled by default.

In some cases, only the routing information satisfying certain conditions will be received. You can configure the filtering conditions using the **ipv6 filter-policy** command.

Related commands: **ipv6 filter-policy export.**

Examples # Reference the IPv6 ACL 2003 to filter the received routes.

```

<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 filter-policy 2003 import

```

ipv6 import-route

Syntax **ipv6 import-route** *protocol* [*process-id*] [**allow-ibgp**] [**cost** *cost* | [**level-1** | **level-2** | **level-1-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo ipv6 import-route *protocol* [*process-id*]

View IS-IS view

Parameters *protocol*: Redistributes routes from a specified routing protocol, which can be **direct**, **static**, **ripng**, **isisv6**, **bgp4+** or **ospfv3**.

process-id: Process ID of the routing protocol of **ripng**, **isisv6** or **ospfv3**, in the range of 1 to 65535. The default is 1.

cost: Cost for redistributed routes, ranging from 0 to 4261412864.

level-1: Redistributes routes into Level-1 routing table.

level-2: Redistributes routes into Level-2 routing table.

level-1-2: Redistributes routes into Level-1 and Level-2 routing tables.

route-policy-name: Name of a routing policy used to filter routes when they are being redistributed, a string of 1 to 19 characters.

tag: Specifies a administrative tag number for the redistributed routes, in the range of 1 to 4294967295.

allow-ibgp: Allows the redistribution of IBGP routes. This keyword is optional when the *protocol* is **bgp4+**.

Description Use the **ipv6 import-route** command to enable IPv6 IS-IS to redistribute routes from another routing protocol.

Use the **undo ipv6 import-route** command to disable route redistribution.

Route redistribution is disabled by default.

If no level is specified, the routes are imported to Level-2 routing table by default.

IPv6 IS-IS considers redistributed routes as routes to destinations outside the local routing domain.

You can specify a cost and a level for redistributed routes.



CAUTION: Using the **import-route bgp4+ allow-ibgp** command will redistribute both EBGP and IBGP routes. The redistributed IBGP routes may cause routing loops. Therefore, be cautious with this command.

Examples # Configure IPv6-IS-IS to redistribute static routes and sets the cost 15 for them.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]ipv6 import-route static cost 15
```

ipv6 import-route isisv6 level-2 into level-1

Syntax **ipv6 import-route isisv6 level-2 into level-1** [**filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag*]*

undo ipv6 import-route isisv6 level-2 into level-1

View IS-IS view

Parameters *acl6-number*: Number of a basic or advanced ACL6 used to filter routes when they are leaking from Level-2 to Level-1, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter routes when they are leaking from Level-2 to Level-1, a string of 1 to 19 characters.

route-policy-name: Name of a routing policy used to filter routes when they are leaking from Level-2 to Level-1, a string of 1 to 19 characters.

tag: Specifies a administrative tag number for the leaked routes, in the range of 1 to 4294967295.

Description Use the **ipv6 import-route isisv6 level-2 into level-1** to enable IPv6 IS-IS route leaking from Level-2 to Level-1.

Use the **undo ipv6 import-route isisv6 level-2 into level-1** command to disable the leaking.

The leaking is disabled by default.

The route leaking feature enables a Level-1-2 router to advertise routes destined to the Level-2 area and other Level-1 areas to the Level-1 and Level-1-2 routers in the local area.

Examples # Enable IPv6 IS-IS route leaking from Level-2 to Level-1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ipv6 import-route isisv6 level-2 into level-1
```

ipv6 maximum load-balancing

Syntax **ipv6 maximum load-balancing** *number*

undo ipv6 maximum load-balancing

View IS-IS view

Parameters *number*: Maximum number of equal-cost routes for load balancing. Its value is in the range 1 to 4 and defaults to 4.

Description Use the **ipv6 maximum load-balancing** command to configure the maximum number of equal-cost routes for load balancing.

Use the **undo ipv6 maximum load-balancing** command to restore the default.

The maximum number range and default vary by device.



Configure the maximum number of equivalent load-balanced routes according to the memory capacity.

Examples # Configure the maximum number of equivalent load-balanced routing as 2.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] ipv6 maximum load-balancing 2
```

ipv6 preference

Syntax **ipv6 preference** { **route-policy** *route-policy-name* | *preference* } *

undo ipv6 preference

View IS-IS view

Parameters *preference*: Preference for IPv6 IS-IS, ranging from 1 to 255.

route-policy-name: Name of a routing policy, a string of 1 to 19 characters.

Description Use the **ipv6 preference** command to configure the preference for IPv6 IS-IS protocol.

Use the **undo ipv6 preference** command to configure the default preference for IPv6 IS-IS protocol.

The default preference is 15.

When a router runs multiple dynamic routing protocols at the same time, the system will assign a preference to each routing protocol. If several protocols find routes to the same destination, the route found by the protocol with the highest preference is selected.

Examples # Configure the preference of IPv6 IS-IS protocol as 20.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 preference 20
```

ipv6 summary

Syntax `ipv6 summary ipv6-prefix prefix-length [avoid-feedback | generate_null0_route | [level-1 | level-1-2 | level-2] | tag tag] *`
`undo ipv6 summary ipv6-prefix prefix-length [level-1 | level-1-2 | level-2]`

View IS-IS view

Parameters *ipv6-prefix*: IPv6 prefix of the summary route.

prefix-length: Length of the IPv6 prefix, in the range of 0 to 128.

avoid-feedback: Specifies to avoid learning summary routes via routing calculation.

generate_null0_route: Generates the NULL 0 route to avoid routing loops.

level-1: Specifies to summarize only the routes redistributed to Level-1 area.

level-1-2: Specifies to summarize all the routes redistributed to Level-1 and Level-2 areas.

level-2: Specifies to summarize only the routes redistributed to Level-2 area.

tag: Value of a administrative tag, in the range of 1 to 4294967295.



*If no level is specified in the command, the default is **level-2**.*

Description Use the **ipv6 summary** command to configure an IPv6 IS-IS summary route.

Use the **undo ipv6 summary** command to remove the summary route.

Route summarization is disabled by default.

Configuring summary routes can reduce the size of the route table, LSPs and LSDB. Routes to be summarized can be IS-IS routes or redistributed routes. The cost of a summary route is the smallest cost among all summarized routes.

Examples # Configure a summary route of 2002::/32.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 summary 2002:: 32
```

isis ipv6 enable

Syntax `isis ipv6 enable [process-id]`

`undo isis ipv6 enable`

View Interface view

Parameters *process-id*: IS-IS process ID, ranging from 1 to 65535. The default is 1.

Description Use the **isis ipv6 enable** command to enable IPv6 for the specified IS-IS process on the interface.

Use the **undo isis ipv6 enable** command to disable the configuration.

IPv6 is disabled on the interface by default.

Examples # Enable global IPv6, create IS-IS routing process 1, enable IPv6 for the process, and enable IPv6 for the process on VLAN-interface100.

```
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] ipv6 enable
[Sysname-isis-1] quit
[Sysname] interface Vlan-interface 100
[Sysname--Vlan-interface100] ipv6 address 2002::1/64
[Sysname--Vlan-interface100] isis ipv6 enable 1
```

33

IPv6 BGP CONFIGURATION COMMANDS



At present, the 0231A92P modules in the S7900E do not support IPv6.

balance

Syntax **balance** *number*

undo balance

View IPv6 address family view

Parameters *number*: Number of BGP4+ routes participating in load balancing. Its value is in the range 1 to 4. When it is set to 1, load balancing is disabled.

Description Use the **balance** command to configure the number of routes participating in IPv6 BGP load balancing.

Use the **undo balance** command to restore the default.

The feature is not available by default.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by defining its routing rule.

Examples # Set the number of routes participating in IPv6 BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] balance 2
```

bestroute as-path-neglect

Syntax **bestroute as-path-neglect**

undo bestroute as-path-neglect

View IPv6 address family view

Parameters None

Description Use the **bestroute as-path-neglect** command to configure the IPv6 BGP router to not evaluate the AS_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure the IPv6 BGP router to use the AS_PATH during best route selection.

By default, the router takes AS_PATH as a factor when selecting the best route.

Examples # Ignore AS_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute as-path-neglect
```

bestroute compare-med

Syntax **bestroute compare-med**

undo bestroute compare-med

View IPv6 address family view

Parameters None

Description Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.



CAUTION: After the **bestroute compare-med** command is executed, the **balance** command does not take effect.

Examples # Compare the MED for paths from an AS for selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute compare-med
```

bestroute med-confederation

Syntax **bestroute med-confederation**

undo bestroute med-confederation

View IPv6 address family view

- Parameters** None
- Description** Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers for best route selection.
- Use the **undo bestroute med-confederation** command to disable the comparison.
- By default, this comparison is not enabled.
- With this feature enabled, the system can only compare the MED for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.
- Examples** # Compare the MED for paths from peers within the confederation.
- ```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute med-confederation
```

## compare-different-as-med

- Syntax** **compare-different-as-med**
- undo compare-different-as-med**
- View** IPv6 address family view
- Parameters** None
- Description** Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.
- Use the **undo compare-different-as-med** command to disable the comparison.
- The comparison is disabled by default.
- If there are several paths available for one destination, the path with the smallest MED value is selected.
- Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.
- Examples** # Enable to compare the MED for paths from peers in different ASs.
- ```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] compare-different-as-med
```

dampening

Syntax **dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View IPv6 address family view

Parameters *half-life-reachable*: Half-life for reachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Half-life for unreachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Reuse threshold value for suppressed routes, in the range 1 to 20000. Penalty value of a suppressed route decreasing under the value is reused. By default, its value is 750.

suppress: Suppression threshold from 1 to 20000, which should be bigger than the *reuse* value. Routes with a penalty value bigger than the threshold are suppressed. By default, it is 2000.

ceiling: Ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

half-life-reachable, *half-life-unreachable*, *reuse*, *suppress* and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

Description Use the **dampening** command to enable IPv6 BGP route dampening or/and configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

Related commands: **reset bgp ipv6 dampening**, **reset bgp ipv6 flap-info**, **display bgp ipv6 routing-table dampened**, **display bgp ipv6 routing-table dampening parameter**, **display bgp ipv6 routing-table flap-info**.

Examples # Enable IPv6 BGP route dampening and configure route dampening parameters.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] dampening 10 10 1000 2000 3000
```

default local-preference

Syntax **default local-preference** *value*

undo default local-preference

View IPv6 address family view

Parameters *value*: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

Description Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default value.

By default, the default local preference is 100.

Use this command to affect IPv6 BGP route selection.

Examples # Two devices A and B in the same AS are connected to another AS. Change the local preference of B from default value 100 to 180, making the route passing B preferred.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default local-preference 180
```

default med

Syntax **default med** *med-value*

undo default med

View IPv6 address family view

Parameters *med-value*: MED value, in the range 0 to 4294967295.

Description Use the **default med** command to specify the default MED value.

Use the **undo default med** command to restore the default.

By default, the default *med-value* is 0.

The multi-exit discriminator (MED) is an external metric of a route. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with the identical destination and different next-hops from various external peers, it will select the best route depending on the MED

value. In the case that all other conditions are the same, the system first selects the route with the smaller MED value as the best route for the autonomous system.

Examples # Devices A and B belong to AS100 and device C belongs to AS200. C is the peer of A and B. Configure the MED of A as 25 to make C select the path from B.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default med 25
```

default-route imported

Syntax **default-route imported**
undo default-route imported

View IPv6 address family view

Parameters None

Description Use the **default-route imported** command to enable the redistribution of default route into the IPv6 BGP routing table.

Use the **undo default-route imported** command to disable the redistribution.

By default, the redistribution is not enabled.

Examples # Enable the redistribution of default route from OSPFv3 into IPv6 BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default-route imported
[Sysname-bgp-af-ipv6] import-route ospfv3 1
```

display bgp ipv6 group

Syntax **display bgp ipv6 group** [*ipv6-group-name*]

View Any view

Parameters *ipv6-group-name*: Peer group name, a string of 1 to 47 characters.

Description Use the **display bgp ipv6 group** command to display IPv6 peer group information.

If no *ipv6-group-name* is specified, information about all peer groups is displayed.

Examples # Display the information of the IPv6 peer group **aaa**.

```

<Sysname> display bgp ipv6 group aaa

BGP peer-group is aaa
remote AS number not specified
Type : external
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Peer Preferred Value: 0
No routing policy is configured
Members:
Peer      V    AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
20:20::20:1  4    200      170      141      0        2 02:13:35 Established

```

Table 129 Field descriptions of the display bgp ipv6 group command

| Field | Description |
|---|--|
| BGP peer-group | Name of the peer group |
| remote AS | AS number of the peer group |
| Type | Type of the peer group |
| Maximum allowed prefix number | Maximum allowed prefix number |
| Threshold | Threshold value |
| hold timer value | Holdtime |
| Keepalive timer value | Keepalive interval |
| Minimum time between advertisement runs | Minimum interval between advertisements |
| Peer Preferred Value | Preferred value of the routes from the peer |
| No routing policy is configured | No routing policy is configured for the peer |
| Members | Group members |
| Peer | IPv6 address of the peer |
| V | Peer BGP version |
| AS | AS number |
| MsgRcvd | Number of messages received |
| MsgSent | Number of messages sent |
| OutQ | Number of messages to be sent |
| PrefRcv | Number of prefixes received |
| Up/Down | The lasting time of a session/the lasting time of present state (when no session is established) |
| State | State machine of peer |

display bgp ipv6 network**Syntax** display bgp ipv6 network**View** Any view**Parameters** None

Description Use the **display bgp ipv6 network** command to display IPv6 routes advertised with the **network** command.

Examples # Display IPv6 routes advertised with the **network** command.

```
<Sysname> display bgp ipv6 network
  BGP Local Router ID is 1.1.1.2.
  Local AS Number is 200.
  Network          Mask          Route-policy      Short-cut
  2002::          64
  2001::          64                      Short-cut
```

Table 130 Field descriptions of the display bgp ipv6 network command

| Field | Description |
|---------------------|---------------------|
| BGP Local Router ID | BGP Local Router ID |
| Local AS Number | Local AS Number |
| Network | Network address |
| Prefix | Prefix length |
| Route-policy | Routing policy |
| Short-cut | Shortcut route |

display bgp ipv6 paths

Syntax **display bgp ipv6 paths** [*as-regular-expression*]

View Any view

Parameters *as-regular-expression*: AS path regular expression.

Description Use the **display bgp ipv6 paths** command to display IPv6 BGP path information.

If no parameter is specified, all path information will be displayed.

Examples # Display IPv6 BGP path information.

```
<Sysname> display bgp ipv6 paths

  Address      Hash    Refcount  MED      Path/Origin
  0x5917098    1       1         0        i
  0x59171D0    9       2         0        100i
```

Table 131 Field descriptions of the display bgp ipv6 paths command

| Field | Description |
|----------|---|
| Address | Route destination address in local database, in dotted hexadecimal notation |
| Hash | Hash index |
| Refcount | Count of routes that used the path |
| MED | MED of the path |

Table 131 Field descriptions of the display bgp ipv6 paths command

| Field | Description |
|--------|---|
| Path | AS_PATH attribute of the path, recording the ASs it has passed, for avoiding routing loops |
| Origin | Origin attribute of the route, which can take on one of the following values: <ul style="list-style-type: none"> i Indicates the route is interior to the AS.
Summary routes and routes defined using the network command are considered IGP routes. e Indicates that a route is learned from the exterior gateway protocol (EGP). ? Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE. |

display bgp ipv6 peer

Syntax **display bgp ipv6 peer** [*ipv6-group-name* **log-info** | *ipv6-address* { **log-info** | **verbose** } | **verbose**]

View Any view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

ipv6-address: Specifies the IPv6 address of a peer to be displayed.

log-info: Displays log information of the specified peer.

verbose: Displays the detailed information of the peer.

Description Use the **display bgp ipv6 peer** command to display peer/peer group information.

If no parameter specified, information about all peers and peer groups is displayed.

Examples # Display all IPv6 peer information.

```
<Sysname> display bgp ipv6 peer

  BGP Local router ID : 20.0.0.1
  local AS number : 100
  Total number of peers : 1                Peers in established state : 1

Peer      V   AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down    State
-----
20::21   4   200    17       19       0         3  00:09:59  Established
```

Table 132 Field descriptions of the display bgp ipv6 peer command

| Field | Description |
|-------|--------------------------|
| Peer | IPv6 address of the peer |

Table 132 Field descriptions of the display bgp ipv6 peer command

| Field | Description |
|---------|--|
| V | Peer BGP version |
| AS | AS number |
| MsgRcvd | Messages received |
| MsgSent | Messages sent |
| OutQ | Messages to be sent |
| PrefRcv | Number of prefixes received |
| Up/Down | The lasting time of a session/the lasting time of present state (when no session is established) |
| State | Peer state |

display bgp ipv6 routing-table

Syntax `display bgp ipv6 routing-table [ipv6-address prefix-length]`

View Any view

Parameters *ipv6-address*: Destination IPv6 address.

prefix-length: Prefix length of the IPv6 address, in the range 0 to 128.

Description Use the **display bgp ipv6 routing-table** command to display IPv6 BGP routing table information.

Examples # Display the IPv6 BGP routing table.

```
<Sysname> display bgp ipv6 routing-table

Total Number of Routes: 2

BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30::                               PrefixLen : 64
   NextHop : 30:30::30:1                           LocPrf    :
   PrefVal  : 0                                     Label     : NULL
   MED     : 0
   Path/Ogn: i

*> Network : 40:40::                               PrefixLen : 64
   NextHop : 40:40::40:1                           LocPrf    :
   PrefVal  : 0                                     Label     : NULL
   MED     : 0
   Path/Ogn: i
```

Table 133 Field descriptions of the display bgp ipv6 routing-table command

| Field | Description |
|-----------------|-----------------|
| Local router ID | Local router ID |

Table 133 Field descriptions of the display bgp ipv6 routing-table command

| Field | Description |
|--------------|--|
| Status codes | Status codes:
* - valid
> - best
d - damped
h - history
i - internal (IGP)
s - summary suppressed (suppressed)
S - Stale |
| Origin | i - IGP (originated in the AS)
e - EGP (learned through EGP)
? - incomplete (learned by other means) |
| Network | Destination network address |
| PrefixLen | Prefix length |
| NextHop | Next Hop |
| MED | MULTI_EXIT_DISC attribute |
| LocPrf | Local preference value |
| Path | AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops |
| PrefVal | Preferred value |
| Label | Label |
| Ogn | Origin attribute of the route, which can take on one of the following values:

i Indicates that a route is interior to the AS.
Summary routes and the routes configured using the network command are considered IGP routes.

e Indicates that a route is learned from the exterior gateway protocol (EGP).

? Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE. |

display bgp ipv6 routing-table as-path-acl

Syntax `display bgp ipv6 routing-table as-path-acl as-path-acl-number`

View Any view

Parameters *as-path-acl-number*: Number of an AS path ACL permitted by which to display routing information, ranging from 1 to 256.

Description Use the **display bgp ipv6 routing-table as-path-acl** command to display routes filtered through the specified AS path ACL.

Examples # Display routes filtered through the AS path ACL 20.

```

<Sysname> display bgp ipv6 routing-table as-path-acl 20
BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30::                               PrefixLen : 64
   NextHop : 30:30::30:1                             LocPrf   :
   PrefVal  : 0                                       Label    : NULL
   MED     : 0
   Path/Ogn: i

```

Refer to Table 133 for description on the fields above.

display bgp ipv6 routing-table community

Syntax `display bgp ipv6 routing-table community [aa:nn&<1-13>] [no-advertise | no-export | no-export-subconfed] * [whole-match]`

View Any view

Parameters *aa:nn*: Specifies a community number; both aa and nn are in the range 0 to 65535.

&<1-13>: Indicates the argument before it can be entered up to 13 times.

no-advertise: Displays routes not advertised to any peer.

no-export: Displays routes advertised outside the AS; if there is a confederation, it displays routes not advertised outside the confederation, but to other sub ASs in the confederation.

no-export-subconfed: Displays routes neither advertised outside the AS nor to other sub ASs if the confederation is configured.

whole-match: Displays the exactly matched routes.

Description Use the **display bgp ipv6 routing-table community** command to display the routing information of the specified community.

Examples # Display the routing information of the community no-export.

```

<Sysname> display bgp ipv6 routing-table community no-export
BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30::                               PrefixLen : 64
   NextHop : 30:30::30:1                             LocPrf   :
   PrefVal  : 0                                       Label    : NULL
   MED     : 0
   Path/Ogn: i

```

Refer to Table 133 for description on the fields above.

display bgp ipv6 routing-table community-list

- Syntax** `display bgp ipv6 routing-table community-list { basic-community-list-number [whole-match] | adv-community-list-number }&<1-16>`
- View** Any view
- Parameters** *basic-community-list-number*: Specifies a basic community-list number, in the range 1 to 99.
- adv-community-list-number*: Specifies an advanced community-list number, in the range 100 to 199.
- whole-match**: Displays routes exactly matching the specified *basic-community-list-number*.
- &<1-16>: Specifies to allow entering the argument before it up to 16 times.
- Description** Use the **display bgp ipv6 routing-table community-list** command to view the routing information matching the specified IPv6 BGP community list.
- Examples** # Display the routing information matching the specified IPv6 BGP community list.
- ```
<Sysname> display bgp ipv6 routing-table community-list 99
BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30:: PrefixLen : 64
 NextHop : 30:30::30:1 LocPrf :
 PrefVal : 0 Label : NULL
 MED : 0
 Path/Ogn: i
```
- Refer to Table 133 for description on the fields above.

---

## display bgp ipv6 routing-table dampened

- Syntax** `display bgp ipv6 routing-table dampened`
- View** Any view
- Parameters** None
- Description** Use the **display bgp ipv6 routing-table dampened** command to display the IPv6 BGP dampened routes.
- Examples** # Display IPv6 BGP dampened routes.
- ```
<Sysname> display bgp ipv6 routing-table dampened
```

```

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*d Network : 111::                                PrefixLen : 64
  From    : 122::1                                Reuse     : 00:29:34
  Path/Ogn: 200?

```

Table 134 Field descriptions of the display bgp ipv6 routing-table dampened command

| Field | Description |
|-------|------------------------------|
| From | Source IP address of a route |
| Reuse | Time for reuse |

Refer to Table 133 for description on the fields above.

display bgp ipv6 routing-table dampening parameter

Syntax `display bgp ipv6 routing-table dampening parameter`

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table dampening parameter** command to display IPv6 BGP routing dampening parameters.

Related commands: **dampening.**

Examples # Display IPv6 BGP routing dampening parameters.

```

<Sysname> display bgp ipv6 routing-table dampening parameter
Maximum Suppress Time(in second)      : 3069
Ceiling Value                          : 16000
Reuse Value                            : 750
HalfLife Time(in second)              : 900
Suppress-Limit                        : 2000

```

Table 135 Description on the above fields

| Field | Description |
|-----------------------|------------------------------|
| Maximum Suppress Time | Maximum Suppress Time |
| Ceiling Value | Upper limit of penalty value |
| Reuse Value | Reuse Value |
| HalfLife Time | Half life Time |
| Suppress-Limit | Suppress value |

display bgp ipv6 routing-table different-origin-as

Syntax `display bgp ipv6 routing-table different-origin-as`

| | |
|--------------------|--|
| View | Any view |
| Parameters | None |
| Description | Use the display bgp ipv6 routing-table different-origin-as command to display IPv6 BGP routes originating from different autonomous systems. |
| Examples | <pre># Display routes from different ASs. <Sysname> display bgp ipv6 routing-table different-origin-as BGP Local router ID is 2.2.2.2 Status codes: * - valid, > - best, d - damped, h - history, i - internal, s - suppressed, S - Stale Origin : i - IGP, e - EGP, ? - incomplete *> Network : 222:: PrefixLen : 64 NextHop : 122::2 LocPrf : PrefVal : 0 Label : NULL MED : 0 Path/Ogn: 100 ?</pre> <p>Refer to Table 133 for description on the fields above.</p> |

display bgp ipv6 routing-table flap-info

| | |
|--------------------|--|
| Syntax | display bgp ipv6 routing-table flap-info [regular-expression <i>as-regular-expression</i> as-path-acl <i>as-path-acl-number</i> <i>ipv6-address</i> [<i>prefix-length</i> [longer-match]]] |
| View | Any view |
| Parameters | <p><i>as-regular-expression</i>: AS path regular expression to be matched.</p> <p><i>as-path-acl-number</i>: Number of the specified AS path ACL to be matched, ranging from 1 to 256.</p> <p><i>ipv6-address</i>: IPv6 address of a route to be displayed.</p> <p><i>prefix-length</i>: Prefix length of the IPv6 address, in the range 0 to 128.</p> <p>longer-match: Matches the longest prefix.</p> |
| Description | Use the display bgp ipv6 routing-table flap-info command to display IPv6 BGP route flap statistics. |
| Examples | <pre># Display IPv6 BGP route flap statistics. <Sysname> display bgp ipv6 routing-table flap-info BGP Local router ID is 1.1.1.1 Status codes: * - valid, > - best, d - damped, h - history, i - internal, s - suppressed, S - Stale Origin : i - IGP, e - EGP, ? - incomplete</pre> |

```
*d Network : 111::
   From   : 122::1
   Duration : 00:13:47
   Path/Ogn : 200?
   PrefixLen : 64
   Flaps     : 3
   Reuse     : 00:16:36
```

Table 136 Field descriptions of the display bgp ipv6 routing-table flap-info command

| Field | Description |
|----------|-------------------------|
| Flaps | Number of flaps |
| Duration | Flap duration |
| Reuse | Reuse time of the route |

Refer to Table 133 for description on the fields above.

display bgp ipv6 routing-table peer

Syntax **display bgp ipv6 routing-table peer** *ipv6-address* { **advertised-routes** | **received-routes** } [*network-address prefix-length* | **statistic**]

View Any view

Parameters *ipv6-address*: Specifies the IPv6 peer to be displayed.

advertised-routes: Routing information advertised to the specified peer.

received-routes: Routing information received from the specified peer.

network-address prefix-length: IPv6 address and prefix length. The prefix length ranges from 0 to 128.

statistic: Displays route statistics.

Description Use the **display bgp ipv6 routing-table peer** command to display the routing information advertised to or received from the specified IPv6 BGP peer.

Examples # Display the routing information advertised to the specified BGP peer.

```
<Sysname> display bgp ipv6 routing-table peer 10:10::10:1 advertised-routes
Total Number of Routes: 2

BGP Local router ID is 20.20.20.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 20:20::
   NextHop : 20:20::20:1
   PrefVal  : 0
   MED     : 0
   Path/Ogn: i
   PrefixLen : 64
   LocPrf   :
   Label    : NULL

*> Network : 40:40::
   NextHop : 30:30::30:1
   PrefVal  : 0
   MED     : 0
   Path/Ogn: 300 i
   PrefixLen : 64
   LocPrf   :
   Label    : NULL
```

Refer to Table 133 for description on the fields above.

display bgp ipv6 routing-table regular-expression

Syntax **display bgp ipv6 routing-table regular-expression** *as-regular-expression*

View Any view

Parameters *as-regular-expression*: AS regular expression.

Description Use the **display bgp ipv6 routing-table regular-expression** command to display the routes permitted by the specified AS regular expression.

Examples # Display routing information matching the specified AS regular expression.

```
<Sysname> display bgp ipv6 routing-table regular-expression ^100
```

```
BGP Local router ID is 20.20.20.1
Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 50:50::                               PrefixLen : 64
   NextHop  : 10:10::10:1                           LocPrf    :
   PrefVal  : 0                                       Label     : NULL
   MED      : 0
   Path/Ogn: 100 i
```

Refer to Table 133 for description on the fields above.

display bgp ipv6 routing-table statistic

Syntax **display bgp ipv6 routing-table statistic**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table statistic** command to display IPv6 BGP routing statistics.

Examples # Display IPv6 BGP routing statistics.

```
<Sysname> display bgp ipv6 routing-table statistic
```

```
Total Number of Routes: 1
```

filter-policy export

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol process-id*]

undo filter-policy export [*protocol process-id*]

View IPv6 address family view

Parameters *acl6-number*: Specifies the number of an ACL6 used to match against the destination of routing information. The number is in the range 2000 to 3999.

ipv6-prefix-name: Specifies the name of an IPv6 prefix list used to match against the destination address field of routing information. The name is a string of 1 to 19 characters.

protocol: Filters routes redistributed from the routing protocol. It can be **direct**, **isisv6**, **ospfv3**, **ripng**, and **static** at present. If no protocol is specified, all routes will be filtered when advertised.

process-id: Process ID of the routing protocol, in the range 1 to 65535. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

Description Use the **filter-policy export** command to filter outbound routes using a specified filter.

Use the **undo filter-policy export** command to cancel filtering outbound routes.

By default, no outbound routing information is filtered.

If a protocol is specified, only routes redistributed from the specified protocol are filtered. If no protocol is specified, all redistributed routes will be filtered.

Examples # Reference ACL6 2001 to filter all outbound IPv6 BGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 export
```

filter-policy import

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View IPv6 address family view

- Parameters** *acl6-number*: Number of an IPv6 ACL used to match against the destination address field of routing information, ranging from 2000 to 3999.
- ipv6-prefix-name*: Name of an IPv6 prefix list used to match against the destination address field of routing information, a string of 1 to 19 characters.
- Description** Use the **filter-policy import** command to filter inbound routing information using a specified filter.
- Use the **undo filter-policy import** command to cancel filtering inbound routing information.
- By default, no inbound routing information is filtered.
- Examples** # Reference ACL6 2001 to filter all inbound routes.
- ```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 import
```

---

## group

- Syntax** **group** *ipv6-group-name* [ **internal** | **external** ]
- undo group** *ipv6-group-name*
- View** IPv6 address family view
- Parameters** *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.
- internal**: Creates an IBGP peer group.
- external**: Creates an EBGP peer group, which can be a group of another sub AS in the confederation.
- Description** Use the **group** command to create a peer group.
- Use the **undo group** command to delete a peer group.
- An IBGP peer group will be created if neither **internal** nor **external** is selected.
- Examples** # Create an IBGP peer group named **test**.
- ```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv6-family
[Sysname-bgp-af-ipv6] group test
```

import-route

Syntax **import-route** *protocol* [*process-id* [**med** *med-value* | **route-policy** *route-policy-name*] *]

undo import-route *protocol* [*process-id*]

View IPv6 address family view

Parameters *protocol*: Redistributes routes from the specified routing protocol, which can be **direct**, **isisv6**, **ospfv3**, **ripng**, or **static** at present.

process-id: Routing protocol process ID, in the range 1 to 65535 and with the default as 1. It is available only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

med-value: Applies the MED value to redistributed routes. The value is in the range 0 to 4294967295. If not specified, the cost of the redistributed route is used as its MED in the IPv6 BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes, a string of 1 to 19 characters.

Description Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to remove the configuration.

By default, IPv6 BGP does not redistribute routes from any routing protocol.

The routes redistributed using the **import-route** command has the incomplete origin attribute.

Examples # Redistribute routes from RIPng 1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] import-route ripng 1
```

ipv6-family

Syntax **ipv6-family**

undo ipv6-family

View BGP view

Parameters None

Description Use the **ipv6-family** command to enter IPv6 address family view.

Use the **undo ipv6-family** command to remove all configurations from the view.

IPv4 BGP unicast view is the default.

Examples # Enter IPv6 address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6]
```

network

Syntax **network** *ipv6-address prefix-length* [**short-cut** | **route-policy** *route-policy-name*]

undo network *ipv6-address prefix-length* [**short-cut**]

View IPv6 address family view

Parameters *ipv6-address*: IPv6 address.

prefix-length: Prefix length of the address, in the range 0 to 128.

short-cut: If the keyword is specified for an EBGp route, the route will use the local routing management value rather than that of EBGp routes, so the preference of the route is reduced.

route-policy-name: Name of a routing policy, a string of 1 to 19 characters.

Description Use the **network** command to advertise a network to the IPv6 BGP routing table.

Use the **undo network** command to remove an entry from the IPv6 BGP routing table.

By default, no route is advertised.

Note that:

- The route to be advertised must exist in the local IP routing table, and using a routing policy makes route management more flexible.
- The route advertised to the BGP routing table using the **network** command has the IGP origin attribute.

Examples # Advertise the network 2002::/16 into the IPv6 BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] network 2002:: 16
```

peer advertise-community

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **advertise-community**
undo peer { *ipv6-group-name* | *ipv6-address* } **advertise-community**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.
ipv6-address: IPv6 address of a peer.

Description Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attribute is advertised to any peer group/peer.

Examples # Advertise the community attribute to the peer 1:2::3:4.

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-community
```

peer advertise-ext-community

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **advertise-ext-community**
undo peer { *ipv6-group-name* | *ipv6-address* } **advertise-ext-community**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.
ipv6-address: IPv6 address of a peer.

Description Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to remove the configuration.

By default, no extended community attribute is advertised to a peer/peer group.

Examples # Advertise the extended community attribute to the peer 1:2::3:4.

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-ext-community

```

peer allow-as-loop

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **allow-as-loop** [*number*]

undo peer { *ipv6-group-name* | *ipv6-address* } **allow-as-loop**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

number: Specifies the repeating times of the local AS number, in the range 1 to 10. The default number is 1.

Description Use the **peer allow-as-loop** command to configure IPv6 BGP to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the repeating times of the local AS number.

Use the **undo peer allow-as-loop** command to disable the function.

The local AS number is not allowed to exist in the AS_PATH attribute of routes by default.

Examples # Configure the repeating times of the local AS number allowed in the AS_PATH of routes from peer 1::1 as 2.

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1::1 allow-as-loop 2

```

peer as-number

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **as-number** *as-number*

undo peer *ipv6-group-name* **as-number**

undo peer *ipv6-address*

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-number: AS number of the peer/peer group, in the range 1 to 65535.

Description Use the **peer as-number** command to specify an AS number for a peer/peer group.

Use the **undo peer as-number** command to delete the AS number of a peer group.

Use the **undo peer** command to delete a peer.

By default, no AS number is configured for a peer/peer group.

Examples # Specify the AS number of the peer group test as 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test as-number 200
```

peer as-path-acl

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-path-acl-number: Number of an AS path ACL, in the range 1 to 256.

import: Filters incoming routes.

export: Filters outgoing routes.

Description Use the **peer as-path-acl** command to specify an AS path ACL to filter routes incoming from or outgoing to a peer/peer group.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path list is specified for filtering.

Examples # Specify the AS path ACL 3 to filter routes outgoing to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] ip as-path-acl 3 permit ^200
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-path-acl 3 export
```

peer capability-advertise route-refresh

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

undo peer { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description Use the **peer capability-advertise route-refresh** command to enable IPv6 BGP route-refresh.

Use the **undo peer capability-advertise route-refresh** command to disable the function.

By default, route-refresh is enabled.

Examples # Disable route-refresh of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] undo peer 1:2::3:4 capability-advertise route-refresh
```

peer connect-interface

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **connect-interface** *interface-type* *interface-number*

undo peer { *ipv6-group-name* | *ipv6-address* } **connect-interface**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

interface-type interface-number: Specifies the type and name of the interface.

Description Use the **peer connect-interface** command to specify the source interface for establishing TCP connections to an IPv6 BGP peer or peer group.

Use the **undo peer connect-interface** command to restore the default.

By default, BGP uses the outbound interface of the best route to the IPv6 BGP peer/peer group as the source interface for establishing a TCP connection.

Note that:

To establish multiple BGP connections to a BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router; otherwise, the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.

Examples # Specify loopback 0 as the source interface for routing updates to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 connect-interface loopback 0
```

peer default-route-advertise

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *ipv6-group-name* | *ipv6-address* } **default-route-advertise**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

route-policy-name: Route-policy name, a string of 1 to 19 characters.

Description Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable advertising a default route.

By default, no default route is advertised to a peer/peer group.

Using this command does not require the default route available in the routing table. With this command used, the router sends the default route unconditionally to the peer/peer group with the next hop being itself.

Examples # Advertise a default route to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 default-route-advertise
```

peer description

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **description** *description-text*

undo peer { *ipv6-group-name* | *ipv6-address* } **description**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

description-text: Description information for the peer/peer group, a string of 1 to 79 characters.

Description Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer (group).

You need create a peer/peer group before configuring a description for it.

Examples # Configure the description for the peer group **test** as **ISP1**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test description ISP1
```

peer ebgp-max-hop

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *ipv6-group-name* | *ipv6-address* } **ebgp-max-hop**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

hop-count: Maximum hop count, in the range 1 to 255. By default, the value is 64.

Description Use the **peer ebgp-max-hop** command to allow establishing the EBGp connection to a peer/peer group indirectly connected.

Use the **undo peer ebgp-max-hop** command to remove the configuration.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum router hops of the EBGP connection.

Examples # Allow establishing the EBGP connection with the peer group **test** on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test ebgp-max-hop
```

peer fake-as

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **fake-as** *as-number*

undo peer { *ipv6-group-name* | *ipv6-address* } **fake-as**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-number: Local autonomous system number, in the range 1 to 65535.

Description Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

Examples # Configure a fake AS number of 200 for the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test fake-as 200
```

peer filter-policy

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **filter-policy** *acl6-number* { **import** | **export** }

```
undo peer { ipv6-group-name | ipv6-address } filter-policy [ acl6-number ]
{ import | export }
```

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

acl6-number: IPv6 ACL number, in the range 2000 to 3999.

import: Applies the filter-policy to routes received from the peer/peer group.

export: Applies the filter-policy to routes advertised to the peer/peer group.

Description Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Examples # Apply the ACL6 2000 to filter routes advertised to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2001:1:: 64
[Sysname-acl6-basic-2000] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 filter-policy 2000 export
```

peer group

Syntax **peer** *ipv6-address* **group** *ipv6-group-name* [**as-number** *as-number*]

undo peer *ipv6-address* **group** *ipv6-group-name*

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-number: Specifies the AS number of the peer/peer group, in the range 1 to 65535.

Description Use the **peer group** command to add a peer to a configured peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, the peer does not belong to any peer group.

Examples # Create a peer group named **test** and add the peer 1:2::3:4 to the peer group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 200
[Sysname-bgp-af-ipv6] peer 1:2::3:4 group test
```

peer ignore

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **ignore**

undo peer { *ipv6-group-name* | *ipv6-address* } **ignore**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description Use the **peer ignore** command to terminate the session to a peer or peer group.

Use the **undo peer ignore** command to remove the configuration.

By default, a router can establish sessions with a peer or peer group.

After the **peer ignore** command is executed, the system terminates the active session(s) with the specified peer or peer group and clears all the related routing information. For a peer group, this means all the sessions with the peer group will be tore down.

Examples # Terminate the session with peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ignore
```

peer ipv6-prefix

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** { **import** | **export** }

View IPv6 address family view

- Parameters** *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.
- ipv6-address*: IPv6 address of a peer.
- ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.
- import**: Applies the filtering policy to routes received from the specified peer/peer group.
- export**: Applies the filtering policy to routes advertised to the specified peer/peer group.
- Description** Use the **peer ipv6-prefix** command to specify an IPv6 prefix list to filter routes incoming from or outgoing to a peer or peer group.
- Use the **undo peer ipv6-prefix** command to remove the configuration.
- By default, no IPv6 prefix list is specified for filtering.
- Examples** # Reference the IPv6 prefix list **list 1** to filter routes outgoing to peer 1:2::3:4.
- ```
<Sysname> system-view
[Sysname] ip ipv6-prefix list1 permit 2002:: 64
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ipv6-prefix list1 export
```

---

## peer keep-all-routes

- Syntax** **peer** { *ipv6-group-name* | *ipv6-address* } **keep-all-routes**
- undo peer** { *ipv6-group-name* | *ipv6-address* } **keep-all-routes**
- View** IPv6 address family view
- Parameters** *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.
- ipv6-address*: IPv6 address of a peer.
- Description** Use the **peer keep-all-routes** command to save the original routing information from a peer or peer group, including even routes that failed to pass the inbound policy.
- Use the **undo peer keep-all-routes** command to disable this function.
- By default, the function is not enabled.
- Examples** # Save routing information from peer 1:2::3:4.
- ```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 keep-all-routes
```

peer log-change

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **log-change**
undo peer { *ipv6-group-name* | *ipv6-address* } **log-change**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.
ipv6-address: IPv6 address of a peer.

Description Use the **peer log-change** command to enable the logging of session state and event information of a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

Examples # Enable the logging of session state and event information of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 log-change
```

peer next-hop-local

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **next-hop-local**
undo peer { *ipv6-group-name* | *ipv6-address* } **next-hop-local**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.
ipv6-address: IPv6 address of a peer.

Description Use the **peer next-hop-local** command to configure the next hop of routes advertised to a peer/peer group as the local router.

Use the **undo peer next-hop-local** command to restore the default.

By default, the system sets the next hop of routes advertised to an EBGp peer/peer group to the local router, but does not set for routes outgoing to an IBGP peer/peer group.

Examples # Set the next hop of routes advertised to EBGp peer group **test** to the router itself.

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test next-hop-local

```

peer preferred-value

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value*
undo peer { *ipv6-group-name* | *ipv6-address* } **preferred-value**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.
ipv6-address: IPv6 address of a peer.
value: Preferred value, in the range 0 to 65535.

Description Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default.

By default, routes received from a peer or peer group have a preferred value of 0.

Routes learned from peers each have an initial preferred value. Among multiple routes to the same destination, the route with the biggest value is selected.

Note that:

If you both reference a routing policy and use the command **peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value* to set a preferred value for routes from a peer, the routing policy sets a non-zero preferred value for routes matching it. Other routes not matching the routing policy uses the value set with the command. If the preferred value in the routing policy is zero, the routes matching it will also use the value set with the command. For information about using a routing policy to set a preferred value, refer to the **peer** { *ipv6-group-name* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** } command and the **apply preferred-value** *preferred-value* command.

Examples # Configure the preferred value as 50 for routes from peer 1:2::3:4.

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 preferred-value 50

```

peer public-as-only

Syntax `peer { ipv6-group-name | ipv6-address } public-as-only`
undo peer { ipv6-group-name | ipv6-address } public-as-only

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.
ipv6-address: IPv6 address of a peer.

Description Use the **peer public-as-only** command to configure IPv6 BGP updates to a peer/peer group to not carry private AS numbers.

Use the **undo peer public-as-only** command to allow IPv6 BGP updates to a peer/peer group to carry private AS numbers.

By default, BGP updates carry the private AS number.

The command does not take effect if the BGP update has both the public AS number and private AS number. The range of private AS number is from 64512 to 65535.

Examples # Carry no private AS number in BGP updates sent to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 public-as-only
```

peer reflect-client

Syntax `peer { ipv6-group-name | ipv6-address } reflect-client`
undo peer { ipv6-group-name | ipv6-address } reflect-client

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.
ipv6-address: IPv6 address of a peer.

Description Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients, reflector cluster-id.**

Examples # Configure the local device as a route reflector and specify the peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test
[Sysname-bgp-af-ipv6] peer test reflect-client
```

peer route-limit

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **route-limit** *limit* [*percentage*]

undo peer { *ipv6-group-name* | *ipv6-address* } **route-limit**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

limit: Specifies the upper limit of IPv6 address prefixes that can be received from the peer or peer group. The limit varies with devices.

percentage: Specifies the percentage of routes to generate alarm information, ranging from 1 to 100, with the default as 75.

Description Use the **peer route-limit** command to set the maximum number of prefixes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

By default, the router has no limit on prefixes from a peer/peer group.

The router will end the peer relation when the number of address prefixes received for the peer exceeds the limit.

Examples # Set the number of prefixes allowed to receive from the peer 1:2::3:4 to 1000.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-limit 1000
```

peer route-policy

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

```
undo peer { ipv6-group-name | ipv6-address } route-policy route-policy-name
{ import | export }
```

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

route-policy-name: Specifies route-policy name, a string of 1 to 19 characters.

import: Applies the routing policy to routes from the peer (group).

export: Applies the routing policy to routes to the peer (group).

Description Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no routing policy is specified for the peer (group).

Use of the **peer route-policy** command does not apply the **if-match interface** clause defined in the routing policy. Refer to "Routing Policy Common Configuration Commands" on page 447 and "IPv4 Routing Policy Configuration Commands" on page 467.

Examples # Apply the routing policy test-policy to routes received from the peer group **test**.

```
<Sysname> system-view
[Sysname] route-policy test-policy permit node 10
[Sysname-route-policy] if-match cost 10
[Sysname-route-policy] apply cost 65535
[Sysname-route-policy] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test route-policy test-policy import
```

peer route-update-interval

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **route-update-interval** *seconds*

undo peer { *ipv6-group-name* | *ipv6-address* } **route-update-interval**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

seconds: Specifies the minimum interval for sending the same update to a peer (group) from 5 to 600 seconds.

Description Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default.

By default, the interval is 15 seconds for the IBGP peer, and 30 seconds for the EBGP peer.

Examples # Specify the interval for sending the same update to the peer 1:2::3:4 as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-update-interval 10
```

peer substitute-as

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **substitute-as**
undo peer { *ipv6-group-name* | *ipv6-address* } **substitute-as**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description Use the **peer substitute-as** command to substitute the local AS number for the AS number of a peer/peer group in the AS_PATH attribute.

Use the **undo peer substitute-as** command to remove the configuration.

The substitution is not configured by default.

Examples # Substitute the local AS number for the AS number of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 substitute-as
```

peer timer

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **timer keepalive** *keepalive* **hold** *holdtime*

undo peer { *ipv6-group-name* | *ipv6-address* } **timer**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

keepalive: Specifies the keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Specifies the holdtime in seconds, ranging from 3 to 65535.

Description Use the **peer timer** command to configure keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

keepalive interval defaults to 60 seconds, and *holdtime* interval defaults to 180 seconds

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer**.

Examples # Configure the keepalive interval and holdtime interval for the peer group test as 60 seconds and 180 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test timer keepalive 60 hold 180
```

preference

Syntax **preference** { *external-preference* *internal-preference* *local-preference* | **route-policy** *route-policy-name* }

undo preference

View IPv6 address family view

Parameters *external-preference*: Preference of EBGp route learned from an EBGp peer, in the range 1 to 255.

internal-preference: Preference of IBGp route learned from an IBGp peer, in the range 1 to 255.

local-preference: Preference of IPv6 BGP local route, in the range 1 to 255.

route-policy-name: Routing policy name, a string of 1 to 19 characters. The routing policy can set a preference for routes passing it. The default value applies to the routes filtered out.

Description Use the **preference** command to configure preferences for EBGP, IBGP, and local routes.

Use the **undo preference** command to restore the default.

The bigger the preference value is, the lower the preference is. The default values of *external-preference*, *internal-preference* and *local-preference* are 255, 255 and 130 respectively.

Examples # Configure preferences for EBGP, IBGP, and local routes as 20, 20 and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] preference 20 20 200
```

reflect between-clients

Syntax **reflect between-clients**

undo reflect between-clients

View IPv6 address family view

Parameters None

Description Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects routes between clients. If the clients are fully meshed, it is recommended to disable route reflection on the route reflector to reduce costs.

Related commands: **reflector cluster-id**, **peer reflect-client**.

Examples # Enable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflect between-clients
```

reflector cluster-id

Syntax **reflector cluster-id** *cluster-id*

undo reflector cluster-id

View IPv6 address family view

Parameters *cluster-id*: Specifies the cluster ID of the route reflector, an integer from 1 to 4294967295 (the system translates it into an IPv4 address) or an IPv4 address.

Description Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, a route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster, so the router ID of the route reflector identifies the cluster. If multiple route reflectors are configured to improve the stability of the network, you should use this command to configure the identical cluster ID for all the reflectors to avoid routing loops.

Related commands: **reflect between-clients**, **peer reflect-client**.

Examples # Set 50 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflector cluster-id 50
```

refresh bgp ipv6

Syntax **refresh bgp ipv6** { *ipv6-address* | **all** | **external** | **group** *ipv6-group-name* | **internal** } { **export** | **import** }

View User view

Parameters *ipv6-address*: Soft-resets the connection with an IPv6 BGP peer.

all: Soft-resets all IPv6 BGP connections.

external: Soft-resets EBGp connections.

group *ipv6-group-name*: Soft-resets connections with a peer group. The name of the peer group is a string of 1 to 47 characters.

internal: Soft-resets IBGP connections.

export: Performs soft reset in outbound direction.

import: Performs soft reset in inbound direction.

Description Use the **refresh bgp ipv6** command to soft reset specified IPv6 BGP connections. With this feature, you can refresh the IPv6 BGP routing table and apply a new available policy without tearing down BGP connections.

To perform IPv6 BGP soft reset, all routers in the network should support route-refresh. If a router not supporting route refresh exists in the network, you need to use the **peer keep-all-routes** command on the local router to save all route updates before performing soft reset.

Examples # Soft reset inbound IPv6 BGP connections.
 <Sysname> refresh bgp ipv6 all import

reset bgp ipv6

Syntax **reset bgp ipv6** { *as-number* | *ipv6-address* [**flap-info**] } | **all** | **group** *ipv6-group-name* | **external** | **internal** }

View User view

Parameters *as-number*: Resets the IPv6 BGP connections to peers in the specified AS.

ipv6-address: Resets the connection to the specified IPv6 BGP peer.

flap-info: Clears the history information of routing flaps.

all: Resets all IPv6 BGP connections.

group *ipv6-group-name*: Resets the connections to the specified IPv6 BGP peer group.

external: Resets all the EBGP connections.

internal: Resets all the IBGP connections.

Description Use the **reset bgp ipv6** command to reset specified IPv6 BGP connections.

Examples # Reset all the IPv6 BGP connections.
 <Sysname> reset bgp ipv6 all

reset bgp ipv6 dampening

Syntax **reset bgp ipv6 dampening** [*ipv6-address prefix-length*]

| | |
|--------------------|--|
| View | User view |
| Parameters | <p><i>ipv6-address</i>: IPv6 address</p> <p><i>prefix-length</i>: Prefix length of the address, in the range 0 to 128.</p> |
| Description | <p>Use the reset bgp ipv6 dampening command to clear dampened IPv6 BGP route information and release suppressed routes.</p> <p>If no <i>ipv6-address prefix-length</i> is specified, all dampened IPv6 BGP route information will be cleared.</p> |
| Examples | <p># Clear the dampened information of routes to 2345::/64 and release suppressed routes.</p> <pre><Sysname> reset bgp ipv6 dampening 2345:: 64</pre> |

reset bgp ipv6 flap-info

| | |
|--------------------|--|
| Syntax | reset bgp ipv6 flap-info [<i>ipv6-address/prefix-length</i> regex <i>as-path-regexp</i> as-path-acl <i>as-path-acl-number</i>] |
| View | User view |
| Parameters | <p><i>ipv6-address</i>: Clears the flap statistics for the specified IPv6 address.</p> <p><i>prefix-length</i>: Prefix length of the address, in the range 1 to 128.</p> <p><i>as-path-regexp</i>: Clears the flap statistics for routes matching the AS path regular expression.</p> <p><i>as-path-acl-number</i>: Clears the flap statistics for routes matching the AS path ACL. The number is in the range 1 to 256.</p> |
| Description | <p>Use the reset bgp ipv6 flap-info command to clear IPv6 routing flap statistics.</p> <p>If no parameters are specified, the flap statistics of all the routes will be cleared</p> |
| Examples | <p># Clear the flap statistics of the routes matching AS path ACL 10.</p> <pre><Sysname> system-view [Sysname] ip as-path 10 permit ^100.*200\$ [Sysname] quit <Sysname> reset bgp ipv6 flap-info as-path-acl 10</pre> |

router-id

| | |
|---------------|-----------------------------------|
| Syntax | router-id <i>router-id</i> |
| | undo router-id |

| | |
|--------------------|--|
| View | BGP view |
| Parameters | <i>router-id</i> : Router ID in IP address format. |
| Description | <p>Use the router-id command to specify a router ID for the router.</p> <p>Use the undo router-id command to remove a router ID.</p> <p>To run IPv6 BGP protocol, a router must have a router ID, an unsigned 32-bit integer and the unique ID of the router in the AS.</p> <p>A router ID can be configured manually. If not, the system will select a router ID automatically from the current interfaces' IPv4 addresses. The selection sequence is the highest IPv4 address of Loopback interfaces' addresses, then the highest IPv4 address of physical interfaces' addresses if no Loopback interfaces are configured.</p> <p>Only when the interface with the router ID is removed or the manually configured router ID is removed, will the system select another Router ID. To improve network reliability, it is recommended to configure the IPv4 address of a loopback interface as the router ID.</p> |
| Examples | <pre># Specify the router ID of the router as 10.18.4.221. <Sysname> system-view [Sysname] bgp 100 [Sysname-bgp] router-id 10.18.4.221</pre> |

synchronization

| | |
|--------------------|--|
| Syntax | <p>synchronization</p> <p>undo synchronization</p> |
| View | IPv6 address family view |
| Parameters | None |
| Description | <p>Use the synchronization command to enable the synchronization between IPv6 BGP and IGP.</p> <p>Use the undo synchronization command to disable the synchronization.</p> <p>The feature is disabled by default.</p> <p>With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, IPv6 BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.</p> |

By default, upon receiving an IPv6 IBGP route, the BGP router only checks whether the next hop is reachable before advertisement. If synchronization is enabled, the IBGP route can be advertised to EBGP peers only when the route is also advertised by the IGP.

Examples # Enable the route synchronization between IPv6 BGP and IGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] synchronization
```

timer

Syntax **timer keepalive** *keepalive* **hold** *holdtime*

undo timer

View IPv6 address family view

Parameters *keepalive*: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description Use the **timer** command to specify IPv6 BGP keepalive interval and holdtime interval.

Use the **undo timer** command to restore the default.

By default, the keepalive and holdtime intervals are 60s and 180s respectively.

Note that:

- Timer configured using the peer timer command is preferred to the timer configured using the timer command.
- The holdtime interval must be at least three times the keepalive interval.
- The configured timer applies to all the IPv6 BGP peers. It becomes valid only after the corresponding IPv6 BGP connections are reset.

Related commands: **peer timer**.

Examples # Configure keepalive interval and holdtime interval as 60 and 180 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] timer keepalive 60 hold 180
```

34

IPv6 ROUTING POLICY CONFIGURATION COMMANDS

apply ipv6 next-hop

Syntax **apply ipv6 next-hop** *ipv6-address*

undo apply ipv6 next-hop

View Routing policy view

Parameters *ipv6-address*: Next hop IPv6 address.

Description Use the **apply ipv6 next-hop** command to apply a next hop to IPv6 routes.

Use the **undo apply ipv6 next-hop** command to remove the clause configuration.

No next hop address is set for IPv6 routing information by default.

Using the **apply ipv6 next-hop** command to set a next hop when redistributing routes does not take effect.

Examples # Create routing policy **policy1** with node 10, matching mode **permit**. If a route matches AS path list 1, set next hop 3ff3:506::1 for it.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ipv6 next-hop 3ffe:506::1
```

display ip ipv6-prefix

Syntax **display ip ipv6-prefix** [*ipv6-prefix-name*]

View Any view

Parameters *ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

Description Use the **display ip ipv6-prefix** command to display the statistics of the specified IPv6 prefix list. If no IPv6 prefix list is specified, the statistics of all the IPv6 prefix lists will be displayed.

Examples # Display the statistics of all the IPv6 prefix lists.

```
<Sysname> display ip ipv6-prefix
Prefix-list6 abc
Permitted 0
Denied 0
      index: 10          permit ::/0
      index: 20          permit ::/1          ge 1   le 128
```

Table 137 Field descriptions of the display ip ipv6-prefix command

| Field | Description |
|--------------|---|
| Prefix-list6 | Name of the IPv6 prefix list |
| Permitted | Number of routes satisfying the match criterion |
| Denied | Number of routes not satisfying the match criterion |
| Index | Internal serial number of address prefix list |
| Permit | Matching mode: permit, deny |
| ::/1 | IPv6 address and its prefix length for matching |
| ge | greater-equal, the lower limit prefix length |
| le | less-equal, the upper limit prefix length |

if-match ipv6

Syntax **if-match ipv6** { **address** | **next-hop** | **route-source** } { **acl** *acl6-number* | **prefix-list** *ipv6-prefix-name* }

undo if-match ipv6 { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

View Routing policy view

Parameters **address**: Matches the destination address of IPv6 routing information.

next-hop: Matches the next hop of IPv6 routing information.

route-source: Matches the source address of IPv6 routing information.

acl *acl6-number*: Specifies the number of an IPv6 ACL for filtering, in the range 2000 to 3999 for **address**, and 2000 to 2999 for **next-hop** and **route-source**.

prefix-list *ipv6-prefix-name*: Specifies the name of a IPv6 prefix list for filtering, a string of 1 to 19 characters.

Description Use the **if-match ipv6** command to configure a destination, next hop or source address based match criterion for IPv6 routes.

Use the **undo if-match ipv6** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to permit the routing information whose next hop address matches IPv6 prefix list p1.

```

<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ipv6 next-hop prefix-list pl

```

ip ipv6-prefix

Syntax **ip ipv6-prefix** *ipv6-prefix-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address prefix-length* [**greater-equal** *min-prefix-length*] [**less-equal** *max-prefix-length*]

undo ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*]

View System view

Parameters *ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters, for uniquely specifying an IPv6 prefix list.

index-number: Index number, in the range 1 to 65535, for uniquely specifying an IPv6 prefix list item. The item with a smaller *index-number* will be tested first.

permit: Specifies the matching mode for the IPv6 prefix list as permit, that is, if a route matches the IPv6 prefix list, it passes the IPv6 prefix list without needing to enter the next item for test. If not, it will enter the next item test.

deny: Specifies the matching mode for the IPv6 prefix list as deny, that is, if a route matches the IPv6 prefix list, the route neither passes the filter nor enters the next node for test; if not, the route will enter the next item test.

ipv6-address prefix-length: Specifies an IPv6 prefix and prefix length, with *prefix-length* being in the range 0 to 128. When specified as :: 0, it matches the default route.

greater-equal *min-prefix-length*: Greater than or equal to the minimum prefix length.

less-equal *max-prefix-length*: Less than or equal to the maximum prefix length.

The length relation is $mask-length \leq min-mask-length \leq max-mask-length \leq 128$. If only *min-prefix-length* is specified, the prefix length range is [*min-prefix-length*, 128]. If only *max-prefix-length* is specified, the prefix length range is [*prefix-length*, *max-prefix-length*]. If both *min-prefix-length* and *max-prefix-length* are specified, the prefix length range is [*min-prefix-length*, *max-prefix-length*].

Description Use the **ip ipv6-prefix** command to configure an IPv6 prefix list item.

Use the **undo ip ipv6-prefix** command to remove an IPv6 prefix list or an item.

No IPv6 prefix list is configured by default.

The IPv6 address prefix list is used to filter IPv6 addresses. It may have multiple items, and each of them specifies a range of IPv6 prefix. The filtering relation among items is logic OR, namely, a route passing an item will pass the prefix list.

The IPv6 prefix range is determined by *prefix-length* and [*min-prefix-length*, *max-prefix-length*]. If both *mask-length* and [*min-mask-length*, *max-mask-length*] are specified, then the IPv6 addresses must satisfy both of them.

If *ipv6-address prefix-length* is specified as :: 0, then only the default route matches.

If you want it to match all the routes, configure it as :: 0 **less-equal** 128.

Examples # Permit the IPv6 addresses with mask length between 32 bits and 64 bits.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc permit :: 0 greater-equal 32 less-equal 64
```

Deny the IPv6 addresses with prefix as 3FEE:D00::/32, prefix length greater than or equal to 32 bits.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc deny 3FEE:D00:: 32 less-equal 128
```

reset ip ipv6-prefix

Syntax **reset ip ipv6-prefix** [*ipv6-prefix-name*]

View User view

Parameters *ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

Description Use the **reset ip ipv6-prefix** command to clear the statistics of the specified IPv6 prefix list. If no name is specified, the statistics of all IPv6 prefix lists will be cleared.

Examples # Clear the statistics of IPv6 prefix list **abc**.

```
<Sysname> reset ip ipv6-prefix abc
```

35

IPv6 BASICS CONFIGURATION COMMANDS



- The 0231A92P module does not support IPv6 features.
- A tunnel interface number is in the A/B/C format, where A, B, and C represent the slot number of a module, the slot number of a sub-card, and the tunnel interface number, respectively. A and B vary with devices while C ranges from 0 to 1023.

display dns ipv6 dynamic-host

Syntax `display dns ipv6 dynamic-host`

View Any view

Parameters None

Description Use the **display dns ipv6 dynamic-host** command to display IPv6 dynamic domain name cache information.

Examples # Display IPv6 dynamic domain name cache information.

```
<Sysname> display dns ipv6 dynamic-host
No  Host                IPv6 Address          TTL
1   aaa                  2001::2              6
```

Table 138 Description on fields of the display dns ipv6 dynamic-host command

| Field | Description |
|--------------|--|
| No | Sequence number |
| Host | Host name |
| IPv6 address | IPv6 address of the host |
| TTL | Time an entry can be cached in seconds |



For a domain name displayed with the **display dns ipv6 dynamic-host** command, no more than 21 characters can be displayed. If the domain name exceeds the maximum length, the first 21 characters will be displayed.

display dns ipv6 server

Syntax `display dns ipv6 server [dynamic]`

View Any view

Parameters **dynamic:** Displays the information of IPv6 DNS servers acquired dynamically through DHCP or other protocols.

Description Use the **display dns ipv6 server** command to display IPv6 DNS server information.

Examples # Display IPv6 DNS server information.

```
<Sysname> display dns ipv6 server
Type:
  D:Dynamic   S:Static

DNS Server  Type  IPv6 Address                               (Interface Name)
  1          S      1::1
  2          S      FE80:1111:2222:3333:4444:5555:6666:7777  Vlan2
```

Table 139 Field descriptions of the display dns ipv6 server command

| Field | Description |
|----------------|---|
| DNS Server | Sequence number of the DNS server, which is assigned automatically by the system, starting from 1. |
| Type | Type of DNS server: S represents a statically configured DNS server, and D represents a DNS server obtained dynamically through DHCP. |
| IPv6 Address | IPv6 address of the DNS server |
| Interface Name | Name of the interface on the DNS server whose IP address is an IPv6 link-local address. |

display ipv6 fib

Syntax **display ipv6 fib** [*slot-number*] [*ipv6-address*]

View Any view

Parameters *slot-number:* Number of the slot whose IPv6 forwarding information base (FIB) entries are to be displayed.

ipv6-address: Destination IPv6 address whose IPv6 FIB entries are to be displayed.

Description Use the **display ipv6 fib** command to display IPv6 FIB entries. If no argument is specified, all IPv6 FIB entries will be displayed.

Examples # Display all IPv6 FIB entries.

```
<Sysname> display ipv6 fib
FIB Table:
Total number of Routes : 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static

Destination:  ::1                               PrefixLength : 128
NextHop      :  ::1                               Flag         : HU
Label        :  NULL                               Tunnel ID    : 0
TimeStamp    :  Date- 8/29/2007, Time- 10:11:42
Interface    :  InLoopBack0
```


Table 140 Description on fields of the display ipv6 fib command

| Field | Description |
|------------------------|--|
| Total number of Routes | Total number of routes in the FIB |
| Destination | Destination address to which a packet is to be forwarded |
| PrefixLength | Prefix length of the destination address |
| NextHop | Next hop of the route to the destination |
| Flag | Route flag: <ul style="list-style-type: none"> ■ U - Usable route ■ G - Gateway route ■ H - Host route ■ B - Black hole route ■ D - Dynamic route ■ S - Static route |
| Label | Label |
| Tunnel ID | ID of a tunnel |
| TimeStamp | Generation time of a FIB entry |
| Interface | Outgoing interface that forwards packets |

display ipv6 host

Syntax `display ipv6 host`

View Any view

Parameters None

Description Use the **display ipv6 host** command to display the mappings between host names and IPv6 addresses in the static DNS database.

Examples # Display the mappings between host names and IPv6 addresses in the static DNS database.

```
<Sysname> display ipv6 host
Host          Age          Flags          IPv6Address
aaa           0            static         2002::1
bbb           0            static         2002::2
```

Table 141 Description on fields of the display ipv6 host command

| Field | Description |
|-------------|---|
| Host | Host name |
| Age | Time for the entry to live. "0" is displayed in the case of static configuration. |
| Flags | Flag indicating the type of mapping between a host name and an IPv6 address. Static indicates a static mapping. |
| IPv6Address | IPv6 address of a host |

display ipv6 interface

Syntax **display ipv6 interface** [**brief**] [*interface-type* [*interface-number*]]

View Any view

Parameters **brief**: Displays brief IPv6 information of an interface.

interface-type: Interface type.

interface-number: Interface number.

Description Use the **display ipv6 interface** command to display the IPv6 information of an interface for which an IPv6 address can be configured.

If *interface-type interface-number* is not specified, the IPv6 information of all interfaces for which IPv6 addresses can be configured is displayed; if only *interface-type* is specified, the IPv6 information of the interfaces of the specified type for which IPv6 addresses can be configured is displayed; if the *interface-type interface-number* is specified, the IPv6 information of the specified interface is displayed.

Examples # Display the IPv6 information of VLAN-interface 2.

```
<Sysname> display ipv6 interface vlan-interface 2
Vlan-interface2 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF65:4322
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Table 142 Description on fields of the display ipv6 interface command

| Field | Description |
|-------------------------------|--|
| Vlan-interface2 current state | Physical state of the interface |
| Line protocol current state | Link layer protocol state of the interface |
| IPv6 is enabled | IPv6 packet forwarding state of the interface (IPv6 packet forwarding is enabled in the example) |
| link-local address | Link-local address configured for the interface |
| Global unicast address(es) | Aggregatable global unicast address(es) configured for the interface |
| Joined group address(es) | Address(es) of multicast group(s) that the interface joins |
| MTU | Maximum transmission unit of the interface |

Table 142 Description on fields of the display ipv6 interface command

| Field | Description |
|--|---|
| ND DAD is enabled, number of DAD attempts | Number of DAD attempts, with DAD enabled |
| ND reachable time | Neighbor reachable time |
| ND retransmit interval | Interval for retransmitting a neighbor solicitation (NS) message |
| Hosts use stateless autoconfig for addresses | Hosts use stateless auto-configuration mode to acquire IPv6 addresses |

Display the brief IPv6 information of all interfaces for which IPv6 addresses can be configured.

```
<Sysname> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                Physical      Protocol      IPv6 Address
Vlan-interface1          down         down          Unassigned
Vlan-interface2          up           up            2001::1
Vlan-interface100        up           down          Unassigned
```

Table 143 Description on fields of display ipv6 interface brief

| Field | Description |
|--------------|--|
| *down | The interface is down, that is, the interface is closed by using the shutdown command. |
| (s) | Spoofing attribute of the interface, that is, the link protocol state of the interface is up, but the link does not exist, or the link is established on demand, instead of being permanent. |
| Interface | Name of the interface |
| Physical | Physical state of the interface |
| Protocol | Link protocol state of the interface |
| IPv6 Address | IPv6 address of the interface. Only the first of configured IPv6 addresses is displayed. (If no address is configured for the interface, "Unassigned" will be displayed.) |

display ipv6 neighbors

Syntax **display ipv6 neighbors** { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [| { **begin** | **exclude** | **include** } *text*]

View Any view

Parameters *ipv6-address*: IPv6 address whose neighbor information is to be displayed.

all: Displays information of all neighbors, including neighbors acquired dynamically and configured statically.

dynamic: Displays information of all neighbors acquired dynamically.

static: Displays information of all neighbors configured statically.

slot *slot-number*: Displays information of the neighbors of a specified slot.

interface *interface-type interface-number*: Displays information of the neighbors of a specified interface.

vlan *vlan-id*: Displays information of the neighbors of a specified VLAN whose ID ranges from 1 to 4094.

|: Filters the output information.

begin: Displays the neighbor entries from the first one containing the specified character string.

include: Displays the neighbor entries containing the specified character string.

exclude: Displays the neighbor entries without the specified character string.

text: Character string.

Description Use the **display ipv6 neighbors** command to display neighbor information.

Examples # Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
                                Type: S-Static   D-Dynamic
IPv6 Address                    Link-layer          VID  Interface      Sta
te T   Age
FE80::200:5EFF:FE32:B800      0000-5e32-b800    1   Eth3/0/3       REACH
S   -
```

Table 144 Description on fields of the display ipv6 neighbors command

| Field | Description |
|--------------|--|
| IPv6 Address | IPv6 address of a neighbor |
| Link-layer | Link layer address (MAC address of a neighbor) |
| VID | VLAN to which the interface connected with a neighbor belongs |
| Interface | Interface connected with a neighbor |
| State | State of a neighbor, including: <ul style="list-style-type: none"> ■ INCOMP: The address is being resolved. The link layer address of the neighbor is unknown. ■ REACH: The neighbor is reachable. ■ STALE: The reachability of the neighbor is unknown. The device will not verify the reachability any longer unless data is sent to the neighbor. ■ DELAY: The reachability of the neighbor is unknown. The device sends an NS message after a delay. ■ PROBE: The reachability of the neighbor is unknown. The device sends an NS message to verify the reachability of the neighbor. |
| T | Type of neighbor information, including static configuration and dynamic acquisition. |
| Age | For a static entry, a hyphen "-" is displayed. For a dynamic entry, the reachable time (in seconds) elapsed is displayed, and if it is never reachable, "#" is displayed (for a neighbor acquired dynamically). |

display ipv6 neighbors count

- Syntax** **display ipv6 neighbors** { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**
- View** Any view
- Parameters** **all**: Displays the total number of all neighbor entries, including neighbor entries acquired dynamically and configured statically.
- dynamic**: Displays the total number of all neighbor entries acquired dynamically.
- static**: Displays the total number of neighbor entries configured statically.
- slot** *slot-number*: Displays the total number of neighbor entries of a specified slot.
- interface** *interface-type interface-number*: Displays the total number of neighbor entries of a specified interface.
- vlan** *vlan-id*: Displays the total number of neighbor entries of a specified VLAN whose ID ranges from 1 to 4094.
- Description** Use the **display ipv6 neighbors count** command to display the total number of neighbor entries satisfying the specified condition.
- Examples** # Display the total number of neighbor entries acquired dynamically.
- ```
<Sysname> display ipv6 neighbors dynamic count
Total dynamic entry(ies): 2
```

---

**display ipv6 pathmtu**

- Syntax** **display ipv6 pathmtu** { *ipv6-address* | **all** | **dynamic** | **static** }
- View** Any view
- Parameters** *ipv6-address*: IPv6 address whose PMTU information is to be displayed.
- all**: Displays all PMTU information.
- dynamic**: Displays all dynamic PMTU information.
- static**: Displays all static PMTU information.
- Description** Use the **display ipv6 pathmtu** command to display the PMTU information of IPv6 addresses.
- Examples** # Display all PMTU information.

```
<Sysname> display ipv6 pathmtu all
IPv6 Destination Address ZoneID PathMTU Age Type
fe80::12 0 1300 40 Dynamic
2222::3 0 1280 - Static
```

**Table 145** Description on fields of the display ipv6 pathmtu command

Field	Description
IPv6 Destination Address	Destination IPv6 address
ZoneID	ID of address zone, currently invalid
PathMTU	PMTU of an IPv6 address
Age	Time for a PMTU to live. For a static PMTU, a hyphen "-" is displayed.
Type	Indicates the PMTU is dynamically negotiated or statically configured.

## display ipv6 socket

**Syntax** **display ipv6 socket** [ **socketype** *socket-type* ] [ *task-id* *socket-id* ] [ **slot** *slot-number* ]

**View** Any view

**Parameters** **socketype** *socket-type*: Displays the socket information of this type. The socket type is in the range of 1 to 3. The value "1" represents a TCP socket, "2" a UDP socket, and "3" a raw IP socket.

*task-id*: Displays the socket information of the task. The task ID is in the range 1 to 100.

*socket-id*: Displays the information of the socket. The socket ID is in the range 0 to 3072.

*slot-number*: Number of a slot.

**Description** Use the **display ipv6 socket** command to display socket information.

**Examples** # Display the information of all sockets.

```
<Sysname> display ipv6 socket
SOCK_STREAM:
Task = VTYP(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDSOCKETID,
socket state = SS_PRIV SS_ASYNC

Task = VTYP(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDSOCKETID,
socket state = SS_PRIV SS_ASYNC
```

```

SOCK_DGRAM:
Task = AGNT(51), socketid = 2, Proto = 17,
LA = ::->161, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = TRAP(52), socketid = 2, Proto = 17,
LA = ::->1024, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option =,
socket state = SS_PRIV

SOCK_RAW:
Task = ROUT(86), socketid = 5, Proto = 89,
LA = ::, FA = ::,
sndbuf = 262144, rcvbuf = 262144, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR,
socket state = SS_PRIV SS_ASYNC

```

**Table 146** Description on fields of the display ipv6 socket command

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task ID of the created socket
socketid	ID assigned by the kernel to the created socket
Proto	Protocol ID
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Size of the send buffer
rcvbuf	Size of the receive buffer
sb_cc	Number of bytes sent by the send buffer
rb_cc	Number of bytes received by the receive buffer
socket option	Socket option set by the application
socket state	State of the socket

---

## display ipv6 statistics

**Syntax** **display ipv6 statistics** [ *slot slot-number* ]

**View** Any view

**Parameters** **slot slot-number**: Display statistics of IPv6 packets and IPv6 ICMP packets on the slot.

**Description** Use the **display ipv6 statistics** command to display statistics of IPv6 packets and IPv6 ICMP packets.

**Examples** # Display the statistics of IPv6 packets and IPv6 ICMP packets.

```

<Sysname> display ipv6 statistics
IPv6 Protocol:

Sent packets:
 Total: 0
 Local sent out: 0 forwarded: 0
 raw packets: 0 discarded: 0
 routing failed: 0 fragments: 0
 fragments failed: 0

Received packets:
 Total: 0
 local host: 0 hopcount exceeded: 0
 format error: 0 option error: 0
 protocol error: 0 fragments: 0
 reassembled: 0 reassembly failed: 0
 reassembly timeout: 0

ICMPv6 protocol:

Sent packets:
 Total: 0
 unreachable: 0 too big: 0
 hopcount exceeded: 0 reassembly timeout: 0
 parameter problem: 0
 echo request: 0 echo replied: 0
 neighbor solicit: 0 neighbor advert: 0
 router solicit: 0 router advert: 0
 redirected: 0
 Send failed:
 ratelimited: 0 other errors: 0

Received packets:
 Total: 0
 checksum error: 0 too short: 0
 bad code: 0
 unreachable: 0 too big: 0
 hopcount exceeded: 0 reassembly timeout: 0
 parameter problem: 0 unknown error type: 0
 echoed: 0 echo replied: 0
 neighbor solicit: 0 neighbor advert: 0
 router solicit: 0 router advert: 0
 redirected: 0 router renumbering: 0
 unknown info type: 0
 Deliver failed:
 bad length: 0 ratelimited: 0

```

**Table 147** Description on fields of the display ipv6 statistics command

Field	Description
IPv6 Protocol:	Statistics of IPv6 packets
Sent packets:	Statistics of sent IPv6 packets, including:
Total: 0	<ul style="list-style-type: none"> <li>■ Total number of sent packets</li> </ul>
Local sent out: 0 forwarded: 0	<ul style="list-style-type: none"> <li>■ Number of packets sent locally</li> </ul>
raw packets: 0 discarded: 0	<ul style="list-style-type: none"> <li>■ Number of forwarded packets</li> </ul>
routing failed: 0 fragments: 0	<ul style="list-style-type: none"> <li>■ Number of packets sent via raw socket</li> </ul>
fragments failed: 0	<ul style="list-style-type: none"> <li>■ Number of discarded packets</li> <li>■ Number of packets failing to be routed</li> <li>■ Number of sent fragment packets</li> <li>■ Number of fragments failing to be sent</li> </ul>



**Table 147** Description on fields of the display ipv6 statistics command

Field	Description
Received packets:	Statistics of received IPv6 packets, including
Total: 0	<ul style="list-style-type: none"> <li>■ Total number of received packets</li> </ul>
local host: 0 hopcount exceeded: 0	<ul style="list-style-type: none"> <li>■ Number of packets received locally</li> </ul>
format error: 0 option error: 0	<ul style="list-style-type: none"> <li>■ Number of packets exceeding the hop limit</li> </ul>
protocol error: 0 fragments: 0	<ul style="list-style-type: none"> <li>■ Number of packets in an incorrect format</li> </ul>
reassembled: 0 reassembly failed: 0	<ul style="list-style-type: none"> <li>■ Number of packets with incorrect options</li> </ul>
reassembly timeout: 0	<ul style="list-style-type: none"> <li>■ Number of packets with incorrect protocol</li> <li>■ Number of received fragment packets</li> <li>■ Number of reassembled packets</li> <li>■ Number of packets failing to be reassembled</li> <li>■ Number of packets whose reassembly times out</li> </ul>
ICMPv6 protocol:	Statistics of IPv6 ICMP packets
Sent packets:	Statistics of sent IPv6 ICMP packets, including
Total: 0	<ul style="list-style-type: none"> <li>■ Total number of sent packets</li> </ul>
unreached: 0 too big: 0	<ul style="list-style-type: none"> <li>■ Number of packets whose destination is unreachable</li> </ul>
hopcount exceeded: 0	<ul style="list-style-type: none"> <li>■ Number of too large packets</li> </ul>
reassembly timeout: 0	<ul style="list-style-type: none"> <li>■ Number of packets exceeding the hop limit</li> </ul>
parameter problem: 0	<ul style="list-style-type: none"> <li>■ Number of packets whose fragmentation and reassembly times out</li> </ul>
echo request: 0 echo replied: 0	<ul style="list-style-type: none"> <li>■ Number of packets with parameter errors</li> </ul>
neighbor solicit: 0 neighbor advert: 0	<ul style="list-style-type: none"> <li>■ Number of request packets</li> </ul>
router solicit: 0 router advert 0	<ul style="list-style-type: none"> <li>■ Number of response packets</li> </ul>
redirected: 0	<ul style="list-style-type: none"> <li>■ Number of neighbor solicitation packets</li> <li>■ Number of neighbor advertisement packets</li> <li>■ Number of router solicit packets</li> <li>■ Number of router advertisement packets</li> <li>■ Number of redirected packets</li> </ul>
Send failed:	<ul style="list-style-type: none"> <li>■ Number of packets failing to be sent because of rate limitation</li> </ul>
ratelimited: 0 other errors: 0	<ul style="list-style-type: none"> <li>■ Number of packets with other errors</li> </ul>

**Table 147** Description on fields of the display ipv6 statistics command

Field	Description
Received packets:	Statistics of received IPv6 ICMP packets, including
Total: 0	<ul style="list-style-type: none"> <li>■ Total number of received packets</li> </ul>
checksum error: 0 too short: 0	<ul style="list-style-type: none"> <li>■ Number of packets with checksum errors</li> </ul>
bad code 0	<ul style="list-style-type: none"> <li>■ Number of too small packets</li> </ul>
unreached: 0 too big: 0	<ul style="list-style-type: none"> <li>■ Number of packets with error codes</li> </ul>
hopcount exceeded: 0	<ul style="list-style-type: none"> <li>■ Number of packets whose destination is unreachable</li> </ul>
reassemble timeout: 0	
parameter problem: 0	<ul style="list-style-type: none"> <li>■ Number of too large packets</li> </ul>
unknown error type: 0	<ul style="list-style-type: none"> <li>■ Number of packets exceeding the hop limit</li> </ul>
echoed: 0 echo replied: 0	<ul style="list-style-type: none"> <li>■ Number of packets whose fragmentation and reassembly times out</li> </ul>
neighbor solicit: 0 neighbor advert: 0	
router solicit: 0 router advert 0	<ul style="list-style-type: none"> <li>■ Number of packets with parameter errors</li> </ul>
redirected: 0	<ul style="list-style-type: none"> <li>■ Number of packets with unknown errors</li> </ul>
router renumbering 0	<ul style="list-style-type: none"> <li>■ Number of request packets</li> </ul>
unknown info type: 0	<ul style="list-style-type: none"> <li>■ Number of response packets</li> </ul>
Deliver failed:	<ul style="list-style-type: none"> <li>■ Number of neighbor solicitation messages</li> </ul>
bad length: 0 ratelimited: 0	<ul style="list-style-type: none"> <li>■ Number of neighbor advertisement packets</li> <li>■ Number of router solicitation packets</li> <li>■ Number of router advertisement packets</li> <li>■ Number of redirected packets</li> <li>■ Number of packets recounted by the router</li> <li>■ Number of unknown type of packets</li> <li>■ Number of packets with a incorrect size</li> <li>■ Number of packets failing to be received because of rate limitation</li> </ul>

---

## display tcp ipv6 statistics

**Syntax** `display tcp ipv6 statistics`

**View** Any view

**Parameters** None

**Description** Use the **display tcp ipv6 statistics** command to display IPv6 TCP connection statistics.

**Examples** # Display the statistics of IPv6 TCP connections.

```
<Sysname> display tcp ipv6 statistics
Received packets:
 Total: 0
 packets in sequence: 0 (0 bytes)
 window probe packets: 0, window update packets: 0
 checksum error: 0, offset error: 0, short error: 0
```

```

duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
out-of-order packets: 0 (0 bytes)
packets with data after window: 0 (0 bytes)
packets after close: 0

```

```

ACK packets: 0 (0 bytes)
duplicate ACK packets: 0, too much ACK packets: 0

```

Sent packets:

```

Total: 0
urgent packets: 0
control packets: 0 (including 0 RST)
window probe packets: 0, window update packets: 0

```

```

data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes)
ACK only packets: 0 (0 delayed)

```

```

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, keepalive timeout, so connections disconnected : 0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)

```

**Table 148** Description on fields of the display tcp ipv6 statistics command

Field	Description
Received packets:	Statistics of received packets, including
Total: 0	<ul style="list-style-type: none"> <li>■ Total number of received packets</li> </ul>
packets in sequence: 0 (0 bytes)	<ul style="list-style-type: none"> <li>■ Number of packets received in sequence</li> </ul>
window probe packets: 0	<ul style="list-style-type: none"> <li>■ Number of window probe packets</li> </ul>
window update packets: 0	<ul style="list-style-type: none"> <li>■ Number of window size update packets</li> </ul>
checksum error: 0	<ul style="list-style-type: none"> <li>■ Number of packets with checksum errors</li> </ul>
offset error: 0	<ul style="list-style-type: none"> <li>■ Number of packets with offset errors</li> </ul>
short error: 0	<ul style="list-style-type: none"> <li>■ Number of packets whose total length is less than specified by the packet header</li> </ul>
duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)	<ul style="list-style-type: none"> <li>■ Number of duplicate packets</li> </ul>
out-of-order packets: 0 (0 bytes)	<ul style="list-style-type: none"> <li>■ Number of partially duplicate packets</li> </ul>
packets with data after window: 0 (0 bytes)	<ul style="list-style-type: none"> <li>■ Number of out-of-order packets</li> </ul>
packets after close: 0	<ul style="list-style-type: none"> <li>■ Number of packets exceeding the size of the receiving window</li> </ul>
ACK packets: 0 (0 bytes)	<ul style="list-style-type: none"> <li>■ Number of packets received after the connection is closed</li> </ul>
duplicate ACK packets: 0	<ul style="list-style-type: none"> <li>■ Number of ACK packets</li> </ul>
too much ACK packets: 0	<ul style="list-style-type: none"> <li>■ Number of duplicate ACK packets</li> <li>■ Number of excessive ACK packets</li> </ul>

**Table 148** Description on fields of the display tcp ipv6 statistics command

Field	Description
Sent packets:	Statistics of sent packets, including
Total: 0	■ Total number of packets
urgent packets: 0	■ Number of packets containing an urgent indicator
control packets: 0 (including 0 RST)	■ Number of control packets
window probe packets: 0	■ Number of window probe packets
window update packets: 0	■ Number of window update packets
data packets: 0 (0 bytes) data	■ Number of data packets
packets retransmitted: 0 (0 bytes)	■ Number of retransmitted packets
ACK only packets: 0 (0 delayed)	■ Number of ACK packets
Retransmitted timeout	Number of packets whose retransmission times out
connections dropped in retransmitted timeout	Number of connections dropped because of retransmission timeout
Keepalive timeout	Number of keepalive timeouts
keepalive probe	Number of keepalive probes
Keepalive timeout, so connections disconnected	Number of connections dropped because of keepalive response timeout
Initiated connections	Number of initiated connections
accepted connections	Number of accepted connections
established connections	Number of established connections
Closed connections	Number of closed connections
dropped	Number of dropped connections (after SYN is received from the peer)
initiated dropped	Number of initiated but dropped connections (before SYN is received from the peer)

---

## display tcp ipv6 status

**Syntax** `display tcp ipv6 status`

**View** Any view

**Parameters** None

**Description** Use the **display tcp ipv6** command to display the IPv6 TCP connection status.

**Examples** # Display the IPv6 TCP connection status.

```
<Sysname> display tcp ipv6 status
TCP6CB Local Address Foreign Address State
045d8074 ::->21 ::->0 Listening
```

**Table 149** Description on fields of the display tcp ipv6 status command

Field	Description
TCP6CB	IPv6 address of the TCP control block (hexadecimal)
Local Address	Local IPv6 address and port number
Foreign Address	Remote IPv6 address and port number
State	IPv6 TCP connection status, including <ul style="list-style-type: none"> <li>■ Closed</li> <li>■ Listening</li> <li>■ Syn_Sent</li> <li>■ Syn_Rcvd</li> <li>■ Established</li> <li>■ Close_Wait</li> <li>■ Fin_Wait1</li> <li>■ Closing</li> <li>■ Last_Ack</li> <li>■ Fin_Wait2</li> <li>■ Time_Wait</li> </ul>

---

## display udp ipv6 statistics

**Syntax** `display udp ipv6 statistics`

**View** Any view

**Parameters** None

**Description** Use the **display udp ipv6 statistics** command to display statistics of IPv6 UDP packets.

**Examples** # Display statistics information of IPv6 UDP packets.

```
<Sysname> display udp ipv6 statistics
Received packets:
 Total: 0
 checksum error: 0
 shorter than header: 0, data length larger than packet: 0
 unicast(no socket on port): 0
 broadcast/multicast(no socket on port): 0
 not delivered, input socket full: 0
 input packets missing pcb cache: 0
Sent packets:
 Total: 0
```

**Table 150** Description on fields of the display udp ipv6 statistics command

Field	Description
Total	Total number of received/sent packets
checksum error	Total number of packets with a checksum error

**Table 150** Description on fields of the display udp ipv6 statistics command

Field	Description
shorter than header	Total number of IPv6 UDP packets whose total length is less than specified by the packet header
data length larger than packet	Total number of packets whose data length exceeds that specified by the packet header
unicast(no socket on port)	Total number of unicast packets without any socket received on a port
broadcast/multicast(no socket on port)	Total number of broadcast/multicast packets without any socket received on a port
not delivered, input socket full	Number of packets not handled because of the receive buffer being full
input packet missing pcb cache	Number of packets failing to match the PCB cache

---

## dns server ipv6

**Syntax** **dns server ipv6** *ipv6-address* [ *interface-type interface-number* ]

**undo dns server ipv6** *ipv6-address* [ *interface-type interface-number* ]

**View** System view

**Parameters** *ipv6-address*: IPv6 address of a DNS server.

*interface-type interface-number*: Specifies an interface. When the IPv6 address of the DNS server is a link-local address, this argument must be specified.

**Description** Use the **dns server ipv6** command to configure an IPv6 address for a DNS server.

Use the **undo dns server ipv6** command to remove the configured DNS server.

By default, no DNS server is configured.

**Examples** # Configure the IPv6 address 2002::1 for a DNS server.

```
<Sysname> system-view
[Sysname] dns server ipv6 2002::1
```

---

## ipv6

**Syntax** **ipv6**

**undo ipv6**

**View** System view

**Parameters** None

**Description** Use the **ipv6** command to enable the IPv6 packet forwarding function.

Use the **undo ipv6** command to disable the IPv6 packet forwarding function.

By default, the IPv6 packet forwarding function is disabled.

**Examples** # Enable the IPv6 packet forwarding function.

```
<Sysname> system-view
[Sysname] ipv6
```

---

## ipv6 address

**Syntax** **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

**undo ipv6 address** [ *ipv6-address prefix-length* | *ipv6-address/prefix-length* ]

**View** Interface view

**Parameters** *ipv6-address*: IPv6 address.

*prefix-length*: Prefix length of an IPv6 address, in the range 1 to 128.

**Description** Use the **ipv6 address** command to configure an IPv6 site-local address or aggregatable global unicast address for an interface.

Use the **undo ipv6 address** command to remove the IPv6 address from the interface.

By default, no site-local address or global unicast address is configured for an interface.

Note that except the link-local address automatically configured, all IPv6 addresses will be removed from the interface if you carry out the **undo ipv6 address** command without any parameter specified.

**Examples** # Set the aggregatable global IPv6 unicast address of VLAN-interface 100 to 2001::1/64.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64
```

---

## ipv6 address auto link-local

**Syntax** **ipv6 address auto link-local**

**undo ipv6 address auto link-local**

**View** Interface view

**Parameters** None

**Description** Use the **ipv6 address auto link-local** command to automatically generate a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically generated link-local address for an interface.

By default, a link-local address will automatically be generated after a site-local or global IPv6 unicast address is configured for an interface.

**Examples** # Configure VLAN-interface 100 to automatically generate a link-local address.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto link-local
```

## ipv6 address eui-64

**Syntax** **ipv6 address** *ipv6-address/prefix-length* **eui-64**

**undo ipv6 address** *ipv6-address/prefix-length* **eui-64**

**View** Interface view

**Parameters** *ipv6-address/prefix-length*: IPv6 address and IPv6 prefix. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an IPv6 address in the EUI-64 format.

**Description** Use the **ipv6 address eui-64** command to configure a site-local address or global unicast address in the EUI-64 format for an interface.

Use the **undo ipv6 address eui-64** command to remove the configured site-local address or global unicast address in the EUI-64 format for an interface.

By default, no site-local or global unicast address in EUI-64 format is configured for an interface.

**Examples** # Configure an IPv6 address in EUI-64 format for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

## ipv6 address link-local

**Syntax** **ipv6 address** *ipv6-address* **link-local**

**undo ipv6 address** *ipv6-address* **link-local**



<b>View</b>	Interface view
<b>Parameters</b>	<i>ipv6-address</i> : IPv6 link-local address. The first ten bits of an address must be 1111111010 (binary), that is, the first group of hexadecimal in the address must be FE80 to FEBF.
<b>Description</b>	Use the <b>ipv6 address link-local</b> command to configure a link-local address manually for a specified interface. Use the <b>undo ipv6 address link-local</b> command to remove the configured link-local address for an interface.
<b>Examples</b>	<pre># Configure a link-local address for VLAN-interface 100.  &lt;Sysname&gt; system-view [Sysname] interface vlan-interface 100 [Sysname-Vlan-interface100] ipv6 address fe80::1 link-local</pre>

---

## ipv6 host

<b>Syntax</b>	<pre><b>ipv6 host</b> <i>hostname</i> <i>ipv6-address</i> <b>undo ipv6 host</b> <i>hostname</i> [ <i>ipv6-address</i> ]</pre>
<b>View</b>	System view
<b>Parameters</b>	<p><i>hostname</i>: Host name, a string of up to 20 characters. The character string can contain letters, numerals, "_", "-", or "." and must contain at least one letter.</p> <p><i>ipv6-address</i>: IPv6 address.</p>
<b>Description</b>	<p>Use the <b>ipv6 host</b> command to configure the mappings between host names and IPv6 addresses.</p> <p>Use the <b>undo ipv6 host</b> command to remove the mappings between host names and IPv6 addresses.</p> <p>Each host name can correspond to only one IPv6 address.</p>
<b>Examples</b>	<pre># Configure the mapping between a host name and an IPv6 address.  &lt;Sysname&gt; system-view [Sysname] ipv6 host aaa 2001::1</pre>

---

## ipv6 icmp-error

<b>Syntax</b>	<pre><b>ipv6 icmp-error</b> { <b>bucket</b> <i>bucket-size</i>   <b>ratelimit</b> <i>interval</i> } *</pre> <pre><b>undo ipv6 icmp-error</b></pre>
<b>View</b>	System view

**Parameters** **bucket** *bucket-size*: Number of tokens in a token bucket, in the range of 1 to 200.

**ratelimit** *interval*: Update period of the token bucket in milliseconds, in the range of 0 to 2,147,483,647. The update period "0" indicates that the number of ICMPv6 error packets sent is not restricted.

**Description** Use the **ipv6 icmp-error** command to configure the size and update period of the token bucket.

Use the **undo ipv6 icmp-error** command to restore the defaults.

By default, the size is 10 and the update period is 100 milliseconds. That is, at most 10 IPv6 ICMP error packets can be sent within these 100 milliseconds.

**Examples** # Set the capacity of the token bucket to 50 and the update period to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ipv6 icmp-error bucket 50 ratelimit 100
```

## ipv6 icmpv6 multicast-echo-reply enable

**Syntax** **ipv6 icmpv6 multicast-echo-reply enable**

**undo ipv6 icmpv6 multicast-echo-reply**

**View** System view

**Parameters** None

**Description** Use the **ipv6 icmpv6 multicast-echo-reply enable** command to enable sending of multicast echo replies.

Use the **undo ipv6 icmpv6 multicast-echo-reply** command to disable sending of multicast echo replies.

By default, the device is disabled from sending multicast echo replies.

**Examples** # Enable sending of multicast echo replies.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

## ipv6 nd autoconfig managed-address-flag

**Syntax** **ipv6 nd autoconfig managed-address-flag**

**undo ipv6 nd autoconfig managed-address-flag**

**View** Interface view

<b>Parameters</b>	None
<b>Description</b>	<p>Use the <b>ipv6 nd autoconfig managed-address-flag</b> command to set the managed address configuration (M) flag to 1 so that the host can acquire an IPv6 address through stateful auto-configuration (for example, DHCP server).</p> <p>Use the <b>undo ipv6 nd autoconfig managed-address-flag</b> command to restore the M flag to the default value "0" so that the host can acquire an IPv6 address through stateless auto-configuration.</p> <p>By default, the M flag is set to "0".</p>
<b>Examples</b>	<pre># Configure the host to acquire an IPv6 address through stateful auto-configuration.  &lt;Sysname&gt; system-view [Sysname] interface vlan-interface 100 [Sysname-Vlan-interface100] ipv6 nd autoconfig managed-address-flag</pre>

---

### ipv6 nd autoconfig other-flag

<b>Syntax</b>	<pre><b>ipv6 nd autoconfig other-flag</b> <b>undo ipv6 nd autoconfig other-flag</b></pre>
<b>View</b>	Interface view
<b>Parameters</b>	None
<b>Description</b>	<p>Use the <b>ipv6 nd autoconfig other-flag</b> command to set the other stateful configuration flag (O) flag to 1 so that the host can acquire information other than IPv6 address through stateful auto-configuration (for example, DHCP server).</p> <p>Use the <b>undo ipv6 nd autoconfig other-flag</b> command to remove the setting so that the host can acquire other information through stateless auto-configuration.</p> <p>By default, the O flag is set to "0".</p>
<b>Examples</b>	<pre># Configure the host to acquire information other than IPv6 address through stateless auto-configuration.  &lt;Sysname&gt; system-view [Sysname] interface vlan-interface 100 [Sysname-Vlan-interface100] undo ipv6 nd autoconfig other-flag</pre>

---

### ipv6 nd dad attempts

<b>Syntax</b>	<pre><b>ipv6 nd dad attempts</b> <i>value</i> <b>undo ipv6 nd dad attempts</b></pre>
---------------	--------------------------------------------------------------------------------------

<b>View</b>	Interface view
<b>Parameters</b>	<i>value</i> : Number of attempts to send a neighbor solicitation message for DAD, in the range of 0 to 600. The default value is "1". When it is set to 0, the DAD is disabled.
<b>Description</b>	Use the <b>ipv6 nd dad attempts</b> command to configure the number of attempts to send a neighbor solicitation message for DAD.  Use the <b>undo ipv6 nd dad attempts</b> command to restore the default.  By default, the number of attempts to send a neighbor solicitation message for DAD is 1.
<b>Examples</b>	# Set the number of attempts to send a neighbor solicitation message for DAD to 20.  <pre>&lt;Sysname&gt; system-view [Sysname] interface vlan-interface 100 [Sysname-Vlan-interface100] ipv6 nd dad attempts 20</pre>

## ipv6 nd hop-limit

<b>Syntax</b>	<b>ipv6 nd hop-limit</b> <i>value</i>  <b>undo ipv6 nd hop-limit</b>
<b>View</b>	System view
<b>Parameters</b>	<i>value</i> : Number of hops, in the range of 0 to 255. When it is set to 0, the Cur Hop Limit field in RA messages sent by the device is 0. That is, the number of hops is determined by the host itself, but not specified by the device.
<b>Description</b>	Use the <b>ipv6 nd hop-limit</b> command to configure the hop limit advertised by the device.  Use the <b>undo ipv6 nd hop-limit</b> command to restore the default hop limit.  By default, the hop limit advertised by the device is 64.
<b>Examples</b>	# Set the hop limit advertised by the device to 100.  <pre>&lt;Sysname&gt; system-view [Sysname] ipv6 nd hop-limit 100</pre>

## ipv6 nd ns retrans-timer

<b>Syntax</b>	<b>ipv6 nd ns retrans-timer</b> <i>value</i>  <b>undo ipv6 nd ns retrans-timer</b>
---------------	------------------------------------------------------------------------------------------

<b>View</b>	Interface view
<b>Parameters</b>	<i>value</i> : Interval for sending NS messages in milliseconds, in the range of 1,000 to 4,294,967,295.
<b>Description</b>	<p>Use the <b>ipv6 nd ns retrans-timer</b> command to set the interval for sending NS messages. The local interface sends NS messages at intervals of this value. Furthermore, the Retrans Timer field in RA messages sent by the local interface is equal to this value.</p> <p>Use the <b>undo ipv6 nd ns retrans-timer</b> command to restore the default interval.</p> <p>By default, the local interface sends NS messages at intervals of 1,000 milliseconds and the Retrans Timer field in RA messages sent by the local interface is 0.</p>
<b>Examples</b>	<p># Specify VLAN-interface 100 to send NS messages at intervals of 10,000 milliseconds.</p> <pre>&lt;Sysname&gt; system-view [Sysname] interface vlan-interface 100 [Sysname-Vlan-interface100] ipv6 nd ns retrans-timer 10000</pre>

---

## ipv6 nd nud reachable-time

<b>Syntax</b>	<b>ipv6 nd nud reachable-time</b> <i>value</i> <b>undo ipv6 nd nud reachable-time</b>
<b>View</b>	Interface view
<b>Parameters</b>	<i>value</i> : Neighbor reachable time in milliseconds, in the range of 1 to 3,600,000.
<b>Description</b>	<p>Use the <b>ipv6 nd nud reachable-time</b> command to configure the neighbor reachable time on an interface. This time value serves as not only the neighbor reachable time on the local interface, but also the value of the Reachable Timer field in RA messages sent by the local interface.</p> <p>Use the <b>undo ipv6 nd nud reachable-time</b> command to restore the default neighbor reachable time and to specify the value of the Reachable Timer field in RA messages as 0 so that the number of hops is determined by the host itself, but not specified by the device.</p> <p>By default, the neighbor reachable time on the local interface is 30,000 milliseconds and the Reachable Timer field in RA messages is 0.</p>
<b>Examples</b>	<p># Set the neighbor reachable time on VLAN-interface 100 to 10,000 milliseconds.</p> <pre>&lt;Sysname&gt; system-view [Sysname] interface vlan-interface 100 [Sysname-Vlan-interface100] ipv6 nd nud reachable-time 10000</pre>

---

## ipv6 nd ra halt

<b>Syntax</b>	<b>ipv6 nd ra halt</b> <b>undo ipv6 nd ra halt</b>
<b>View</b>	Interface view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>ipv6 nd ra halt</b> command to suppress RA messages. Use the <b>undo ipv6 nd ra halt</b> command to disable the RA message suppression. By default, RA messages are suppressed.
<b>Examples</b>	# Suppress RA messages on VLAN-interface 100. <pre>&lt;Sysname&gt; system-view [Sysname] interface vlan-interface 100 [Sysname-Vlan-interface100] ipv6 nd ra halt</pre>

---

## ipv6 nd ra interval

<b>Syntax</b>	<b>ipv6 nd ra interval</b> <i>max-interval-value</i> <i>min-interval-value</i> <b>undo ipv6 nd ra interval</b>
<b>View</b>	Interface view
<b>Parameters</b>	<i>max-interval-value</i> : Maximum interval for advertising RA messages in seconds, in the range of 4 to 1,800. <i>min-interval-value</i> : Minimum interval for advertising RA messages in seconds, in the range of 3 to 1,350.
<b>Description</b>	Use the <b>ipv6 nd ra interval</b> command to set the maximum and minimum interval for advertising RA messages. The device advertises RA messages at intervals of a random value between the maximum interval and the minimum interval. Use the <b>undo ipv6 nd ra interval</b> command to restore the default. By default, the maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds. Note the following: <ul style="list-style-type: none"><li>■ The minimum interval should be three-fourths of the maximum interval or less.</li></ul>

- The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

**Examples** # Set the maximum interval for advertising RA messages to 1,000 seconds and the minimum interval to 700 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra interval 1000 700
```

---

## ipv6 nd ra prefix

**Syntax** **ipv6 nd ra prefix** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } *valid-lifetime preferred-lifetime* [ **no-autoconfig** | **off-link** ] \*

**undo ipv6 nd ra prefix** *ipv6-prefix*

**View** Interface view

**Parameters** *ipv6-address*: IPv6 address or IPv6 address prefix.

*prefix-length*: Prefix length of an IPv6 address.

*ipv6-prefix*: IPv6 address prefix.

*valid-lifetime*: Valid lifetime of a prefix in seconds, in the range of 0 to 4,294,967,295.

*preferred-lifetime*: Preferred lifetime of a prefix used for stateless auto-configuration in seconds, in the range of 0 to 4,294,967,295.

**no-autoconfig**: Specifies a prefix not to be used for stateless auto-configuration. If this keyword is not provided, the prefix is used for stateless auto-configuration.

**off-link**: Specifies the address with the prefix not to be directly reachable on the link. If this keyword is not provided, the address with the prefix is directly reachable on the link.

**Description** Use the **ipv6 nd ra prefix** command to configure the prefix information in RA messages.

Use the **undo ipv6 nd ra prefix** command to remove the prefix information from RA messages.

By default, no prefix information is configured in RA messages and the IPv6 address of the interface sending RA messages is used as the prefix information.

**Examples** # Configure the prefix information for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

---

**ipv6 nd ra router-lifetime**

**Syntax** **ipv6 nd ra router-lifetime** *value*

**undo ipv6 nd ra router-lifetime**

**View** Interface view

**Parameters** *value*: Router lifetime in seconds, in the range of 0 to 9,000. When it is set to 0, the device does not serve as the default router.

**Description** Use the **ipv6 nd ra router-lifetime** command to configure the router lifetime in RA messages.

Use the **undo ipv6 nd ra router-lifetime** command to restore the default configuration.

By default, the router lifetime in RA messages is 1,800 seconds.

Note that the router lifetime in RA messages should be greater than or equal to the advertising interval.

**Examples** # Set the router lifetime in RA messages on VLAN-interface 100 to 1,000 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

---

**ipv6 neighbor**

**Syntax** **ipv6 neighbor** *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

**undo ipv6 neighbor** *ipv6-address interface-type interface-number*

**View** System view

**Parameters** *ipv6-address*: IPv6 address in a static neighbor entry.

*mac-address*: Link layer address in a static neighbor entry (48 bits long, in the format of H-H-H).

*vlan-id*: VLAN ID in a static neighbor entry, in the range of 1 to 4094.

*port-type port-number*: Type and number of a Layer 2 port in a static neighbor entry.

**interface** *interface-type interface-number*: Type and number of a Layer 3 interface in a static neighbor entry.



- Description** Use the **ipv6 neighbor** command to configure a static neighbor entry.
- Use the **undo ipv6 neighbor** command to remove a static neighbor entry.
- Note that you can adopt the IPv6 address and link layer address of the Layer 3 VLAN interface or those of the VLAN port to configure a static neighbor entry.
- If a static neighbor entry is configured by using the first method, the neighbor entry is in the INCMP state. After the device obtains the corresponding Layer 2 VLAN port information through resolution, the neighbor entry will go into the REACH state.
  - If a static neighbor entry is configured by using the second method, the corresponding VLAN interface must exist and the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id*. After a static neighbor entry is configured, the device will relate the VLAN interface with the IPv6 address to identify a static neighbor entry uniquely and the entry will be in the REACH state.
- You only need to specify the corresponding VLAN interface before removing a static neighbor entry.

**Examples** # Configure a static neighbor entry for layer 2 port Ethernet 3/0/1 of VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 100 ethernet 3/0/1
```

---

## ipv6 neighbors max-learning-num

**Syntax** **ipv6 neighbors max-learning-num** *number*

**undo ipv6 neighbors max-learning-num**

**View** Interface view

**Parameters** *number*: Maximum number of neighbors that can be dynamically learned by an interface, in the range 1 to 2048.

**Description** Use the **ipv6 neighbors max-learning-num** command to configure the maximum number of neighbors that can be dynamically learned on a specified interface.

Use the **undo ipv6 neighbors max-learning-num** command to restore the default.

**Examples** # Set the maximum number of neighbors that can be dynamically learned on VLAN-interface 100 to 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

---

**ipv6 pathmtu**

**Syntax** `ipv6 pathmtu ipv6-address [ value ]`

`undo ipv6 pathmtu ipv6-address`

**View** System view

**Parameters** *ipv6-address*: Specified IPv6 address.

*value*: PMTU of a specified IPv6 address in bytes. The value range and the default value vary with devices. It ranges from 1280 to 10000.

**Description** Use the **ipv6 pathmtu** command to configure a static PMTU for a specified IPv6 address.

Use the **undo ipv6 pathmtu** command to remove the PMTU configuration for a specified IPv6 address.

By default, no static PMTU is configured.

**Examples** # Configure a static PMTU for a specified IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

---

**ipv6 pathmtu age**

**Syntax** `ipv6 pathmtu age age-time`

`undo ipv6 pathmtu age`

**View** System view

**Parameters** *age-time*: Aging time for PMTU in minutes, in the range of 10 to 100.

**Description** Use the **ipv6 pathmtu age** command to configure the aging time for a dynamic PMTU.

Use the **undo ipv6 pathmtu age** command to restore the default.

By default, the aging time is 10 minutes.

Note that the aging time is invalid for a static PMTU.

**Related commands:** **display ipv6 pathmtu.**

**Examples** # Set the aging time for a dynamic PMTU to 40 minutes.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

---

## reset dns ipv6 dynamic-host

**Syntax** `reset dns ipv6 dynamic-host`

**View** User view

**Parameters** None

**Description** Use the **reset dns ipv6 dynamic-host** command to clear IPv6 dynamic domain name cache information.

**Examples** # Clear IPv6 dynamic domain name cache information.  

```
<Sysname> reset dns ipv6 dynamic-host
```

---

## reset ipv6 neighbors

**Syntax** `reset ipv6 neighbors { all | dynamic | interface interface-type interface-number | slot slot-number | static }`

**View** User view

**Parameters** **all**: Clears the static and dynamic neighbor information on all interfaces.

**dynamic**: Clears the dynamic neighbor information on all interfaces.

**interface** *interface-type interface-number*: Clears dynamic neighbor information on a specified interface.

**slot** *slot-number*: Clears the dynamic neighbor information on a specified slot.

**static**: Clears the static neighbor information on all interfaces.

**Description** Use the **reset ipv6 neighbors** command to clear IPv6 neighbor information.

**Examples** # Clear neighbor information on all interfaces.  

```
<Sysname> reset ipv6 neighbors all
```

---

## reset ipv6 pathmtu

**Syntax** `reset ipv6 pathmtu { all | static | dynamic }`

**View** User view

<b>Parameters</b>	<p><b>all:</b> Clears all PMTUs.</p> <p><b>static:</b> Clears all static PMTUs.</p> <p><b>dynamic:</b> Clears all dynamic PMTUs.</p>
<b>Description</b>	Use the <b>reset ipv6 pathmtu</b> the command to clear the PMTU information.
<b>Examples</b>	<pre># Clear all PMTUs. &lt;Sysname&gt; reset ipv6 pathmtu all</pre>

### reset ipv6 statistics

<b>Syntax</b>	<b>reset ipv6 statistics</b> [ <b>slot</b> <i>slot-number</i> ]
<b>View</b>	User view
<b>Parameters</b>	<b>slot</b> <i>slot number</i> : Clears the statistics of IPv6 packets and ICMPv6 packets on the slot.
<b>Description</b>	Use the <b>reset ipv6 statistics</b> command to clear the statistics of IPv6 packets and ICMPv6 packets.
<b>Examples</b>	<pre># Clear the statistics of IPv6 packets and ICMPv6 packets. &lt;Sysname&gt; reset ipv6 statistics</pre>

### reset tcp ipv6 statistics

<b>Syntax</b>	<b>reset tcp ipv6 statistics</b>
<b>View</b>	User view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>reset tcp ipv6 statistics</b> command to clear the statistics of all IPv6 TCP connections.
<b>Examples</b>	<pre># Clear the statistics of all IPv6 TCP connections. &lt;Sysname&gt; reset tcp ipv6 statistics</pre>

### reset udp ipv6 statistics

<b>Syntax</b>	<b>reset udp ipv6 statistics</b>
---------------	----------------------------------

<b>View</b>	User view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>reset udp ipv6 statistics</b> command to clear the statistics of all IPv6 UDP packets.
<b>Examples</b>	# Clear the statistics of all IPv6 UDP packets. <pre>&lt;Sysname&gt; reset udp ipv6 statistics</pre>

---

### tcp ipv6 timer fin-timeout

<b>Syntax</b>	<b>tcp ipv6 timer fin-timeout</b> <i>wait-time</i>  <b>undo tcp ipv6 timer fin-timeout</b>
<b>View</b>	System view
<b>Parameters</b>	<i>wait-time</i> : Length of the finwait timer for IPv6 TCP connections in seconds, in the range of 76 to 3,600.
<b>Description</b>	Use the <b>tcp ipv6 timer fin-timeout</b> command to set the finwait timer for IPv6 TCP connections  Use the <b>undo tcp ipv6 timer fin-timeout</b> command to restore the default finwait timer length.  By default, the length of the finwait timer is 675 seconds.
<b>Examples</b>	# Set the finwait timer length of IPv6 TCP connections to 800 seconds. <pre>&lt;Sysname&gt; system-view [Sysname] tcp ipv6 timer fin-timeout 800</pre>

---

### tcp ipv6 timer syn-timeout

<b>Syntax</b>	<b>tcp ipv6 timer syn-timeout</b> <i>wait-time</i>  <b>undo tcp ipv6 timer syn-timeout</b>
<b>View</b>	System view
<b>Parameters</b>	<i>wait-time</i> : Length of the synwait timer for IPv6 TCP connections in seconds, in the range of 2 to 600.
<b>Description</b>	Use the <b>tcp ipv6 timer syn-timeout</b> command to set the synwait timer for IPv6 TCP connections

Use the **undo tcp ipv6 timer syn-timeout** command to restore the default synwait timer length.

By default, the length of the synwait timer of IPv6 TCP connections is 75 seconds.

**Examples** # Set the synwait timer length of IPv6 TCP connections to 100 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer syn-timeout 100
```

## tcp ipv6 window

**Syntax** **tcp ipv6 window** *size*

**undo tcp ipv6 window**

**View** System view

**Parameters** *size*: Size of the IPv6 TCP sending/receiving buffer in KB (kilobyte), in the range of 1 to 32.

**Description** Use the **tcp ipv6 window** command to set the size of the IPv6 TCP sending/receiving buffer.

Use the **undo tcp ipv6 window** command to restore the default.

By default, the size of the IPv6 TCP sending/receiving buffer is 8 KB.

**Examples** # Set the size of the IPv6 TCP sending/receiving buffer to 4 KB.

```
<Sysname> system-view
[Sysname] tcp ipv6 window 4
```

# 36

## IPv6 DUAL STACK CONFIGURATION COMMANDS

---

### ipv6

**Syntax** **ipv6**  
**undo ipv6**

**View** System view

**Parameters** None

**Description** Use the **ipv6** command to enable the IPv6 packet forwarding function.  
Use the **undo ipv6** command to disable the IPv6 packet forwarding function.  
By default, the function is disabled.

**Examples** # Enable the IPv6 packet forwarding function.  

```
<Sysname> system-view
[Sysname] ipv6
```

---

### ipv6 address

**Syntax** **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }  
**undo ipv6 address** [ *ipv6-address prefix-length* | *ipv6-address/prefix-length* ]

**View** Interface view

**Parameters** *ipv6-address*: IPv6 address for the interface.  
*prefix-length*: Length of the prefix in bits, in the range of 1 to 128.

**Description** Use the **ipv6 address** command to configure a site-local address or global unicast address for an interface.  
Use the **undo ipv6 address** command to remove the configuration.  
By default, neither site-local addresses nor global unicast addresses are configured.

Note that:

- Up to seven global unicast addresses and site-local addresses can be configured on an interface in total.
- The **undo ipv6 address** command without parameters removes all IPv6 addresses manually configured, except link-local addresses automatically configured on the interface.

**Examples** # Specify the global unicast address of the interface VLAN-interface 100 as 2001::1/64.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64
```

## ipv6 address auto link-local

**Syntax** **ipv6 address auto link-local**  
**undo ipv6 address auto link-local**

**View** Interface view

**Parameters** None

**Description** Use the **ipv6 address auto link-local** command to enable the device to automatically generate a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically generated link-local address.

By default, a link-local address will automatically be generated when an IPv6 site-local address or IPv6 global unicast address is configured for an interface.

**Examples** # Enable the interface VLAN-interface 100 to generate a link-local address automatically.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto link-local
```

## ipv6 address eui-64

**Syntax** **ipv6 address ipv6-address/prefix-length eui-64**  
**undo ipv6 address ipv6-address/prefix-length eui-64**

**View** Ethernet interface view



- Parameters** *ipv6-address/prefix-length*: IPv6 address and prefix length. They together specify the prefix length of an IPv6 address in the EUI-64 format. The prefix length of an EUI-64 address ranges from 1 to 64.
- Description** Use the **ipv6 address eui-64** command to configure a site-local address or global unicast address in the EUI-64 format on an interface.
- Use the **undo ipv6 address eui-64** command to delete the site-local address or global unicast address in the EUI-64 format on an interface.
- By default, no site-local or global unicast address in the EUI-64 format is configured for an interface.
- Examples** # Configure the interface VLAN-interface 100 to generate an IPv6 address in the EUI-64 format.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

ipv6 address link-local

- Syntax** **ipv6 address** *ipv6-address* **link-local**
- undo ipv6 address** *ipv6-address* **link-local**
- View** Interface view
- Parameters** *ipv6-address*: IPv6 link-local address. The high-order ten bits of an IPv6 link-local address must be 111111010 (binary), that is to say, the first group of the IPv6 link-local address must range from FE80 to FEBF (hexadecimal).
- Description** Use the **ipv6 address link-local** command to configure manually a link-local address for an interface.
- Use the **undo ipv6 address link-local** command to remove the link-local address of an interface.
- By default, a link-local address will automatically be generated when an IPv6 site-local address or global unicast address is configured for an interface.
- Examples** # Configure a link-local address on the interface VLAN-interface 100.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address fe80::1 link-local
```



# 37

## IPv6 TUNNELING CONFIGURATION COMMANDS

---

### aggregation-group

**Syntax** `aggregation-group aggregation-group-id`

`undo aggregation-group`

**View** Tunnel interface view

**Parameters** *aggregation-group-id*: Link aggregation group ID. The value ranges from 1 to 484.

**Description** Use the **aggregation-group** command to reference a link aggregation group.

Use the **undo aggregation-group** command to remove the link aggregation group referenced by the tunnel.

By default, a tunnel does not reference any link aggregation group.

Before specifying a link aggregation group for a tunnel in tunnel interface view, you have configured the manual link aggregation group and set the service type of the link aggregation group to tunnel in system view.

Make sure the ports in the manual link aggregation group are not up, and STP is disabled.

One tunnel interface can reference only one link aggregation group.

**Related commands:** **link-aggregation group description, link-aggregation group mode, link-aggregation group service-type.**

**Examples** # Create link aggregation group 1, and set the configuration mode to manual and the service type to tunnel.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode manual
[Sysname] link-aggregation group 1 service-type tunnel
```

# Add a layer 2 Ethernet interface to link aggregation group 1.

```
[Sysname] interface ethernet 3/0/1
[Sysname-Ethernet3/0/1] stp disable
[Sysname-Ethernet3/0/1] port link-aggregation group 1
[Sysname-Ethernet3/0/1] quit
```

```
Configure the tunnel to reference link aggregation group 1 in tunnel interface
view.
```

```
[Sysname] interface tunnel 1/0/3
[Sysname-Tunnel1/0/3] aggregation-group 1
```

---

## destination

**Syntax** **destination** *ip-address*

**undo destination**

**View** Tunnel interface view

**Parameter** *ip-address*: Destination IPv4 address to be specified for the tunnel interface.

**Description** Use the command **destination** to specify the destination address of the tunnel interface.

Use the **undo destination** command to remove the configured destination IP address.

By default, no destination address is configured for the tunnel interface.

Note that:

- The destination address of a tunnel interface is the address of the peer interface receiving packets and is usually the source address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.

**Related command:** **interface tunnel** and **source**.

**Example** # Set VLAN1 (193.101.1.1) of Sysname1 to the source interface and destination interface of a tunnel between two devices, respectively.

```
<Sysname1> system-view
[Sysname1] interface Tunnel 1/0/3
[Sysname1-Tunnel1/0/3] source 193.101.1.1
[Sysname1-Tunnel1/0/3] destination 192.100.1.1
```

# Set VLAN1 (192.100.1.1) of Sysname2 to the source interface and destination interface of a tunnel between two devices, respectively.

```
<Sysname2> system-view
[Sysname2] interface Tunnel 1/0/3
[Sysname2-Tunnel1/0/3] source 192.100.1.1
[Sysname2-Tunnel1/0/3] destination 193.101.1.1
```

---

**display interface tunnel**

**Syntax** **display interface tunnel** [ *number* ]

**View** Any view

**Parameters** *number*: Tunnel interface number. If the *number* argument is not specified, the information of all tunnel interfaces will be displayed.

**Description** Use the **display interface tunnel** command to display related information of a specified tunnel interface, such as source address, destination address, and encapsulation mode.

**Related commands:** **interface tunnel, source, destination, tunnel-protocol.**

**Examples** # Display the information of the interface Tunnel 1/0/3.

```
<Sysname> display interface Tunnell1/0/3
Tunnell1/0/3 current state: UP
Line protocol current state: UP
Description: Tunnell1/0/3 Interface
The Maximum Transmit Unit is 64000
Internet Address is 10.1.2.1/24 Primary
Encapsulation is TUNNEL, aggregation ID not set
Tunnel source 192.13.2.1, destination 192.13.2.2
Tunnel protocol/transport IPv6/IP
 Last 300 seconds input: 0 bytes/sec, 0 packets/sec
 Last 300 seconds output: 0 bytes/sec, 0 packets/sec
 361 packets input, 9953388 bytes
 0 input error
 361 packets output, 30324 bytes
 0 output error
```

**Table 151** Description on fields of the display interface tunnel command

Field	Description
Tunnel1/0/3 current state: UP	The physical layer protocol state of the tunnel interface.
Line protocol current state: UP	The link layer protocol state of the tunnel interface.
Description	Descriptive information of a tunnel interface
Tunnel1/0/3 Interface	Tunnel interface number
Maximum Transmit Unit	Maximum transmission unit (MTU) in a tunnel
Encapsulation is TUNNEL	The encapsulation protocol is tunnel.
Aggregation ID	Link aggregation group ID referenced by a tunnel. If the device supports link aggregation groups, the link aggregation group ID configured in tunnel interface view is displayed. If device does not support, "aggregation ID not set" is displayed.
Tunnel source	Tunnel source address
Destination	Tunnel destination address
Tunnel protocol/transport	Tunnel protocol and transport protocol.
Last 300 seconds input	Number of bytes and packets input per second in the last five minutes.

**Table 151** Description on fields of the display interface tunnel command

Field	Description
Last 300 seconds output	Number of bytes and packets output per second in the last five minutes.
packets input	Total number of input packets.
input error	Number of error packets among all input packets.
packets output	Total number of output packets.
output error	Number of error packets in all output packets

## display ipv6 interface tunnel

**Syntax** `display ipv6 interface tunnel number`

**View** Any view

**Parameters** *number*: Tunnel interface number.

**Description** Use the **display ipv6 interface tunnel** command to display related IPv6 information of a specified tunnel interface, including link state, IPv6 protocol state, and IPv6 address.

**Examples** # Display the information of the interface Tunnel 1/0/3.

```
<Sysname> display ipv6 interface Tunnel1/0/3
Tunnel1/0/3 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::101:101
Global unicast address(es):
 2002:101:101::1, subnet is 2002::/16
Joined group address(es):
 FF02::1:FF01:101
 FF02::1:FF00:1
 FF02::2
 FF02::1
MTU is 1500 bytes
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
```

**Table 152** Description on fields of the display interface tunnel command

Field	Description
Tunnel1/0/3 current state: UP	The physical layer of the tunnel interface is reachable.
Line protocol current state: UP	The link layer of the tunnel interface is reachable.
IPv6 is enabled	Enables IPv6 on a tunnel interface
link-local address	Link-local address of a tunnel interface
Global unicast address(es)	Aggregatable global unicast address of a tunnel interface.
Joined group address(es)	Multicast address of a tunnel interface.
MTU is 1500 bytes	Size of the MTU in a tunnel. The MTU in this example is 1,500 bytes.

**Table 152** Description on fields of the display interface tunnel command

Field	Description
ND reachable time	Neighbor reachable time
ND retransmit interval	Interval for retransmitting a neighbor discovery message.
Hosts use stateless autoconfig for addresses	Hosts use the stateless auto-configuration mode to acquire IPv6 addresses.

---

## interface tunnel

**Syntax** **interface tunnel** *number*  
**undo interface tunnel** *number*

**View** System view

**Parameters** *number*: Tunnel interface number. A tunnel interface number is in the A/B/C format, where A, B, and C represent the slot number of a module, the slot number of a sub-card, and the tunnel interface number, respectively. A and B vary with devices while C ranges from 0 to 1023. The number of tunnels that can be created is restricted to the total number of interfaces and the memory.

**Description** Use the **interface tunnel** command to create a tunnel interface and enter tunnel interface view.

Use the **undo interface tunnel** command to remove a specified tunnel interface.

By default, there is no tunnel interface on the device.

Carry out the **interface tunnel** command to enter interface view of a specified tunnel. If the tunnel interface is not created, you must create it before entering tunnel interface view.

A tunnel interface number has only local significance, and therefore, the same interface number or different interface numbers can be set at both ends of a tunnel.

**Related commands:** **display interface tunnel, source, destination, tunnel-protocol.**

**Examples** # Create the interface Tunnel 1/0/3.  

```
<Sysname> system-view
[Sysname] interface Tunnel1/0/3
[Sysname- Tunnel1/0/3]
```

---

## mtu

**Syntax** **mtu** *mtu-size*

**undo mtu****View** Tunnel interface view**Parameters** *mtu-size*: Tunnel interface MTU in bytes, in the range of 100 to 64,000.**Description** Use the **mtu** command to configure the tunnel interface MTU.  
Use the **undo mtu** command to restore the default tunnel interface MTU.**Examples** # Set the tunnel interface MTU to 10,000 bytes.

```

<Sysname> system-view
[Sysname] interface tunnel 1/0/3
[Sysname-Tunnel1/0/3] mtu 10000

```

**source****Syntax** **source** { *ip-address* | *interface-type interface-number* }**undo source****View** Tunnel interface view**Parameters** *ip-address*: Tunnel source IPv4 address.*interface-type interface-number*: Specifies an interface. The interface types include Vlan-interface, tunnel, and so on.**Description** Use the **source** command to specify the source address for the tunnel interface.  
Use the **undo source** command to remove the configured tunnel source address.  
By default, no tunnel source address is configured.

Note that:

- The tunnel source address is the address of the interface sending packets and is usually the destination address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.

**Related commands:** **interface tunnel, destination.****Examples** # Set the tunnel source address to VLAN-interface 1 on the interface Tunnel 1/0/3.

```

<Sysname> system-view
[Sysname] interface tunnel 1/0/3
[Sysname-Tunnel1/0/3] source 192.100.1.1

```

Or



```

<Sysname> system-view
[Sysname] interface tunnel 1/0/3
[Sysname-Tunnel1/0/3] source Vlan-interface 1

```

---

## tunnel-protocol

**Syntax** **tunnel-protocol** { **ipv6-ipv4** [ **6to4** | **isatap** ] | **mpls te** }  
**undo tunnel-protocol**

**View** Tunnel interface view

**Parameters** **ipv6-ipv4**: Sets the tunnel to an IPv6 over IPv4 tunnel.  
**ipv6-ipv4 6to4**: Sets the tunnel to IPv6 over IPv4 6to4 tunnel.  
**ipv6-ipv4 isatap**: Sets the tunnel to an IPv6 over IPv4 ISATAP tunnel.  
**mpls te**: Sets the tunnel to an MPLS TE tunnel. Now S7900E ethernet switches do not support MPLS TE tunnel.

**Description** Use the **tunnel-protocol** command to configure the tunnel type.  
Use the **undo tunnel-protocol** to restore the tunnel type to the default.

Note that:

- A proper tunnel type can be selected for packet encapsulation according to the network topology and application. The same tunnel type must be configured at both ends of the tunnel. Otherwise, packet delivery will fail.
- Only one automatic tunnel can be configured at the same tunnel source.

**Examples** # Specify the tunnel type as IPv6 over IPv4 for a tunnel interface.

```

<Sysname> system-view
[Sysname] interface tunnel 1/0/3
[Sysname-Tunnel1/0/3] tunnel-protocol ipv6-ipv4

```



# 38

## IGMP SNOOPING CONFIGURATION COMMANDS

---

### display igmp-snooping group

**Syntax** `display igmp-snooping group [ vlan vlan-id ] [ slot slot-id ] [ verbose ]`

**View** Any view

**Parameters** **vlan** *vlan-id*: Displays the IGMP Snooping forwarding table information in the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command will display the multicast group information in all VLANs.

**slot** *slot-id*: Displays the IGMP Snooping forwarding table information for the specified module.

**verbose**: Specifies to display the detailed IGMP Snooping forwarding table information.

**Description** Use the **display igmp-snooping group** command to view the IGMP Snooping forwarding table information.

**Examples** # View the detailed IGMP Snooping forwarding table information in VLAN 2.

```
<Sysname> display igmp-snooping group vlan 2 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):2.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port.
Eth1/0/2 (D) (00:01:30)
IP group(s):the following ip group(s) match to one mac group.
IP group address:224.1.1.1
(1.1.1.1, 224.1.1.1):
Attribute: Host Port
Host port(s):total 1 port.
Eth1/0/1 (D) (00:03:23)
MAC group(s):
MAC group address:0100-5e01-0101
Host port(s):total 1 port.
Eth1/0/1
```

**Table 153** Description of the fields of the display igmp-snooping group command

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups
Total 1 IP Source(s).	Total number of multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port	Port flags: D for dynamic port, S for static port, A for aggregation port, C for port copied from a (*, G) entry to an (S, G) entry
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for real egress sub-VLAN under the current entry, C for sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
IP group address	Address of IP multicast group
MAC group address	Address of MAC multicast group
Attribute	Attribute of IP multicast group
Host port(s)	Number of host member ports

## display igmp-snooping statistics

**Syntax** `display igmp-snooping statistics`

**View** Any view

**Parameters** None

**Description** Use the **display igmp-snooping statistics** command to view the statistics information of IGMP messages learned by IGMP Snooping.

**Examples** # View the statistics information of IGMP messages learned by IGMP Snooping.

```
<Sysname> display igmp-snooping statistics
Received IGMP general queries:0.
Received IGMPv1 reports:0.
Received IGMPv2 reports:19.
Received IGMP leaves:0.
Received IGMPv2 specific queries:0.
Sent IGMPv2 specific queries:0.
Received IGMPv3 reports:1.
Received IGMPv3 reports with right and wrong records:0.
Received IGMPv3 specific queries:0.
Received IGMPv3 specific sg queries:0.
Sent IGMPv3 specific queries:0.
Sent IGMPv3 specific sg queries:0.
Received error IGMP messages:19.
```

**Table 154** Description of the fields of the display igmp-snooping statistics command

Field	Description
general queries	General query messages
specific queries	Group-specific query messages

**Table 154** Description of the fields of the display igmp-snooping statistics command

Field	Description
reports	Report messages
leaves	Leave messages
reports with right and wrong records	Report messages with correct and incorrect records
specific sg query packet(s)	Group-and-source-specific query message(s)
error IGMP messages	IGMP messages with errors

---

## drop-unknown

**Syntax** **drop-unknown**

**undo drop-unknown**

**View** IGMP-Snooping view

**Parameters** None

**Description** Use the **drop-unknown** command to enable globally the function of dropping unknown multicast data.

Use the **undo drop-unknown** command to disable globally the function of dropping unknown multicast data.

By default, this function is disabled, that is, unknown multicast data is flooded.

This command works only on an IGMP Snooping-enabled VLAN, but not on a VLAN with IGMP enabled on the corresponding VLAN interface.

**Related commands:** **igmp-snooping drop-unknown.**

**Examples** # Globally enable the device to drop unknown multicast data.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] drop-unknown
```

---

## fast-leave

**Syntax** **fast-leave** [ **vlan** *vlan-list* ]

**undo fast-leave** [ **vlan** *vlan-list* ]

**View** IGMP-Snooping view

**Parameters** **vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a

VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

**Description** Use the **fast-leave** command to enable the fast leave feature globally.

Use the **undo fast-leave** command to disable the fast leave feature globally.

By default, the fast leave feature is disabled.

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

**Related commands:** **igmp-snooping fast-leave.**

**Examples** # Enable the fast leave feature globally in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] fast-leave vlan 2
```

## group-policy

**Syntax** **group-policy** *acl-number* [ **vlan** *vlan-list* ]

**undo group-policy** [ **vlan** *vlan-list* ]

**View** IGMP-Snooping view

**Parameters** *acl-number*: Basic ACL number, in the range of 2000 to 2999.

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

**Description** Use the **group-policy** command to configure a global multicast group filter.

Use the **undo group-policy** command to remove the configured global multicast group filter.

By default, no global multicast group filter is configured, namely a host can join any multicast group.

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.
- If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.
- You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

**Related commands:** **igmp-snooping group-policy.**

**Examples** # Configure ACL 2000 as the multicast group filter in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

---

## host-aging-time

**Syntax** **host-aging-time** *interval*

**undo host-aging-time**

**View** IGMP-Snooping view

**Parameters** *interval*: Member port aging time, in units of seconds. The effective range is 200 to 1,000.

**Description** Use the **host-aging-time** command to configure the aging time of group member ports globally.

Use the **undo host-aging-time** command to restore the default setting.

By default, the aging time of group member ports is 260 seconds.

This command works only on IGMP Snooping-enabled VLANs, but not on VLANs with IGMP enabled on the corresponding VLAN interfaces.

**Related commands:** **igmp-snooping host-aging-time.**

**Examples** # Set the aging time of group member ports globally to 300 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-aging-time 300
```

---

## igmp-snooping

**Syntax** **igmp-snooping**  
**undo igmp-snooping**

**View** System view

**Parameters** None

**Description** Use the **igmp-snooping** command to enable IGMP Snooping globally and enter IGMP-Snooping view.

Use the **undo igmp-snooping** command to disable IGMP Snooping globally.

By default, IGMP Snooping is disabled.

**Related commands:** **igmp-snooping enable.**

**Examples** # Enable IGMP Snooping globally and enter IGMP-Snooping view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping]
```

---

## igmp-snooping drop-unknown

**Syntax** **igmp-snooping drop-unknown**  
**undo igmp-snooping drop-unknown**

**View** VLAN view

**Parameters** None

**Description** Use the **igmp-snooping drop-unknown** command to enable the function of dropping unknown multicast data in the current VLAN.

Use the **undo igmp-snooping drop-unknown** command to disable the function of dropping unknown multicast data in the current VLAN.

By default, this function is disabled, that is, unknown multicast data is flooded.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

**Related commands:** **drop-unknown.**

**Examples** # In VLAN 2, enable the function of dropping unknown multicast data.



```

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping drop-unknown

```

---

## igmp-snooping enable

**Syntax** **igmp-snooping enable**  
**undo igmp-snooping enable**

**View** VLAN view

**Parameters** None

**Description** Use the **igmp-snooping enable** command to enable IGMP Snooping in the current VLAN.

Use the **undo igmp-snooping enable** command to disable IGMP Snooping in the current VLAN.

By default, IGMP Snooping is disabled in a VLAN.

IGMP Snooping must be enabled globally before it can be enabled in a VLAN.

**Related commands:** **igmp-snooping.**

**Examples** # Enable IGMP Snooping in VLAN 2.

```

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable

```

---

## igmp-snooping fast-leave

**Syntax** **igmp-snooping fast-leave [ vlan *vlan-list* ]**  
**undo igmp-snooping fast-leave [ vlan *vlan-list* ]**

**View** Ethernet interface view, port group view

**Parameters** **vlan *vlan-list***: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

**Description** Use the **igmp-snooping fast-leave** command to enable the fast leave feature on the current port or group of ports.

Use the **undo igmp-snooping fast-leave** command to disable the fast leave feature on the current port or group of ports.

By default, the fast leave feature is disabled.

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.
- If you do not specify any VLAN when you use this command in Ethernet port view, the command will take effect no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in manual port group view, the command will take effect on all the ports in this group no matter which VLANs these port belong to; if you specify a VLAN or multiple VLANs, the command will take effect on those ports in this group that belong to the specified VLAN(s).
- Configurations made in aggregation port group view are effective only for the master port in the group. If you do not specify any VLAN in aggregation port group view, the command will take effect no matter which VLAN the master port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the master port belongs to the specified VLAN(s).

**Related commands:** **fast-leave.**

**Examples** # Enable the fast leave feature on Ethernet 2/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] igmp-snooping fast-leave vlan 2
```

---

## igmp-snooping general-query source-ip

**Syntax** **igmp-snooping general-query source-ip** { **current-interface** | *ip-address* }

**undo igmp-snooping general-query source-ip**

**View** VLAN view

**Parameters** **current-interface:** Sets the source address of IGMP general queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 will be used as the source IP address of IGMP general queries.

*ip-address:* Specifies the source address of IGMP general queries, which can be any legal IP address.

**Description** Use the **igmp-snooping general-query source-ip** command to configure the source address of IGMP general queries.

Use the **undo igmp-snooping general-query source-ip** command to restore the default configuration.

By default, the source IP address of IGMP general queries is 0.0.0.0.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

**Examples** # Set the IP address of the interface of VLAN 2 to 10.1.1.1, with the subnet mask of 255.255.255.0, and specify this IP address as the source IP address of IGMP general queries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping general-query source-ip current-interface
```

---

## igmp-snooping group-limit

**Syntax** **igmp-snooping group-limit** *limit* [ **vlan** *vlan-list* ]

**undo igmp-snooping group-limit** [ **vlan** *vlan-list* ]

**View** Ethernet interface view, port group view

**Parameters** *limit*: Maximum number of multicast groups that can be joined on a port, ranging from 1 to 512.

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094. If you do not provide this option, the command will take effect on each VLAN to which this port belongs.

**Description** Use the **igmp-snooping group-limit** command to configure the maximum number of multicast groups that can be joined on a port.

Use the **undo igmp-snooping group-limit** command to restore the default setting.

The default value is 512.

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect on the port no matter which VLAN the port belongs to; if you

specify a VLAN or multiple VLANs, the command will take effect on the port only if the port belongs to the specified VLAN(s).

- If you do not specify any VLAN in port group view, the command will take effect on all the ports in this group no matter which VLANs these ports belong to; if you specify a VLAN or multiple VLANs, the command will take effect on those ports in this group that belong to the specified VLAN(s).

**Examples** # Specify to allow a maximum of 10 multicast groups to be joined on Ethernet 2/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] igmp-snooping group-limit 10 vlan 2
```

---

## igmp-snooping group-policy

**Syntax** **igmp-snooping group-policy** *acl-number* [ **vlan** *vlan-list* ]

**undo igmp-snooping group-policy** [ **vlan** *vlan-list* ]

**View** Ethernet interface view, port group view

**Parameters** *acl-number*: Basic ACL number, in the range of 2000 to 2999.

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

**Description** Use the **igmp-snooping group-policy** command to configure a multicast group filter on the current port(s).

Use the **undo igmp-snooping group-policy** command to remove a multicast group filter on the current port(s).

By default, no multicast group filter is configured on an interface, namely a host can join any multicast group

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect on the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect on the port only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in port group view, the command will take effect on all the ports in this group no matter which VLANs these port belong

to; if you specify a VLAN or multiple VLANs, the command will take effect on those ports in this group that belong to the specified VLAN(s).

- If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.
- You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

**Related commands:** **group-policy**.

**Examples** # Configure ACL 2000 as the multicast group filter on Ethernet 2/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] igmp-snooping group-policy 2000 vlan 2
```

## igmp-snooping host-aging-time

**Syntax** **igmp-snooping host-aging-time** *interval*

**undo igmp-snooping host-aging-time**

**View** VLAN view

**Parameters** *interval*: Member port aging time, in units of seconds. The effective range is 200 to 1,000.

**Description** Use the **igmp-snooping host-aging-time** command to configure the aging time of group member ports in the current VLAN.

Use the **undo igmp-snooping host-aging-time** command to restore the default setting.

By default, the aging time of group member ports is 260 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

**Related commands:** **host-aging-time**.

**Examples** # Set the aging time of group member ports to 300 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping host-aging-time 300
```

## igmp-snooping host-join

**Syntax** **igmp-snooping host-join** *group-address* [ **source-ip** *source-address* ] **vlan** *vlan-id*

**undo igmp-snooping host-join** *group-address* [ **source-ip** *source-address* ]  
**vlan** *vlan-id*

**View** Ethernet interface view, port group view

**Parameters** *group-address*: Address of the multicast group that the simulated host is to join, in the range of 224.0.1.0 to 239.255.255.255.

*source-address*: Address of the multicast source that the simulated host is to join. The value of this argument should be a valid unicast address or 0.0.0.0. If the value is 0.0.0.0, this means that no multicast source is specified.

**vlan** *vlan-id*: Specifies the VLAN that comprises the Ethernet port(s), where *vlan-id* is in the range of 1 to 4094.

**Description** Use the **igmp-snooping host-join** command to configure the current port(s) as simulated multicast group member host(s).

Use the **undo igmp-snooping host-join** command to remove the current port(s) as simulated multicast group member host(s).

By default, this function is disabled.

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces. The version of IGMP on the simulated host depends on the version of IGMP Snooping running in the VLAN or the version of IGMP running on the VLAN interface.
- The **source-ip** *source-address* option in the command is meaningful only for IGMP Snooping version 3. If IGMP Snooping version 2 is running, although you can include **source-ip** *source-address* in the command, the simulated host does not respond to a query message.
- If configured in Ethernet interface view, this feature takes effect on the port only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

**Examples** # Configure Ethernet 2/0/1 as a simulated member host in VLAN 2 for multicast source 1.1.1.1 and multicast group 224.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] igmp-snooping host-join 224.1.1.1 source-ip 1.1.1.1 vlan 2
```

---

## igmp-snooping last-member-query-interval

**Syntax** **igmp-snooping last-member-query-interval** *interval*

**undo igmp-snooping last-member-query-interval**

**View** VLAN view

**Parameters** *interval*: Interval between IGMP last-member queries, in units of seconds. The effective range is 1 to 5.

**Description** Use the **igmp-snooping last-member-query-interval** command to configure the interval between IGMP last-member queries in the VLAN.

Use the **undo igmp-snooping last-member-query-interval** command to restore the default setting.

By default, the IGMP last-member query interval is 1 second.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

**Related commands:** **last-member-query-interval.**

**Examples** # Set the interval between IGMP last-member queries to 3 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping last-member-query-interval 3
```

---

## igmp-snooping max-response-time

**Syntax** **igmp-snooping max-response-time** *interval*

**undo igmp-snooping max-response-time**

**View** VLAN view

**Parameters** *interval*: Maximum response time to IGMP general queries, in units of seconds. The effective range is 1 to 25.

**Description** Use the **igmp-snooping max-response-time** command to configure the maximum response time to IGMP general queries in the VLAN.

Use the **undo igmp-snooping max-response-time** command to restore the default setting.

By default, the maximum response time to IGMP general queries is 10 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

**Related commands:** **max-response-time, igmp-snooping query-interval.**

**Examples** # Set the maximum response time to IGMP general queries to 5 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping max-response-time 5
```

---

## igmp-snooping overflow-replace

**Syntax** **igmp-snooping overflow-replace** [ **vlan** *vlan-list* ]

**undo igmp-snooping overflow-replace** [ **vlan** *vlan-list* ]

**View** Ethernet interface view, port group view

**Parameters** **vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

**Description** Use the **igmp-snooping overflow-replace** command to enable the multicast group replacement function on the current port(s).

Use the **undo igmp-snooping overflow-replace** command to disable the multicast group replacement function on the current port(s).

By default, the multicast group replacement function is disabled.

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect on the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect on the port only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in port group view, the command will take effect on all the ports in this group no matter which VLANs these port belong to; if you specify a VLAN or multiple VLANs, the command will take effect on those ports in this group that belong to the specified VLAN(s).

**Related commands:** **overflow-replace.**

**Examples** # Enable the multicast group replacement function on Ethernet 2/0/1, which belongs to VLAN 2.



```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] igmp-snooping overflow-replace vlan 2
```

---

## igmp-snooping querier

**Syntax** **igmp-snooping querier**  
**undo igmp-snooping querier**

**View** VLAN view

**Parameters** None

**Description** Use the **igmp-snooping querier** command to enable the IGMP Snooping querier function.

Use the **undo igmp-snooping querier** command to disable the IGMP Snooping querier function.

By default, the IGMP Snooping querier function is disabled.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

**Examples** # Enable the IGMP Snooping querier function in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping querier
```

---

## igmp-snooping query-interval

**Syntax** **igmp-snooping query-interval** *interval*  
**undo igmp-snooping query-interval**

**View** VLAN view

**Parameters** *interval*: Interval between IGMP general queries, in units of seconds. The effective range is 2 to 300.

**Description** Use the **igmp-snooping query-interval** command to configure the interval between IGMP general queries.

Use the **undo igmp-snooping query-interval** command to restore the default setting.

By default, the IGMP general query interval is 60 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

**Related commands:** **igmp-snooping querier**, **igmp-snooping max-response-time**, **max-response-time**.

**Examples** # Set the interval between IGMP general queries to 20 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping query-interval 20
```

## igmp-snooping router-aging-time

**Syntax** **igmp-snooping router-aging-time** *interval*

**undo igmp-snooping router-aging-time**

**View** VLAN view

**Parameters** *interval*: Router port aging time, in units of seconds. The effective range is 1 to 1,000.

**Description** Use the **igmp-snooping router-aging-time** command to configure the aging time of router ports in the current VLAN.

Use the **undo igmp-snooping router-aging-time** command to restore the default setting.

By default, the aging time of router ports is 105 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

**Related commands:** **router-aging-time**.

**Examples** # Set the aging time of router ports to 100 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

## igmp-snooping source-deny

**Syntax** **igmp-snooping source-deny**

**undo igmp-snooping source-deny**

**View** Ethernet interface view, port group view

**Parameters** None

- Description** Use the **igmp-snooping source-deny** command to enable multicast source port filtering.
- Use the **undo igmp-snooping source-deny** command to disable multicast source port filtering.
- By default, multicast source port filtering is disabled.
- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.
- Examples** # Enable source port filtering for multicast data on Ethernet 2/0/1.
- ```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] igmp-snooping source-deny
```

igmp-snooping special-query source-ip

- Syntax** **igmp-snooping special-query source-ip** { **current-interface** | *ip-address* }
- undo igmp-snooping special-query source-ip**
- View** VLAN view
- Parameters** **current-interface**: Sets the source address of IGMP group-specific queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 will be used as the source IP address of IGMP group-specific queries.
- ip-address*: Sets the source address of IGMP group-specific queries to the specified address.
- Description** Use the **igmp-snooping special-query source-ip** command to configure the source IP address of IGMP group-specific queries.
- Use the **undo igmp-snooping special-query source-ip** command to restore the default configuration.
- By default, the source IP address of IGMP group-specific queries is 0.0.0.0.
- This command takes effect only if IGMP Snooping is enabled in the VLAN.
- Examples** # Set the IP address of the interface of VLAN 2 to 10.1.1.1, with the subnet mask of 255.255.255.0, and specify this IP address as the source IP address of IGMP group-specific queries.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping special-query source-ip current-interface
```

---

**igmp-snooping static-group**

**Syntax** **igmp-snooping static-group** *group-address* [ **source-ip** *source-address* ] **vlan** *vlan-id*

**undo igmp-snooping static-group** *group-address* [ **source-ip** *source-address* ] **vlan** *vlan-id*

**View** Ethernet interface view, port group view

**Parameters** *group-address*: Address of the multicast group to be statically joined, in the range of 224.0.0.0 to 239.255.255.255.

*source-address*: Address of multicast source to be statically joined. The value of this argument should be a valid unicast address or 0.0.0.0. If the value is 0.0.0.0, this means no multicast source is specified.

**vlan** *vlan-id*: Specifies the VLAN that comprises the Ethernet port(s), where *vlan-id* is in the range of 1 to 4094.

**Description** Use the **igmp-snooping static-group** command to enable the static (\*, G) or (S, G) joining function, namely to configure the current port or port group as static multicast group or source-group member(s).

Use the **undo igmp-snooping static-group** command to disable the static (\*, G) or (S, G) joining function.

By default, this function is disabled.

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.
- The **source-ip** *source-address* option in the command is meaningful only for IGMP Snooping version 3. If IGMP Snooping version 2 is running, although you can include the **source-ip** *source-address* option in your command, the configuration will not take effect.
- If configured in Ethernet interface view, this feature takes effect on the port only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

**Examples** # Configure Ethernet 2/0/1 in VLAN 2 to be a static member port for (1.1.1.1, 224.1.1.1).

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] igmp-snooping static-group 224.1.1.1 source-ip 1.1.1.1 vlan 2
```

---

## igmp-snooping static-router-port

**Syntax** **igmp-snooping static-router-port** *vlan* *vlan-id*  
**undo igmp-snooping static-router-port** *vlan* *vlan-id*

**View** Ethernet interface view, port group view

**Parameters** **vlan** *vlan-id*: Specifies a VLAN in which one or more static router ports are to be configured, where *vlan-id* is in the range of 1 to 4094.

**Description** Use the **igmp-snooping static-router-port** command to enable the static router port function.

Use the **undo igmp-snooping static-router-port** command to disable the static router port function.

By default, the static router port function is not enabled.

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.
- If configured in Ethernet interface view, this feature takes effect on the port only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

**Examples** # Enable the static router port function on Ethernet 2/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] igmp-snooping static-router-port vlan 2
```

---

## igmp-snooping version

**Syntax** **igmp-snooping version** *version-number*  
**undo igmp-snooping version**

**View** VLAN view

**Parameters** *version-number*: IGMP snooping version, in the range of 2 to 3.

**Description** Use the **igmp-snooping version** command to configure the IGMP Snooping version.

Use the **undo igmp-snooping version** command to restore the default setting.

By default, the IGMP version is 2.

This command can take effect only if IGMP Snooping is enabled in the VLAN.

**Related commands:** **igmp-snooping enable.**

**Examples** # Enable IGMP Snooping in VLAN 2, and set the IGMP Snooping version to version 3.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
```

## last-member-query-interval

**Syntax** **last-member-query-interval** *interval*

**undo last-member-query-interval**

**View** IGMP-Snooping view

**Parameters** *interval*: Interval between IGMP last-member queries, in units of seconds. The effective range is 1 to 5.

**Description** Use the **last-member-query-interval** command to configure the interval between IGMP last-member queries globally.

Use the **undo last-member-query-interval** command to restore the default setting.

By default, the interval between IGMP last-member queries is 1 second.

This command works only on IGMP Snooping-enabled VLANs, but not on VLANs with IGMP enabled on the corresponding VLAN interfaces.

**Related commands:** **igmp-snooping last-member-query-interval.**

**Examples** # Set the interval between IGMP last-member queries globally to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

## max-response-time

**Syntax** **max-response-time** *interval*

**undo max-response-time**

**View** IGMP-Snooping view

**Parameters** *interval*: Maximum response time to IGMP general queries, in units of seconds. The effective range is 1 to 25.

**Description** Use the **max-response-time** command to configure the maximum response time to IGMP general queries globally.

Use the **undo max-response-time** command to restore the default value.

This command works only on IGMP Snooping-enabled VLANs, but not on VLANs with IGMP enabled on the corresponding VLAN interfaces.

**Related commands:** **igmp-snooping max-response-time**, **igmp-snooping query-interval**.

**Examples** # Set the maximum response time to IGMP general queries globally to 5 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

**overflow-replace**

**Syntax** **overflow-replace** [ **vlan** *vlan-list* ]

**undo overflow-replace** [ **vlan** *vlan-list* ]

**View** IGMP-Snooping view

**Parameters** **vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

**Description** Use the **overflow-replace** command to enable the multicast group replacement function globally.

Use the **undo overflow-replace** command to disable the multicast group replacement function globally.

By default, the multicast group replacement function is disabled.

Note that:

- This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.

- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

**Related commands:** **igmp-snooping overflow-replace.**

**Examples** # Enable the multicast group replacement function globally in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

## report-aggregation

**Syntax** **report-aggregation**

**undo report-aggregation**

**View** IGMP-Snooping view

**Parameters** None

**Description** Use the **report-aggregation** command to enable IGMP report suppression.

Use the **undo report-aggregation** command to disable IGMP report suppression.

By default, IGMP report suppression is enabled.

This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.

**Examples** # Disable IGMP report suppression.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation
```

## reset igmp-snooping group

**Syntax** **reset igmp-snooping group** { *group-address* | **all** } [ **vlan** *vlan-id* ]

**View** User view

**Parameters** *group-address*: Address of the multicast group for which the IGMP Snooping forwarding entries are to be cleared. The value range is 224.0.1.0 to 239.255.255.255.

**all**: Specifies to clear all IGMP Snooping forwarding entries.



**vlan** *vlan-id*: Specifies a VLAN in which all IGMP Snooping forwarding entries are to be cleared, where *vlan-id* is in the range of 1 to 4094.

**Description** Use the **reset igmp-snooping group** command to clear IGMP Snooping forwarding entries.

Note that:

- This command works only on IGMP Snooping-enabled VLANs, but not on VLANs with IGMP enabled on the corresponding VLAN interfaces.
- This command cannot clear IGMP Snooping forwarding entries of static joins.

**Examples** # Clear all IGMP Snooping forwarding entries saved in the switch.

```
<Sysname> reset igmp-snooping group all
```

## reset igmp-snooping statistics

**Syntax** **reset igmp-snooping statistics**

**View** User view

**Parameters** None

**Description** Use the **reset igmp-snooping statistics** command to clear the statistics information of IGMP messages learned by IGMP Snooping.

**Examples** # Clear the statistics information of all kinds of IGMP messages learned by IGMP Snooping.

```
<Sysname> reset igmp-snooping statistics
```

## router-aging-time

**Syntax** **router-aging-time** *interval*

**undo router-aging-time**

**View** IGMP-Snooping view

**Parameters** *interval*: Router port aging time, in units of seconds. The effective range is 1 to 1,000.

**Description** Use the **router-aging-time** command to configure the aging time of router ports globally.

Use the **undo router-aging-time** command to restore the default setting.

By default, the aging time of router ports is 105 seconds.

This command works only on IGMP Snooping-enabled VLANs, but not on VLANs with IGMP enabled on the corresponding VLAN interfaces.

**Related commands:** **igmp-snooping router-aging-time.**

**Examples** # Set the aging time of router ports globally to 100 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100
```

## source-deny

**Syntax** **source-deny port** *interface-list*

**undo source-deny port** *interface-list*

**View** IGMP-Snooping view

**Parameters** *interface-list*: Ethernet port list. You can specify multiple Ethernet ports or port ranges by providing the this argument in the form of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] }, where *interface-type* is port type and *interface-number* is port number.

**Description** Use the **source-deny** command to enable multicast source port filtering so that all multicast data packets are blocked.

Use the **undo source-deny** command to disable multicast source port filtering.

By default, multicast source port filtering is not enabled.

This command works on IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.

**Examples** # Enable source port filtering for multicast data on interfaces Ethernet 2/0/1 through Ethernet 2/0/5.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] source-deny port ethernet 2/0/1 to ethernet 2/0/5
```

# 39

## MULTICAST VLAN CONFIGURATION COMMANDS

---

### display multicast-vlan

**Syntax** `display multicast-vlan [ vlan-id ]`

**View** Any view

**Parameters** *vlan-id*: VLAN ID of a multicast VLAN, in the range of 1 to 4094. If this argument is not provided, the information about all multicast VLANs and their sub-VLANs will be displayed.

**Description** Use the **display multicast-vlan** command to view the information about the specified multicast VLAN and its sub-VLANs.

**Examples** # View the information about all multicast VLANs and their sub-VLANs.

```
<Sysname> display multicast-vlan
multicast vlan 100's subvlan list:
 vlan 2 4-8
multicast vlan 200's subvlan list:
 no subvlan
multicast vlan 300's subvlan list:
 no subvlan
multicast vlan 400's subvlan list:
 no subvlan
```

---

### multicast-vlan enable

**Syntax** `multicast-vlan vlan-id enable`  
`undo multicast-vlan vlan-id enable`

**View** System view

**Parameters** *vlan-id*: Specifies a VLAN by its ID, in the range of 1 to 4094.

**Description** Use the **multicast-vlan enable** command to configure the specified VLAN as a multicast VLAN.

Use the **undo multicast-vlan enable** command to remove the specified VLAN as a multicast VLAN.

No VLAN is a multicast VLAN by default.

Note that:

- The specified VLAN must exist.
- The multicast VLAN feature cannot be enabled on a device with IP multicast routing enabled.
- After a VLAN is configured into a multicast VLAN, IGMP Snooping must be enabled in the VLAN before the multicast VLAN feature can be implemented, while it is not necessary to enable IGMP Snooping in the sub-VLANs of the multicast VLAN.

**Examples** # Configure VLAN 100 as a multicast VLAN.

```
<Sysname> system-view
[Sysname] multicast-vlan 100 enable
```

---

## multicast-vlan subvlan

**Syntax** **multicast-vlan** *vlan-id* **subvlan** *vlan-list*

**undo multicast-vlan** *vlan-id* **subvlan** *vlan-list*

**View** System view

**Parameters** *vlan-id*: VLAN ID of a multicast VLAN, in the range 1 to 4094.

**subvlan** *vlan-list*: Defines one or multiple VLANs as sub-VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

**Description** Use the **multicast-vlan subvlan** command to configure sub-VLAN(s) for the specified multicast VLAN.

Use the **undo multicast-vlan subvlan** command to remove the specified sub-VLAN(s) from the specified multicast VLAN.

A multicast VLAN has no sub-VLANs by default.

Note that:

- The VLAN to be configured as the multicast VLAN and the VLANs to be configured as sub-VLANs of the multicast VLAN must exist.
- The VLANs to be configured as sub-VLANs of the multicast VLAN must not be multicast VLANs.
- The VLANs to be configured as the sub-VLANs of the multicast VLAN must not be sub-VLANs of another multicast VLAN.

- The number of sub-VLANs of the multicast VLAN must not exceed the system-defined limit (an S7900E Ethernet switch supports up to five multicast VLANs, and supports up to 4000 sub-VLANs for each multicast VLAN. The total number of sub-VLANs for all multicast VLANs on the switch cannot exceed 4000).

**Examples** # Configure VLAN 10 through VLAN 15 as sub-VLANs of multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan 100 subvlan 10 to 15
```



# 40

## IGMP CONFIGURATION COMMANDS



The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running IGMP.

---

### display igmp group

**Syntax** `display igmp group [ group-address | interface interface-type interface-number ] [ static | verbose ]`

**View** Any view

**Parameters** *group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

**interface interface-type interface-number**: Displays the IGMP multicast group information about a particular interface.

**static**: Displays the information of statically joined IGMP multicast groups

**verbose**: Displays the detailed information of IGMP multicast groups.

**Description** Use the **display igmp group** command to view IGMP multicast group information.

Note that:

- If you do not specify *group-address*, this command will display the IGMP information of all the multicast groups.
- If you do not specify *interface-type interface-number*, this command will display the IGMP multicast group information on all the interfaces.
- If you do not specify the **static** keyword, this command will display the detailed information about the dynamically joined IGMP multicast groups.

**Examples** # Display the information about dynamically joined IGMP multicast groups on all interfaces.

```
<Sysname> display igmp group
Total 3 IGMP Group(s).
Interface group report information
Vlan-interface1 (20.20.20.20):
Total 3 IGMP Groups reported
 Group Address Last Reporter Uptime Expires
 225.1.1.1 20.20.20.20 00:02:04 00:01:15
```

```

225.1.1.3 20.20.20.20 00:02:04 00:01:15
225.1.1.2 20.20.20.20 00:02:04 00:01:17

```

# Display the detailed information of multicast group 225.1.1.1.

```

<Sysname> display igmp group 225.1.1.1 verbose
Interface group report information
Vlan-interface1 (10.10.1.20):
 Total 3 IGMP Groups reported
 Group: 225.1.1.1
 Uptime: 00:00:34
 Expires: 00:00:40
 Last reporter: 20.20.20.20
 Last-member-query-counter: 0
 Last-member-query-timer-expiry: off
 Version1-host-present-timer-expiry: off

```

**Table 155** Field descriptions of the display igmp group command

Field	Description
Group	Multicast group address
Uptime	Length of time since the multicast group was joined
Expires	Remaining time of the multicast group
Last reporter	Address of the last host that reported its membership for this multicast group
Last-member-query-counter	Number of group-specific queries sent
Last-member-query-timer-expiry	Remaining time of the last member query timer
Version1-host-present-timer-expiry	Remaining time of the IGMPv1 host present timer

## display igmp group port-info

**Syntax** `display igmp group port-info [ vlan vlan-id ] [ slot slot-id ] [ verbose ]`

**View** Any view

**Parameters** *vlan-id*: VLAN ID, in the range of 1 to 4094. If you do not specify a VLAN, this command will display the information of Layer 2 ports in all VLANs.

**slot** *slot-id*: Displays the Layer 2 port information on the specified module.

**verbose**: Displays the detailed information about Layer 2 ports.

**Description** Use the **display igmp group port-info** command to view IGMP Layer 2 port information.

**Examples** # View detailed information of IGMP Layer 2 ports.

```

<Sysname> display igmp group port-info verbose
 Total 1 IP Group(s).
 Total 1 IP Source(s).
 Total 1 MAC Group(s).

```

Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port  
Subvlan flags: R-Real VLAN, C-Copy VLAN



```

Vlan(id):2.
 Total 1 IP Group(s).
 Total 1 IP Source(s).
 Total 1 MAC Group(s).
 Router port(s):total 1 port.
 Eth1/0/2 (D) (00:01:30)
 IP group(s):the following ip group(s) match to one mac group.
 IP group address:224.1.1.1
 (1.1.1.1, 224.1.1.1):
 Attribute: Host Port
 Host port(s):total 1 port.
 Eth1/0/1 (D) (00:03:23)
 MAC group(s):
 MAC group address:0100-5e01-0101
 Host port(s):total 1 port.
 Eth1/0/1

```

**Table 156** Field descriptions of the display igmp group port-info command

Field	Description
Total1 IP Group(s).	Total number of IP multicast groups
Total 1 IP Source(s).	Total number of IP multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port	Port flags: D for dynamic port, S for static port, A for aggregation port, C for port copied from a (*, G) entry to an (S, G) entry
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for real egress sub-VLAN under the current entry, C for sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
IP group address	Address of IP multicast group
MAC group address	Address of MAC multicast group
Attribute	Attribute of IP multicast group
Host port(s)	Number of host member ports

## display igmp interface

**Syntax** `display igmp interface [ interface-type interface-number ] [ verbose ]`

**View** Any view

**Parameters** *interface-type interface-number*: Specifies an interface to display the IGMP information about. If no interface is specified, this command will display the related information of all IGMP-enabled interfaces.

**verbose**: Displays the detailed IGMP configuration and running information.

**Description** Use the **display igmp interface** command to view IGMP configuration and running information of the specified interface or all IGMP-enabled interfaces.

**Examples** # View the IGMP configuration and running status on VLAN-interface 1.

```

<Sysname> display igmp interface Vlan-interface 1 verbose
Vlan-interface1 (10.10.1.20):

```

```

IGMP is enabled
Current IGMP version is 2
Value of query interval for IGMP(in seconds): 60
Value of other querier present interval for IGMP(in seconds): 125
Value of maximum query response time for IGMP(in seconds): 10
Value of last member query interval(in seconds): 1
Value of startup query interval(in seconds): 15
Value of startup query count: 2
General query timer expiry (hours:minutes:seconds): 00:00:54
Querier for IGMP: 10.10.1.10
IGMP activity: 0 joins, 0 leaves
Multicast routing on this interface: enabled
Robustness: 2
Require-router-alert: disabled
Fast-leave: disabled
Startup-query-timer-expiry: off
Other-querier-present-timer-expiry: off

```

**Table 157** Field descriptions of the display igmp interface command

Field	Description
Vlan-interface1 (10.10.1.20)	Interface name (IP address)
Current IGMP version	Version of IGMP currently running on the interface
Value of query interval for IGMP(in seconds)	IGMP query interval, in seconds
Value of other querier present interval for IGMP(in seconds)	Other querier present interval, in seconds
Value of maximum query response time for IGMP(in seconds)	Maximum response time for IGMP general queries, in seconds
Value of last member query interval(in seconds)	IGMP last member query interval, in seconds
Value of startup query interval(in seconds)	IGMP startup query interval, in seconds
Value of startup query count	Number of IGMP general queries the device sends on startup
General query timer expiry	Remaining time of the IGMP general query timer
Querier for IGMP	IP address of the IGMP querier
IGMP activity	Statistics of IGMP activities (joins and leaves)
Robustness	Robustness variable of the IGMP querier
Require-router-alert	Whether IGMP messages without Router-Alert are dropped
Fast-leave	Fast leave processing status
Startup-query-timer-expiry	Remaining time of the startup query timer
Other-querier-present-timer-expiry	Remaining time of the other querier present timer

---

## display igmp routing-table

**Syntax** `display igmp routing-table [ source-address [ mask { mask | mask-length } ] | group-address [ mask { mask | mask-length } ] ] *`

**View** Any view

- Parameters**
- source-address*: Multicast source address.
  - group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.
  - mask*: Subnet mask of the multicast group/source address, 255.255.255.255 by default.
  - mask-length*: Subnet mask length of the multicast group/source address. For a multicast source address, this argument has an effective value range of 0 to 32; for a multicast group address, this argument has an effective value range of 4 to 32. The system default is 32 in both cases.

**Description** Use the **display igmp routing-table** command to view the routing information of the IGMP routing table.

**Examples**

```
View IGMP routing table information
<Sysname> display igmp routing-table
Routing table
Total 2 entries

00001. (*, 225.1.1.1)
 List of 1 downstream interface
 Vlan-interface1 (20.1.1.1),
 Protocol: STATIC

00002. (*, 239.255.255.250)
 List of 1 downstream interface
 Vlan-interface1 (20.20.20.20),
 Protocol: IGMP
```

**Table 158** Field descriptions of the display igmp routing-table command

Field	Description
00001	Sequence number of this (*, G) entry
(*, 225.1.1.1)	An (*, G) entry of the IGMP routing table
List of 1 downstream interface	Downstream interface list, namely the interfaces to which multicast data for this group will be forwarded

---

## fast-leave

**Syntax** **fast-leave** [ **group-policy** *acl-number* ]

**undo fast-leave**

**View** IGMP view

**Parameters** *acl-number*: Basic ACL number, in the range of 2000 to 2999. If you do not include this option in your command, this command will take effect for all multicast groups.

**Description** Use the **fast-leave** command to configure fast leave processing globally.

Use the **undo fast-leave** command to disable fast leave processing globally.

By default, fast leave processing is disabled. Namely, the IGMP querier sends IGMP group-specific queries upon receiving an IGMP leave message from a host, instead of sending a leave notification directly to the upstream.

**Related commands:** **igmp fast-leave, last-member-query-interval.**



*This command takes effect only on Layer 3 interfaces other than VLAN interfaces when executed in IGMP view.*

**Examples** # Enable fast leave processing globally.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] fast-leave
```

## igmp

**Syntax** **igmp**

**undo igmp**

**View** System view

**Parameters** None

**Description** Use the **igmp** command to enter IGMP view.

Use the **undo igmp** command to remove configurations performed in IGMP view.

IP multicast must be enabled on the device before this command can take effect.

**Related commands:** **igmp enable.**

**Examples** # Enter IGMP view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] igmp
[Sysname-igmp]
```

## igmp enable

**Syntax** **igmp enable**

**undo igmp enable**

**View** Interface view

**Parameters** None

**Description** Use the **igmp enable** command to enable IGMP on the current interface.  
Use the **undo igmp enable** command to disable IGMP on the current interface.  
By default, IGMP is disabled on an interface.

Note that:

- IP multicast must be enabled on the device before this command is meaningful.
- Before IGMP is enabled on an interface, any other IGMP feature configured on the interface will not take effect.

**Related commands:** **igmp.**

**Examples** # Enable IGMP on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp enable
```

## igmp fast-leave

**Syntax** **igmp fast-leave** [ **group-policy** *acl-number* ]

**undo igmp fast-leave**

**View** Interface view

**Parameters** *acl-number*: Basic ACL number, in the range of 2000 to 2999. If you do not include this option in your command, this command will take effect for all multicast groups.

**Description** Use the **igmp fast-leave** command to configure fast leave processing on the current interface.

Use the **undo igmp fast-leave** command to disable fast leave processing on the current interface.

By default, fast leave processing is disabled. Namely, the IGMP querier sends IGMP group-specific queries upon receiving an IGMP leave message from a host, instead of sending a leave notification directly to the upstream.



- The **igmp fast-leave** command cannot be used in VLAN interface view. To enable fast leave processing on a specific Layer 2 port or ports, use the **igmp-snooping fast-leave** command or the **fast-leave** command.
- The **igmp-snooping fast-leave** and **fast-leave** commands are effective for both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.

**Related commands:** **fast-leave**, **igmp last-member-query-interval**, **igmp-snooping fast-leave**, **fast-leave**. For the last two commands, refer to “IGMP Snooping Configuration Commands” on page 623.

**Examples** # Enable fast leave processing on LoopBack 1.

```
<Sysname> system-view
[Sysname] interface LoopBack 1
[Sysname-LoopBack1] igmp fast-leave
```

---

## igmp group-policy

**Syntax** **igmp group-policy** *acl-number* [ *version-number* ]

**undo igmp group-policy**

**View** Interface view

**Parameters** *acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999.

*version-number*: IGMP version, in the range of 1 to 3. By default, the system supports IGMPv1, IGMPv2 and IGMPv3 concurrently.

**Description** Use the **igmp group-policy** command to configure a multicast group filter on the current interface.

Use the **undo igmp group-policy** command to remove the configured multicast group filter.

By default, no multicast group filter is configured, namely a host can join any multicast group.



*When you use an advanced ACL as a filter, the source address in the ACL rule is the multicast source address specified in IGMPv3 reports, rather than the source address in the IP packets.*

- The **igmp group-policy** command cannot be used in VLAN interface view. To configure a multicast group filter on a specific Layer 2 port or ports, use the **igmp-snooping group-policy** command or the **group-policy** command.
- The **igmp-snooping group-policy** and **group-policy** commands are effective for both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.

**Related commands:** **igmp-snooping group-policy**, **group-policy**. Refer to “IGMP Snooping Configuration Commands” on page 623.

**Examples** # Configure an ACL rule so that hosts on the subnet attached to LoopBack 1 can join multicast group 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2005
[Sysname-acl-basic-2005] rule permit source 225.1.1.1 0
```

```
[Sysname-acl-basic-2005] quit
[Sysname] interface LoopBack 1
[Sysname-LoopBack1] igmp group-policy 2005
```

---

## igmp last-member-query-interval

**Syntax** **igmp last-member-query-interval** *interval*

**undo igmp last-member-query-interval**

**View** Interface view

**Parameters** *interval*: IGMP last member query interval in seconds, with an effective range of 1 to 5.

**Description** Use the **igmp last-member-query-interval** command to configure the last member query interval, namely the length of time the device waits between sending IGMP group-specific queries, on the current interface.

Use the **undo igmp last-member-query-interval** command to restore the system default.

By default, the IGMP last member query interval is 1 second.

**Related commands:** **last-member-query-interval, igmp robust-count, display igmp interface.**

**Examples** # Set the IGMP last member query interval to 3 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp last-member-query-interval 3
```

---

## igmp max-response-time

**Syntax** **igmp max-response-time** *interval*

**undo igmp max-response-time**

**View** Interface view

**Parameters** *interval*: Maximum response time in seconds for IGMP general queries, with an effective range of 1 to 25.

**Description** Use the **igmp max-response-time** command to configure the maximum response time for IGMP general queries on the current interface.

Use the **undo igmp max-response-time** command to restore the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

**Related commands:** **max-response-time**, **igmp timer other-querier-present**, **display igmp interface**.

**Examples** # Set the maximum response time for IGMP general queries to 8 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp max-response-time 8
```

## igmp require-router-alert

**Syntax** **igmp require-router-alert**  
**undo igmp require-router-alert**

**View** Interface view

**Parameters** None

**Description** Use the **igmp require-router-alert** command to configure the interface to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo igmp require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, namely it passes all the IGMP messages it receives to the upper layer protocol for processing.

**Related commands:** **require-router-alert**, **igmp send-router-alert**.

**Examples** # Configure VLAN-interface 100 to discard IGMP messages that do not carry the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp require-router-alert
```

## igmp robust-count

**Syntax** **igmp robust-count** *robust-value*  
**undo igmp robust-count**

**View** Interface view



**Parameters** *robust-value*: IGMP querier robustness variable, with an effective range of 2 to 5. The IGMP robustness variable determines the number of general queries the IGMP querier sends on startup and the number of IGMP group-specific queries the IGMP querier sends upon receiving an IGMP leave message.

**Description** Use the **igmp robust-count** command to configure the IGMP querier robustness variable on the current interface.

Use the **undo igmp robust-count** command to restore the system default.

By default, the IGMP querier robustness variable is 2.

**Related commands:** **robust-count, igmp timer query, igmp last-member-query-interval, igmp timer other-querier-present, display igmp interface.**

**Examples** # Set the IGMP querier robustness variable to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp robust-count 3
```

## igmp send-router-alert

**Syntax** **igmp send-router-alert**

**undo igmp send-router-alert**

**View** Interface view

**Parameters** None

**Description** Use the **igmp send-router-alert** command on the current interface to enable insertion of the Router-Alert option in IGMP messages to be sent.

Use the **undo igmp send-router-alert** command on the current interface to disable insertion of the Router-Alert option in IGMP messages to be sent.

By default, IGMP messages are sent with the Router-Alert option.

**Related commands:** **send-router-alert, igmp require-router-alert.**

**Examples** # Disable insertion of the Router-Alert option into IGMP messages that leave VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo igmp send-router-alert
```

---

**igmp static-group**

**Syntax** **igmp static-group** *group-address* [ **source** *source-address* ]  
**undo igmp static-group** { **all** | *group-address* [ **source** *source-address* ] }

**View** Interface view

**Parameters** **all**: Specifies to remove all static multicast groups that the current interface has joined.

*group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

*source-address*: Multicast source address.

**Description** Use the **igmp static-group** command to configure the current interface to be a statically connected member of the specified multicast group.

Use the **undo igmp static-group** command to remove the current interface as a statically connected member of the specified multicast group.

By default, an interface is not a static member of any multicast group.

If the specified multicast address is in the SSM multicast address range, and if a multicast source address is specified in the command, multicasts carrying the (S, G) entry, namely the source address information, can be sent out through this interface.



- The **igmp static-group** command cannot be used in VLAN interface view. To configure a specific Layer 2 port or ports to join a multicast group as static member(s), use the **igmp-snooping static-group** command.
- The **igmp-snooping static-group** command is effective for both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.

**Related commands:** **igmp-snooping static-group** in “IGMP Snooping Configuration Commands” on page 623.

**Examples** # Configure LoopBack 1 to be a statically connected member of multicast group 224.1.1.1.

```
<Sysname> system-view
[Sysname] interface LoopBack 1
[Sysname-LoopBack1] igmp static-group 224.1.1.1
```

# Configure LoopBack 2 so that it can forward multicasts that multicast source 192.168.1.1 sends to multicast group 232.1.1.1.

```
<Sysname> system-view
[Sysname] interface LoopBack 2
[Sysname-LoopBack2] igmp static-group 232.1.1.1 source 192.168.1.1
```

---

## igmp timer other-querier-present

**Syntax** `igmp timer other-querier-present interval`

`undo igmp timer other-querier-present`

**View** Interface view

**Parameters** *interval*: IGMP other querier present interval in seconds, in the range of 60 to 300.

**Description** Use the **igmp timer other-querier-present** command to configure the IGMP other querier present interval on the current interface.

Use the **undo igmp timer other-querier-present** command to restore the system default.

By default, the IGMP other querier present interval is [ IGMP query interval ] times [ IGMP querier robustness variable ] plus [ maximum response time for IGMP general queries ] divided by two.



*The three parameters in the above-mentioned formula default to 60 (seconds), 2 and 10 (seconds) respectively, so the default IGMP other querier present interval =  $60 \times 2 + 10 / 2 = 125$  (seconds).*

**Related commands:** **timer other-querier-present, igmp timer query, igmp robust-count, igmp max-response-time, display igmp interface.**

**Examples** # Set the IGMP other querier present interval to 200 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp timer other-querier-present 200
```

---

## igmp timer query

**Syntax** `igmp timer query interval`

`undo igmp timer query`

**View** Interface view

**Parameters** *interval*: IGMP query interval in seconds, namely the interval between IGMP general queries sent by the querier, with an effective range of 1 to 18,000.

**Description** Use the **igmp timer query** command to configure the IGMP query interval on the current interface.

Use the **undo igmp timer query** command to restore the system default.

By default, the IGMP query interval is 60 seconds.

**Related commands:** **timer query, igmp timer other-querier-present, display igmp interface.**

**Examples** # Set the IGMP query interval to 125 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp timer query 125
```

## igmp version

**Syntax** **igmp version** *version-number*

**undo igmp version**

**View** Interface view

**Parameters** *version-number*: IGMP version, in the range of 1 to 3.

**Description** Use the **igmp version** command to configure the IGMP version on the current interface.

Use the **undo igmp version** command to restore the default IGMP version.

The default IGMP version is version 2.

**Related commands:** **version.**

**Examples** # Set the IGMP version to IGMPv1 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp version 1
```

## last-member-query-interval

**Syntax** **last-member-query-interval** *interval*

**undo last-member-query-interval**

**View** IGMP view

**Parameters** *interval*: Last-member query interval in seconds, with an effective range of 1 to 5.

**Description** Use the **last-member-query-interval** command to configure the global IGMP last-member query interval.

Use the **undo last-member-query-interval** command to restore the system default.

By default, the IGMP last-member query interval is 1 second.

**Related commands:** **igmp last-member-query-interval, robust-count, display igmp interface.**

**Examples** # Set the global IGMP last-member interval to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] last-member-query-interval 3
```

## max-response-time

**Syntax** **max-response-time** *interval*  
**undo igmp max-response-time**

**View** IGMP view

**Parameters** *interval*: Maximum response time for IGMP general queries in seconds, with an effective range of 1 to 25.

**Description** Use the **max-response-time** command to configure the maximum response time for IGMP general queries globally.

Use the **undo max-response-time** command to restore the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

**Related commands:** **igmp max-response-time, timer other-querier-present, display igmp interface.**

**Examples** # Set the maximum response time for IGMP general queries to 8 seconds globally.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] max-response-time 8
```

## require-router-alert

**Syntax** **require-router-alert**  
**undo require-router-alert**

**View** IGMP view

**Parameters** None

**Description** Use the **require-router-alert** command to configure the router to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, namely it handles all the IGMP messages it received to the upper layer protocol for processing.

**Related commands:** **igmp require-router-alert, send-router-alert.**

**Examples** # Configure the router to discard IGMP messages that do not carry the Router-Alert option.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] require-router-alert
```

## reset igmp group

**Syntax** **reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [ **mask** { *mask* | *mask-length* } ] [ *source-address* [ **mask** { *mask* | *mask-length* } ] ] ] }

**View** User view

**Parameters** **all**: Specifies to clear all IGMP forwarding entries.

**interface** *interface-type interface-number*: Clears the IGMP forwarding entries on the specified interface.

*group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

*source-address*: Multicast source address.

*mask*: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Subnet mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

**Description** Use the **reset igmp group** command to clear IGMP forwarding entries.

Note that:

When clearing the IGMP forwarding entries of a VLAN interface, this command also clears the IGMP Snooping forwarding entries for that VLAN.

**Related commands:** **display igmp group.**

**Examples** # Clear all the IGMP and IGMP Snooping entries on all interfaces.

```
<Sysname> reset igmp group all
```

# Clear all IGMP forwarding entries on VLAN-interface 100 and all IGMP Snooping forwarding entries in VLAN 100.

```
<Sysname> reset igmp group interface vlan-interface 100 all
```

# Clear the IGMP forwarding entries of multicast group 225.0.0.1 on VLAN-interface 100 and all the IGMP Snooping forwarding entries of this multicast group in VLAN 100.

```
<Sysname> reset igmp group interface vlan-interface 100 225.0.0.1
```

# Clear the IGMP forwarding entries of multicast groups on subnet 225.1.1.0/24 on VLAN-interface 100 and the IGMP Snooping forwarding entries of multicast groups on this subnet in VLAN 100.

```
<Sysname> reset igmp group interface vlan-interface 100 225.1.1.0 mask 24
```

---

## reset igmp group port-info

**Syntax** **reset igmp group port-info** { **all** | *group-address* } [ **vlan** *vlan-id* ]

**View** User view

**Parameters** **all**: Clears Layer 2 port information of all the IGMP multicast groups.

*group-address*: Clears Layer 2 port information of the specified IGMP multicast group. The effective range of *group-address* is 224.0.1.0 to 239.255.255.255.

*vlan-id*: Clears Layer 2 port information of IGMP multicast groups in the specified VLAN. The effective range of *vlan-id* is 1 to 4094.

**Description** Use the **reset igmp group port-info** command to clear Layer 2 port information of IGMP multicast groups.

Note that:

- Layer 2 ports for IGMP multicast groups include member ports and router ports.
- This command cannot clear Layer 2 port information about IGMP multicast groups of static joins.

**Related commands:** **display igmp group port-info.**

**Examples** # Clear Layer 2 port information of all IGMP multicast groups in all VLANs.

```

<Sysname> reset igmp group port-info all

Clear Layer 2 port information of all IGMP multicast groups in VLAN 100.

<Sysname> reset igmp group port-info all vlan 100

Clear Layer 2 port information about multicast group 225.0.0.1 in VLAN 100.

<Sysname> reset igmp group port-info 225.0.0.1 vlan 100

```

---

## robust-count

**Syntax** **robust-count** *robust-value*

**undo robust-count**

**View** IGMP view

**Parameters** *robust-value*: IGMP querier robustness variable, with an effective range of 2 to 5. The IGMP robustness variable determines the number of general queries the IGMP querier sends on startup and the number of IGMP group-specific queries the IGMP querier sends upon receiving an IGMP leave message.

**Description** Use the **robust-count** command to configure the IGMP querier robustness variable globally.

Use the **undo robust-count** command to restore the system default.

By default, the IGMP querier robustness variable is 2.

**Related commands:** **igmp robust-count, timer query, last-member-query-interval, timer other-querier-present, display igmp interface.**

**Examples** # Set the IGMP querier robustness variable to 3 globally.

```

<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] robust-count 3

```

---

## send-router-alert

**Syntax** **send-router-alert**

**undo send-router-alert**

**View** IGMP view

**Parameters** None



**Description** Use the **send-router-alert** command to enable globally the insertion of the Router-Alert option into IGMP messages to be sent.

Use the **undo send-router-alert** command to disable globally the insertion of the Router-Alert option into IGMP messages to be sent.

By default, an IGMP message carries the Router-Alert option.

**Related commands:** **igmp send-router-alert, require-router-alert.**

**Examples** # Globally disable the insertion of the Router-Alert option in IGMP messages to be sent.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] send-router-alert
```

## timer other-querier-present

**Syntax** **timer other-querier-present** *interval*

**undo timer other-querier-present**

**View** IGMP view

**Parameters** *interval*: IGMP other querier present interval, in the range of 60 to 300.

**Description** Use the **timer other-querier-present** command to configure the IGMP other querier present interval globally.

Use the **undo timer other-querier-present** command to restore the system default.

By default, the IGMP other querier present interval is [ IGMP query interval ] times [ IGMP querier robustness variable ] plus [ maximum response time for IGMP general queries ] divided by two.



*The three parameters in the above-mentioned formula default to 60 (seconds), 2 (times) and 10 (seconds) respectively, so the default IGMP other querier present interval =  $60 \times 2 + 10 / 2 = 125$  (seconds).*

**Related commands:** **igmp timer other-querier-present, timer query, robust-count, max-response-time, display igmp interface.**

**Examples** # Set the IGMP other querier present interval to 200 seconds globally.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer other-querier-present 200
```

---

**timer query**

**Syntax** `timer query interval`

`undo timer query`

**View** IGMP view

**Parameters** *interval*: IGMP query interval in seconds, namely interval between IGMP general queries sent by the querier, with an effective range of 1 to 18,000.

**Description** Use the **timer query** command to configure the IGMP query interval globally.  
Use the **undo timer query** command to restore the default setting.  
By default, IGMP query interval is 60 seconds.

**Related commands:** **igmp timer query**, **timer other-querier-present**, **display igmp interface**.

**Examples** # Set the IGMP query interval to 125 seconds globally.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer query 125
```

---

**version**

**Syntax** `version version-number`

`undo version`

**View** IGMP view

**Parameters** *version-number*: IGMP version, in the range of 1 to 3.

**Description** Use the **version** command to configure the IGMP version globally.  
Use the **undo version** command to restore the system default.  
The default IGMP version is version 2.

**Related commands:** **igmp version**.

**Examples** # Set the global IGMP version to IGMPv1.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] version 1
```

# 41

## PIM CONFIGURATION COMMANDS



The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running the PIM protocol.

---

### auto-rp enable

**Syntax** **auto-rp enable**  
**undo auto-rp enable**

**View** PIM view

**Parameters** None

**Description** Use the **auto-rp enable** command to enable auto-RP.  
Use the **undo auto-rp enable** command to disable auto-RP.  
By default, auto-RP is disabled.

**Related commands:** **static-rp.**

**Examples** # Enable auto-RP.  

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] auto-rp enable
```

---

### bsr-policy

**Syntax** **bsr-policy** *acl-number*  
**undo bsr-policy**

**View** PIM view

**Parameters** *acl-number*: Basic ACL number, in the range of 2000 to 2999. When an ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source address range.

**Description** Use the **bsr-policy** command to configure a legal BSR address range to guard against BSR spoofing.

Use the **undo bsr-policy** command to remove the restriction of the BSR address range.

By default, there are no restrictions on the BSR address range, namely all the received BSR messages are regarded to be valid.

**Examples** # Configure a legal BSR address range so that only routers on the segment 10.1.1.0/24 can become the BSR.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] bsr-policy 2000
```

---

## c-bsr

**Syntax** **c-bsr** *interface-type interface-number* [ *hash-length* [ *priority* ] ]

**undo c-bsr**

**View** PIM view

**Parameters** *interface-type interface-number*: Specifies an interface by its type and number. This configuration can take effect only if PIM-SM is enabled on the interface.

*hash-length*: Hash mask length for RP selection calculation, in the range of 0 to 32. If you do not include this keyword in your command, the corresponding global setting will be used.

*priority*: Priority of the C-BSR, in the range of 0 to 255. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

**Description** Use the **c-bsr** command to configure the specified interface as a C-BSR.

Use the **undo c-bsr** command to remove the related C-BSR configuration.

No C-BSR is configured by default.

**Related commands:** **pim sm**, **c-bsr hash-length**, **c-bsr priority**, **c-rp**.

**Examples** # Configure VLAN-interface 100 to be a C-BSR.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr vlan-interface 100
```

---

## c-bsr admin-scope

**Syntax** **c-bsr admin-scope**  
**undo c-bsr admin-scope**

**View** PIM view

**Parameters** None

**Description** Use the **c-bsr admin-scope** command to enable BSR administrative scoping to implement RP-Set distribution based on BSR admin-scope regions.

Use the **undo c-bsr admin-scope** command to disable BSR administrative scoping.

By default, BSR administrative scoping is disabled, namely there is only one BSR in a PIM-SM domain.

**Related commands:** **c-bsr, c-bsr group, c-bsr global.**

**Examples** # Enable BSR administrative scoping.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr admin-scope
```

---

## c-bsr global

**Syntax** **c-bsr global [ hash-length *hash-length* | priority *priority* ] \***  
**undo c-bsr global**

**View** PIM view

**Parameters** *hash-length*: Hash mask length for RP selection calculation in the global scope zone, in the range of 0 to 32. If you do not include this keyword in your command, the corresponding global setting will be used.

*priority*: Priority of the C-BSR in the global scope zone, in the range of 0 to 255. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

**Description** Use the **c-bsr global** command to configure a C-BSR for the global scope zone.

Use the **undo c-bsr global** command to remove the C-BSR configuration for the global scope zone.

By default, no C-BSRs are configured for the global scope zone.

**Related commands:** **c-bsr group**, **c-bsr hash-length**, **c-bsr priority**.

**Examples** # Configure the router to be a C-BSR for the global scope zone, with the priority of 1.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr global priority 1
```

## c-bsr group

**Syntax** **c-bsr group** *group-address* { *mask* | *mask-length* } [ **hash-length** *hash-length* | **priority** *priority* ] \*

**undo c-bsr group** *group-address*

**View** PIM view

**Parameters** *group-address*: Multicast group address, in the range of 239.0.0.0 to 239.255.255.255.

*mask*: Mask of the multicast group address.

*mask-length*: Mask length of the multicast group address, in the range of 8 to 32.

*hash-length*: Hash mask length for RP selection calculation in the BSR admin-scope region corresponding to the specified multicast group, in the range of 0 to 32. If you do not include this keyword in your command, the corresponding global setting will be used.

*priority*: Priority of the C-BSR in the BSR admin-scope region corresponding to a multicast group, in the range of 0 to 255. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

**Description** Use the **c-bsr group** command to configure a C-BSR for the BSR admin-scope region associated with the specified group.

Use the **undo c-bsr group** command to remove the C-BSR configuration for the BSR admin-scope region associated with the specified group.

By default, no C-BSRs are configured for BSR admin-scope regions.

**Related commands:** **c-bsr global**, **c-bsr admin-scope**, **c-bsr hash-length**, **c-bsr priority**.

**Examples** # Configure the router to be a C-BSR in the BSR admin-scope region associated with the multicast group address 239.0.0.0/8, with the priority of 10.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

---

## c-bsr hash-length

**Syntax** **c-bsr hash-length** *hash-length*

**undo c-bsr hash-length**

**View** PIM view

**Parameters** *hash-length*: Hash mask length for RP selection calculation, in the range of 0 to 32.

**Description** Use the **c-bsr hash-length** command to configure the global Hash mask length for RP selection calculation.

Use the **undo c-bsr hash-length** command to restore the system default.

By default, the Hash mask length for RP selection calculation is 30.

**Related commands:** **c-bsr**, **c-bsr global**, **c-bsr group**.

**Examples** # Set the global Hash mask length for RP selection calculation to 16.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr hash-length 16
```

---

## c-bsr holdtime

**Syntax** **c-bsr holdtime** *interval*

**undo c-bsr holdtime**

**View** PIM view

**Parameters** *interval*: Bootstrap timeout in seconds, with an effective range of 1 to 2,147,483,647.

**Description** Use the **c-bsr holdtime** command to configure the bootstrap timeout time, namely the length of time a C-BSR waits before it must receive a bootstrap message from the BSR.

Use the **undo c-bsr holdtime** command to restore the system default.

By default, the bootstrap timeout value is determined by this formula: Bootstrap timeout = Bootstrap interval × 2 + 10.



*The default bootstrap interval is 60 seconds, so the default bootstrap timeout = 60 × 2 + 10 = 130 (seconds).*

**Related commands:** **c-bsr, c-bsr interval.**

**Examples** # Set the bootstrap timeout time to 150 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr holdtime 150
```

## c-bsr interval

**Syntax** **c-bsr interval** *interval*

**undo c-bsr interval**

**View** PIM view

**Parameters** *interval*: Bootstrap interval in seconds, with an effective range of 1 to 2,147,483,647.

**Description** Use the **c-bsr interval** command to configure the bootstrap interval, namely the interval at which the BSR sends bootstrap messages.

Use the **undo c-bsr interval** command to restore the system default.

By default, the bootstrap interval value is determined by this formula: Bootstrap interval = (Bootstrap timeout - 10) ÷ 2.



*The default bootstrap timeout is 130 seconds, so the default bootstrap interval = (130 - 10) ÷ 2 = 60 (seconds).*

**Related commands:** **c-bsr, c-bsr holdtime.**

**Examples** # Set the bootstrap interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr interval 30
```

## c-bsr priority

**Syntax** **c-bsr priority** *priority*

**undo c-bsr priority**

**View** PIM view

**Parameters** *priority*: Priority of the C-BSR, in the range of 0 to 255. A larger value of this argument means a higher priority.



**Description** Use the **c-bsr priority** command to configure the global C-BSR priority.  
 Use the **undo c-bsr priority** command to restore the system default.  
 By default, the C-BSR priority is 0.

**Related commands:** **c-bsr**, **c-bsr global**, **c-bsr group**.

**Examples** # Set the global C-BSR priority to 5.  

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr priority 5
```

## c-rp

**Syntax** **c-rp** *interface-type interface-number* [ **group-policy** *acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval* ] \*  
**undo c-rp** *interface-type interface-number*

**View** PIM view

**Parameters** *interface-type interface-number*: Specifies an interface, the IP address of which will be advertised as a C-RP address.

*acl-number*: Basic ACL number, in the range of 2000 to 2999. This ACL defines a range of multicast groups the C-RP is going to serve, rather than defining a filtering rule. Any group range matching the **permit** statement in the ACL will be advertised as an RP served group, while configurations matching other statements like **deny** will not take effect.

*priority*: Priority of the C-RP, in the range of 0 to 255 and defaulting to 0. A larger value of this argument means a lower priority.

*hold-interval*: C-RP timeout time, in seconds. The effective range is 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting will be used.

*adv-interval*: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting will be used.

**Description** Use the **c-rp** command to configure the specified interface as a C-RP.  
 Use the **undo c-rp** command to remove the related C-RP configuration.  
 No C-RPs are configured by default.

Note that:

- If you do not specify a group range for the C-RP, the C-RP will serve all multicast groups.
- If you wish a router to be a C-RP for multiple group ranges, you need to include these multiple group ranges in multiple rules in the ACL corresponding to the **group-policy** keyword.
- If you carry out this command repeatedly on the same interface, the last configuration will take effect.

**Related commands:** **c-bsr**.

**Examples** # Configure VLAN-interface 100 to be a C-RP for multicast groups 225.1.0.0/16 and 226.2.0.0/16, with a priority of 10.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 226.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] c-rp vlan-interface 100 group-policy 2000 priority 10
```

---

## c-rp advertisement-interval

**Syntax** **c-rp advertisement-interval** *interval*

**undo c-rp advertisement-interval**

**View** PIM view

**Parameters** *interval*: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535.

**Description** Use the **c-rp advertisement-interval** command to configure the interval at which C-RP-Adv messages are sent.

Use the **undo c-rp advertisement-interval** command to restore the system default.

By default, the C-RP-Adv interval is 60 seconds.

**Related commands:** **c-rp**.

**Examples** # Set the global C-RP-Adv interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp advertisement-interval 30
```

---

## c-rp holdtime

**Syntax** `c-rp holdtime interval`

`undo c-rp holdtime`

**View** PIM view

**Parameters** *interval*: C-RP timeout in seconds, with an effective range of 1 to 65,535.

**Description** Use the **c-rp holdtime** command to configure the global C-RP timeout time, namely the length of time the BSR waits before it must receive a C-RP-Adv message.

Use the **undo c-rp holdtime** command to restore the system default.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through BSR bootstrap messages, to prevent loss of BSR bootstrap messages, make sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the bootstrap interval or longer.

**Related commands:** `c-rp`, `c-bsr interval`.

**Examples** # Set the global C-RP timeout time to 200 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp holdtime 200
```

---

## crp-policy

**Syntax** `crp-policy acl-number`

`undo crp-policy`

**View** PIM view

**Parameters** *acl-number*: Advanced ACL number, in the range of 3000 to 3999. When the ACL is defined, the **source** keyword in the **rule** command specifies the address of a C-RP and the **destination** keyword specifies the address range of the multicast groups that the C-RP will serve.

**Description** Use the **crp-policy** command to configure a legal C-RP address range and the range of served multicast groups, so as to guard against C-RP spoofing.

Use the **undo crp-policy** command to remove the restrictions in C-RP address ranges and the ranges of served multicast groups.

By default, there are no restrictions on C-RP address ranges and the address ranges of served groups, namely all received C-RP messages are accepted.

**Examples** # Configure a C-RP address range and a range of served multicast groups so that only routers in the address range of 1.1.1.1/32 can be C-RPs and these C-RPs can serve only multicast groups in the address range of 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 1.1.1.1 0 destination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] crp-policy 3000
```

---

## display pim bsr-info

**Syntax** **display pim bsr-info**

**View** Any view

**Parameters** None

**Description** Use the **display pim bsr-info** command to view the BSR information in the PIM domain and the locally configured C-RP information in effect.

**Related commands:** **c-bsr, c-rp.**

**Examples** # View the BSR information in the PIM-SM domain and the locally configured C-RP information in effect.

```
<Sysname> display pim bsr-info
Elected BSR Address: 12.12.12.9
 Priority: 0
 Hash mask length: 30
 State: Elected
 Scope: Global
 Uptime: 00:00:56
 Next BSR message scheduled at: 00:01:14
Candidate BSR Address: 12.12.12.9
 Priority: 0
 Hash mask length: 30
 State: Elected
 Scope: Global

Candidate RP: 12.12.12.9(LoopBack1)
 Priority: 0
 HoldTime: 150
 Advertisement Interval: 60
 Next advertisement scheduled at: 00:00:48
Candidate RP: 3.3.3.3(Vlan-interfacel)
 Priority: 20
 HoldTime: 90
```

```

Advertisement Interval: 50
Next advertisement scheduled at: 00:00:28
Candidate RP: 5.5.5.5(Vlan-interface2)
Priority: 0
HoldTime: 80
Advertisement Interval: 60
Next advertisement scheduled at: 00:00:48

```

**Table 159** Field descriptions of the display pim bsr-info command

Field	Description
Elected BSR Address	Address of the elected BSR
Candidate BSR Address	Address of the candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length for RP selection calculation
State	BSR state
Scope	Scope of the BSR
Uptime	Length of time for which this BSR has been up, in hours:minutes:seconds
Next BSR message scheduled at	Length of time in which the BSR will expire, in hours:minutes:seconds
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval at which the C-RP sends advertisement messages
Next advertisement scheduled at	Length of time in which the C-RP will send the next advertisement message, in hours:minutes:seconds

## display pim claimed-route

**Syntax** `display pim claimed-route [ source-address ]`

**View** Any view

**Parameters** *source-address*: Displays the information of the unicast route to a particular multicast source. If you do not provide this argument, this command will display the information about all unicast routes used by PIM.

**Description** Use the **display pim claimed-route** command to view the information of unicast routes used by PIM.

If an (S, G) is marked SPT, this (S, G) entry uses a unicast route.

**Examples** # View the information of all unicast routes used by PIM.

```

<Sysname> display pim claimed-route
RPF information about: 172.168.0.0
 RPF interface: Vlan-interface2, RPF neighbor: 172.168.0.2
 Referenced route/mask: 172.168.0.0/24
 Referenced route type: unicast (direct)
 RPF-route selecting rule: preference-preferred

```

The (S,G) or (\*,G) list dependent on this route entry  
(172.168.0.12, 227.0.0.1)

**Table 160** Field descriptions of the display pim claimed-route command

Field	Description
RPF interface:	RPF interface type and number
RPF neighbor:	IP address of the RPF neighbor
Referenced route/mask:	Address/mask of the referenced route
Referenced route type:	Type of the referenced route
RPF-route selecting rule:	Rule of RPF route selection
The (S,G) or (*,G) list dependent on this route entry	(S, G) or (*, G) entries using this route

## display pim control-message counters

**Syntax** `display pim control-message counters [ message-type { probe | register | register-stop } | [ interface interface-type interface-number | message-type { assert | bsr | crp | graft | graft-ack | hello | join-prune | state-refresh } ] * ]`

**View** Any view

- Parameters**
- probe:** Displays the number of null register messages.
  - register:** Displays the number of register messages.
  - register-stop:** Displays the number of register-stop messages.
  - interface** *interface-type interface-number*: Displays the number of PIM control messages on the specified interface.
  - assert:** Displays the number of assert messages.
  - bsr:** Displays the number of Bootstrap messages.
  - crp:** Displays the number of C-RP-Adv messages.
  - graft:** Displays the number of Graft messages.
  - graft-ack:** Displays the number of Graft-ack messages.
  - hello:** Displays the number of Hello messages.
  - join-prune:** Displays the number of Join/prune messages.
  - state-refresh:** Displays the number of state refresh messages.
- Description** Use the **display pim control-message counters** command to view the statistics information of PIM control messages.

**Examples** # View the statistics information of all types of PIM control messages on all interfaces.

```

<Sysname> display pim control-message counters
PIM global control-message counters:
 Received Sent Invalid
Register 20 37 2
Register-Stop 25 20 1
Probe 10 5 0

PIM control-message counters for interface: Vlan-interface1
 Received Sent Invalid
Assert 10 5 0
Graft 20 37 2
Graft-Ack 25 20 1
Hello 1232 453 0
Join/Prune 15 30 21
State-Refresh 8 7 1
BSR 3243 589 1
C-RP 53 32 0

```

**Table 161** Field descriptions of display pim control-message counters

Field	Description
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages
C-RP	C-RP-Adv messages

## display pim grafts

**Syntax** `display pim grafts`

**View** Any view

**Parameters** None

**Description** Use the **display pim grafts** command to view the information about unacknowledged graft messages.

**Examples** # View the information about unacknowledged graft messages.

```
<Sysname> display pim grafts
Source Group Age RetransmitIn
192.168.10.1 224.1.1.1 00:00:24 00:00:02
```

**Table 162** Field descriptions of the display pim grafts command

Field	Description
Source	Multicast source address in the graft message
Group	Multicast group address in the graft message
Age	Time in which the graft message will get aged out, in hours:minutes:seconds
RetransmitIn	Time in which the graft message will be retransmitted, in hours:minutes:seconds

## display pim interface

**Syntax** **display pim interface** [ *interface-type interface-number* ] [ **verbose** ]

**View** Any view

**Parameters** *interface-type interface-number*: Displays the PIM information on a particular interface.

**verbose**: Displays the detailed PIM information.

**Description** Use the **display pim interface** command to view the PIM information on the specified interface or all interfaces.

**Examples** # View the PIM information on all interfaces.

```
<Sysname> display pim interface
Interface NbrCnt HelloInt DR-Pri DR-Address
Vlan1 1 30 1 10.1.1.2
Vlan2 0 30 1 172.168.0.2 (local)
Vlan3 1 30 1 20.1.1.2
```

**Table 163** Field descriptions of the display pim interface command

Field	Description
Interface	Interface name
NbrCnt	Number of PIM neighbors
HelloInt	Hello interval
DR-Pri	Priority for DR election
DR-Address	DR IP address

# View the detailed PIM information on VLAN-interface 1.

```
<Sysname> display pim interface Vlan-interface 1 verbose
Interface: Vlan-interface1, 10.1.1.1
 PIM version: 2
 PIM mode: Sparse
 PIM DR: 10.1.1.2
 PIM DR Priority (configured): 1
 PIM neighbor count: 1
 PIM hello interval: 30 s
```



```

PIM LAN delay (negotiated): 500 ms
PIM LAN delay (configured): 500 ms
PIM override interval (negotiated): 2500 ms
PIM override interval (configured): 2500 ms
PIM neighbor tracking (negotiated): disabled
PIM neighbor tracking (configured): disabled
PIM generation ID: 0XF5712241
PIM require generation ID: disabled
PIM hello hold interval: 105 s
PIM assert hold interval: 180 s
PIM triggered hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM BSR domain border: disabled
Number of routers on network not using DR priority: 0
Number of routers on network not using LAN delay: 0
Number of routers on network not using neighbor tracking: 2

```

**Table 164** Field descriptions of the display pim interface verbose command

Field	Description
Interface	Interface name and its IP address
PIM version	Running PIM version
PIM mode	PIM mode, dense or sparse
PIM DR	DR IP address
PIM DR Priority (configured)	Configured priority for DR election
PIM neighbor count	Total number of PIM neighbors
PIM hello interval	Hello interval
PIM LAN delay (negotiated)	Negotiated prune delay
PIM LAN delay (configured)	Configured prune delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of Hello messages without Generation_ID (enabled/disabled)
PIM hello hold interval	PIM neighbor timeout time
PIM assert hold interval	Assert timeout time
PIM triggered hello delay	Maximum delay of sending hello messages
PIM J/P interval	Join/prune interval
PIM J/P hold interval	Join/prune timeout time
PIM BSR domain border	BSR administrative scoping status (enabled/disabled)
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides

## display pim join-prune

**Syntax** **display pim join-prune mode** { **sm** [ **flags** *flag-value* ] | **ssm** } [ **interface** *interface-type interface-number* | **neighbor** *neighbor-address* ] \* [ **verbose** ]

**View** Any view

**Parameters** **mode**: Displays the information of join/prune messages to send in the specified PIM mode. PIM modes include **sm** and **ssm**, which represent PIM-SM and PIM-SSM respectively.

**flags** *flag-value*: Displays routing entries containing the specified flag. Values and meanings of *flag-value* are as follows:

- **rpt**: Specifies routing entries on the RPT.
- **spt**: Specifies routing entries on the SPT.
- **wc**: Specifies wildcard routing entries.

*interface-type interface-number*: Displays the information of join/prune messages to send on the specified interface.

*neighbor-address*: Displays the information of join/prune messages to send to the specified PIM neighbor.

**verbose**: Displays the detailed information of join/prune messages to send.

**Description** Use the **display pim join-prune** command to view the information about the join/prune messages to send.

**Examples** # View the information of join/prune messages to send in the PIM-SM mode.

```
<Sysname> display pim join-prune mode sm
 Expiry Time: 22 sec
 Upstream nbr: 192.168.1.55 (Vlan-interface1)
 0 (*, G) join(s), 1 (S, G) join(s), 0 (S, G, rpt) prune(s)

 Expiry Time: 50 sec
 Upstream nbr: 10.1.1.1 (Vlan-interface2)
 1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)

Total (*, G) join(s): 1, (S, G) join(s): 1, (S, G, rpt) prune(s): 1
```

**Table 165** Field descriptions of the display pim join-prune command

Field	Description
Expiry Time:	Expiry time of sending join/prune messages
Upstream nbr:	IP address of the upstream PIM neighbor and the interface connecting to it
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

## display pim neighbor

**Syntax** `display pim neighbor [ interface interface-type interface-number | neighbor-address | verbose ] *`

**View** Any view

**Parameters** *interface-type interface-number*: Displays the PIM neighbor information on a particular interface.

*neighbor-address*: Displays the information of a particular PIM neighbor.

**verbose**: Displays the detailed PIM neighbor information.

**Description** Use the **display pim neighbor** command to view the PIM neighbor information.

**Examples** # View the information of all PIM neighbors.

```
<Sysname> display pim neighbor
Total Number of Neighbors = 2
```

Neighbor	Interface	Uptime	Expires	Dr-Priority
10.1.1.2	Vlan1	02:50:49	00:01:31	1
20.1.1.2	Vlan2	02:49:39	00:01:42	1

**Table 166** Field descriptions of the display pim neighbor command

Field	Description
Total Number of Neighbors	Total number of PIM neighbors
Neighbor	IP address of the PIM neighbor
Interface	Interface connecting the PIM neighbor
Uptime	Length of time for which the PIM neighbor has been up, in hours:minutes:seconds
Expires	Length of time in which the PIM neighbor will expire, in hours:minutes:seconds
Dr-Priority	Designated router priority

# View the PIM neighbor information on VLAN-interface 1.

```
<Sysname> display pim neighbor interface Vlan-interface 1
```

```
Total Number of Neighbors on this interface = 3
```

Neighbor	Interface	Uptime	Expires	Dr-Priority
101.110.110.150	Vlan1	00:37:17	00:01:28	1
11.110.0.40	Vlan2	00:33:20	00:01:25	1
11.110.0.20	Vlan3	00:04:53	00:01:22	1

# View the detailed information of the PIM neighbor whose IP address is 11.110.0.20.

```
<Sysname> display pim neighbor 11.110.0.20 verbose
Neighbor: 11.110.0.20
Interface: Vlan-interface3
Uptime: 00:00:10
```

```

Expiry time: 00:00:30
DR Priority: 1
Generation ID: 0X2ACEFE15
Holdtime: 105 s
LAN delay: 500 ms
Override interval: 2500 ms
State refresh interval: 60 ms
Neighbor tracking: Disabled

```

---

## display pim routing-table

**Syntax** **display pim routing-table** [ *group-address* [ **mask** { *mask-length* | *mask* } ] ] | **source-address** [ **mask** { *mask-length* | *mask* } ] ] | **incoming-interface** [ *interface-type interface-number* | **register** ] ] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } ] | **mode** *mode-type* | **flags** *flag-value* | **fsm** ] \*

**View** Any view

**Parameters** *group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

*source-address*: Multicast source address.

*mask*: Mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Mask length of the multicast group/source address, in the range of 0 to 32. The system default is 32.

**incoming-interface**: Displays routing entries that contain the specified interface as the incoming interface.

*interface-type interface-number*: Specifies an interface by its type and number.

**register**: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

**outgoing-interface**: Displays routing entries of which the outgoing interface is the specified interface.

**include**: Displays routing entries of which the outgoing interface list includes the specified interface.

**exclude**: Displays routing entries of which the outgoing interface list excludes the specified interface.

**match**: Displays routing entries of which the outgoing interface list includes only the specified interface.

**mode** *mode-type*: Specifies a PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies PIM-DM.

- **sm**: Specifies PIM-SM.
- **ssm**: Specifies PIM-SSM.

**flags** *flag-value*: Displays routing entries containing the specified flag(s). The values of *flag-value* and their meanings are as follows:

- **2msdp**: Specifies routing entries to be contained in the next SA message to notify an MSDP peer.
- **act**: Specifies multicast routing entries to which actual data has arrived.
- **del**: Specifies multicast routing entries scheduled to be deleted.
- **exprune**: Specifies multicast routing entries containing outgoing interfaces pruned by other multicast routing protocols.
- **ext**: Specifies routing entries containing outgoing interfaces contributed by other multicast routing protocols.
- **loc**: Specifies multicast routing entries on routers directly connecting to the same subnet with the multicast source.
- **msdp**: Specifies routing entries learned from MSDP SA messages.
- **niif**: Specifies multicast routing entries containing unknown incoming interfaces.
- **nonbr**: Specifies routing entries with PIM neighbor searching failure.
- **rpt**: Specifies routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **spt**: Specifies routing entries on the SPT.
- **swt**: Specifies routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

**fsm**: Displays the detailed information of the finite state machine (FSM).

**Description** Use the **display pim routing-table** command to view PIM routing table information.

**Examples** # View the content of the PIM routing table.

```
<Sysname> display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(172.168.0.12, 227.0.0.1)
 RP: 2.2.2.2
 Protocol: pim-sm, Flag: SPT LOC ACT
 UpTime: 02:54:43
 Upstream interface: Vlan-interface1
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: Vlan-interface2
 Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

**Table 167** Field descriptions of the display pim routing-table command

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry (172.168.0.2, 227.0.0.1)	Number of (S, G) and (*, G) entries in the PIM routing table An (S, G) entry in the PIM routing table
Protocol	PIM mode, PIM-SM or PIM-DM
Flag	Flag bit of the (S, G) or (*, G) entry in the PIM routing table
Uptime	Length of time for which the (S, G) or (*, G) entry has been existing
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry <ul style="list-style-type: none"> <li>■ For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL.</li> <li>■ For a (S, G) entry, if this router directly connects to the multicast source, the RPF neighbor of this (S, G) entry is NULL.</li> </ul>
Downstream interface(s) information	Information of the downstream interface(s), including: <ul style="list-style-type: none"> <li>■ Number of downstream interfaces</li> <li>■ Downstream interface name</li> <li>■ PIM mode on the downstream interface(s)</li> <li>■ Uptime of the downstream interface(s)</li> <li>■ Expiry time of the downstream interface(s)</li> </ul>

---

## display pim rp-info

**Syntax** `display pim rp-info [ group-address ]`

**View** Any view

**Parameters** *group-address*: Address of the multicast group of which the RP information is to be displayed, in the range of 224.0.1.0 to 239.255.255.255. If you do not provide a group address, this command will display the RP information corresponding to all multicast groups.

**Description** Use the **display pim rp-info** command to view the RP information.

Note that:

- The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.
- Because a non-BSR router refreshes its local RP-Set only based on the received BSR bootstrap messages, the system does not delete an RP even if its expiry time is 0. Instead, the system waits for the next bootstrap message from the BSR: if the bootstrap message does not contain information of the RP, the system will delete it.

**Examples** # View the RP information corresponding to the multicast group 224.0.1.1.

```
<Sysname> display pim rp-info 224.0.1.1
BSR RP Address is: 2.2.2.2
 Priority: 0
 HoldTime: 150
 Uptime: 03:01:10
 Expires: 00:02:30
RP mapping for this group is: 2.2.2.2
```

# View the RP information corresponding to all multicast groups.

```
<Sysname> display pim rp-info
PIM-SM BSR RP information:
 Group/MaskLen: 224.0.0.0/4
 RP: 2.2.2.2
 Priority: 0
 HoldTime: 150
 Uptime: 03:01:36
 Expires: 00:02:29
```

**Table 168** Field descriptions of the display pim rp-info command

Field	Description
BSR RP Address is	IP address of the BSR RP
Group/MaskLen	The multicast group served by the RP
RP	IP address of the RP
Priority	RP priority
HoldTime	RP timeout time
Uptime	Length of time for which the RP has been up, in hours:minutes:seconds
Expires	Length of time in which the RP will expire, in hours:minutes:seconds
RP mapping for this group is: 2.2.2.2	The IP address of the RP serving the current multicast group is 2.2.2.2

## hello-option dr-priority

**Syntax** `hello-option dr-priority priority`

`undo hello-option dr-priority`

**View** PIM view

**Parameters** *priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

**Description** Use the **hello-option dr-priority** command to configure the global value of the router priority for DR election.

Use the **undo hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

**Related commands:** **pim hello-option dr-priority.**

**Examples** # Set the router priority for DR election to 3.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option dr-priority 3
```

## hello-option holdtime

**Syntax** **hello-option holdtime** *interval*

**undo hello-option holdtime**

**View** PIM view

**Parameters** *interval*: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535.

**Description** Use the **hello-option holdtime** command to configure the PIM neighbor timeout time.

Use the **undo hello-option holdtime** command to restore the system default.

By default, the PIM neighbor timeout time is 105 seconds.

This command is effective for both PIM-DM and PIM-SM.

**Related commands:** **pim hello-option holdtime.**

**Examples** # Set the global value of the PIM neighbor timeout time to 120 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option holdtime 120
```

## hello-option lan-delay

**Syntax** **hello-option lan-delay** *interval*

**undo hello-option lan-delay**

**View** PIM view

**Parameters** *interval*: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

**Description** Use the **hello-option lan-delay** command to configure the global value of the LAN-delay time, namely the length of time the device waits between receiving a prune message from downstream and taking the prune action. Within this period



of time, if the device receives a prune override message from that downstream device, the prune action will be overridden.

Use the **undo hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

**Related commands:** **hello-option override-interval**, **pim hello-option override-interval**, **pim hello-option lan-delay**.

**Examples** # Set the LAN-delay time to 200 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option lan-delay 200
```

## hello-option neighbor-tracking

**Syntax** **hello-option neighbor-tracking**  
**undo hello-option neighbor-tracking**

**View** PIM view

**Parameters** None

**Description** Use the **hello-option neighbor-tracking** command to globally disable join suppression, namely enable neighbor tracking.

Use the **undo hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

This command is effective for both PIM-DM and PIM-SM.

**Related commands:** **pim hello-option neighbor-tracking**.

**Examples** # Disable join suppression globally.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option neighbor-tracking
```

## hello-option override-interval

**Syntax** **hello-option override-interval** *interval*

**undo hello-option override-interval****View** PIM view**Parameters** *interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.**Description** Use the **hello-option override-interval** command to configure the global value of the prune override interval.Use the **undo hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

**Related commands:** **hello-option lan-delay, pim hello-option lan-delay, pim hello-option override-interval.****Examples** # Set the prune override interval to 2,000 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option override-interval 2000
```

**holdtime assert****Syntax** **holdtime assert** *interval***undo holdtime assert****View** PIM view**Parameters** *interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.**Description** Use the **holdtime assert** command to configure the global value of the assert timeout time.Use the **undo holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

This command is effective for both PIM-DM and PIM-SM.

**Related commands:** **holdtime join-prune, pim holdtime join-prune, pim holdtime assert.****Examples** # Set the global value of the assert timeout time to 100 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime assert 100
```

---

## holdtime join-prune

**Syntax** **holdtime join-prune** *interval*

**undo holdtime join-prune**

**View** PIM view

**Parameters** *interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

**Description** Use the **holdtime join-prune** command to configure the global value of the join/prune timeout time.

Use the **undo holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

**Related commands:** **holdtime assert, pim holdtime assert, pim holdtime join-prune.**

**Examples** # Set the global value of the join/prune timeout time to 280 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime join-prune 280
```

---

## jp-pkt-size

**Syntax** **jp-pkt-size** *packet-size*

**undo jp-pkt-size**

**View** PIM view

**Parameters** *packet-size*: Maximum size of join/prune messages in bytes, with an effective range of 100 to 8,100.

**Description** Use the **jp-pkt-size** command to configure the maximum size of join/prune messages.

Use the **undo jp-pkt-size** command to restore the system default.

By default, the maximum size of join/prune messages is 8,100 bytes.

**Related commands:** **jp-queue-size.**

**Examples** # Set the maximum size of join/prune messages to 1,500 bytes.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-pkt-size 1500
```

## jp-queue-size

**Syntax** **jp-queue-size** *queue-size*

**undo jp-queue-size**

**View** PIM view

**Parameters** *queue-size*: Maximum number of (S, G) entries in a join/prune message, in the range of 1 to 4,096.

**Description** Use the **jp-queue-size** command to configure the maximum number of (S, G) entries in a join/prune message.

Use the **undo jp-queue-size** command to restore the system default.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

When you use this command, take the following into account:

- The size of the forwarding table. In a network that does not support packet fragmentation, if you configure a large queue-size, a join/prune message may contain a large number of groups, causing the message length to exceed the MTU of the network. As a result, the products that do not support fragmentation will drop the join/prune message.
- The (S, G) join/prune state hold time on the upstream device. If you configure a small queue size, the outgoing interface of the corresponding entry may have been pruned due to timeout before the last join/prune message in a queue reaches the upstream device.

**Related commands:** **jp-pkt-size**, **holdtime join-prune**, **pim holdtime join-prune**.

**Examples** # Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-queue-size 2000
```

## pim

**Syntax** **pim**

**undo pim**

<b>View</b>	System view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>pim</b> command to enter PIM view.  Use the <b>undo pim</b> command to remove all configurations performed in PIM view.  IP multicast must be enabled on the device before this command can take effect.
<b>Examples</b>	# Enable IP multicast routing and enter PIM view.  <pre>&lt;Sysname&gt; system-view [Sysname] multicast routing-enable [Sysname] pim [Sysname-pim]</pre>

---

## pim bsr-boundary

<b>Syntax</b>	<b>pim bsr-boundary</b>  <b>undo pim bsr-boundary</b>
<b>View</b>	Interface view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>pim bsr-boundary</b> command to configure a BSR admin-scope region boundary on the current interface.  Use the <b>undo pim bsr-boundary</b> command to remove the configured BSR admin-scope region boundary.  By default, no BSR admin-scope region boundary is configured.
<b>Examples</b>	# Configure VLAN-interface 100 to be the boundary of the BSR admin-scope region.  <pre>&lt;Sysname&gt; system-view [Sysname] interface vlan-interface 100 [Sysname-Vlan-interface100] pim bsr-boundary</pre>

---

## pim dm

<b>Syntax</b>	<b>pim dm</b>  <b>undo pim dm</b>
<b>View</b>	Interface view

**Parameters** None

**Description** Use the **pim dm** command to enable PIM-DM.

Use the **undo pim dm** command to disable PIM-DM.

By default, PIM-DM is disabled.

Note that PIM-DM cannot be used for multicast groups in the SSM group range.

**Related commands:** **pim sm, ssm-policy.**

**Examples** # Enable PIM-DM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
```

## pim hello-option dr-priority

**Syntax** **pim hello-option dr-priority** *priority*

**undo pim hello-option dr-priority**

**View** Interface view

**Parameters** *priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

**Description** Use the **pim hello-option dr-priority** command to configure the router priority for DR election on the current interface.

Use the **undo pim hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

**Related commands:** **hello-option dr-priority.**

**Examples** # Set the router priority for DR election to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option dr-priority 3
```

## pim hello-option holdtime

**Syntax** **pim hello-option holdtime** *interval*

**undo pim hello-option holdtime**

**View** Interface view

**Parameters** *interval*: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535.

**Description** Use the **pim hello-option holdtime** command to configure the PIM neighbor timeout time on the current interface.

Use the **undo pim hello-option holdtime** command to restore the system default.

By default, the PIM neighbor timeout time is 105 seconds.

**Related commands:** **hello-option holdtime.**

**Examples** # Set the PIM neighbor timeout time to 120 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option holdtime 120
```

## pim hello-option lan-delay

**Syntax** **pim hello-option lan-delay** *interval*

**undo pim hello-option lan-delay**

**View** Interface view

**Parameters** *interval*: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

**Description** Use the **pim hello-option lan-delay** command to configure the LAN-delay time, namely the length of time the device waits between receiving a prune message and taking a prune action, on the current interface.

Use the **undo pim hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time to 500 milliseconds.

**Related commands:** **pim hello-option override-interval, hello-option override-interval, hello-option lan-delay.**

**Examples** # Set the LAN-delay time to 200 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option lan-delay 200
```

---

## pim hello-option neighbor-tracking

**Syntax** **pim hello-option neighbor-tracking**  
**undo pim hello-option neighbor-tracking**

**View** Interface view

**Parameters** None

**Description** Use the **pim hello-option neighbor-tracking** command to disable join suppression, namely enable neighbor tracking, on the current interface.

Use the **undo pim hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

**Related commands:** **hello-option neighbor-tracking.**

**Examples** # Disable join suppression on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option neighbor-tracking
```

---

## pim hello-option override-interval

**Syntax** **pim hello-option override-interval** *interval*  
**undo pim hello-option override-interval**

**View** Interface view

**Parameters** *interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

**Description** Use the **pim hello-option override-interval** command to configure the prune override interval on the current interface.

Use the **undo pim hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

**Related commands:** **pim hello-option lan-delay, hello-option lan-delay, hello-option override-interval.**



**Examples** # Set the prune override interval to 2,000 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option override-interval 2000
```

## pim holdtime assert

**Syntax** **pim holdtime assert** *interval*  
**undo pim holdtime assert**

**View** Interface view

**Parameters** *interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

**Description** Use the **pim holdtime assert** command to configure the assert timeout time on the current interface.

Use the **undo pim holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

**Related commands:** **holdtime join-prune, pim holdtime join-prune, holdtime assert.**

**Examples** # Set the assert timeout time to 100 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim holdtime assert 100
```

## pim holdtime join-prune

**Syntax** **pim holdtime join-prune** *interval*  
**undo pim holdtime join-prune**

**View** Interface view

**Parameters** *interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

**Description** Use the **pim holdtime join-prune** command to configure the join/prune timeout time on the interface.

Use the **undo pim holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

**Related commands:** **holdtime assert, pim holdtime assert, holdtime join-prune.**

**Examples** # Set the join/prune timeout time to 280 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim holdtime join-prune 280
```

## pim require-genid

**Syntax** **pim require-genid**

**undo pim require-genid**

**View** Interface view

**Parameters** None

**Description** Use the **pim require-genid** command enable rejection of hello messages without Generation\_ID.

Use the **undo pim require-genid** command to restore the default configuration.

By default, hello messages without Generation\_ID are accepted.

**Examples** # Enable VLAN-interface 100 to reject hello messages without Generation\_ID.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim require-genid
```

## pim sm

**Syntax** **pim sm**

**undo pim sm**

**View** Interface view

**Parameters** None

**Description** Use the **pim sm** command to enable PIM-SM.

Use the **undo pim sm** command to disable PIM-SM.

By default, PIM-SM is disabled.

**Related commands:** **pim dm.**

**Examples** # Enable PIM-SM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim sm
```

---

## pim state-refresh-capable

**Syntax** **pim state-refresh-capable**  
**undo pim state-refresh-capable**

**View** Interface view

**Parameters** None

**Description** Use the **pim state-refresh-capable** command to enable the state fresh feature on the interface.

Use the **undo pim state-refresh-capable** command to disable the state fresh feature.

By default, the state refresh feature is enabled.

**Related commands:** **state-refresh-interval**, **state-refresh-rate-limit**, **state-refresh-ttl**.

**Examples** # Disable state refresh on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim state-refresh-capable
```

---

## pim timer graft-retry

**Syntax** **pim timer graft-retry** *interval*  
**undo pim timer graft-retry**

**View** Interface view

**Parameters** *interval*: Graft retry period in seconds, with an effective range of 1 to 65,535.

**Description** Use the **pim timer graft-retry** command to configure the graft retry period.

Use the **undo pim timer graft-retry** command to restore the system default.

By default, the graft retry period is 3 seconds.

**Examples** # Set the graft retry period to 80 seconds on VLAN-interface 100.

```

<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer graft-retry 80

```

---

## pim timer hello

**Syntax** `pim timer hello interval`

`undo pim timer hello`

**View** Interface view

**Parameters** *interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

**Description** Use the **pim timer hello** command to configure on the current interface the interval at which hello messages are sent.

Use the **undo pim timer hello** command to restore the system default.

By default, hello messages are sent at the interval of 30 seconds.

**Related commands:** **timer hello.**

**Examples** # Set the hello interval to 40 seconds on VLAN-interface 100.

```

<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer hello 40

```

---

## pim timer join-prune

**Syntax** `pim timer join-prune interval`

`undo pim timer join-prune`

**View** Interface view

**Parameters** *interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

**Description** Use the **pim timer join-prune** command to configure on the current interface the interval at which join/prune messages are sent.

Use the **undo pim timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

**Related commands:** **timer join-prune.**

**Examples** # Set the join/prune interval to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer join-prune 80
```

## pim triggered-hello-delay

**Syntax** **pim triggered-hello-delay** *interval*  
**undo pim triggered-hello-delay**

**View** Interface view

**Parameters** *interval*: Maximum delay in seconds between hello messages, with an effective range of 1 to 5.

**Description** Use the **pim triggered-hello-delay** command to configure the maximum delay between hello messages.

Use the **undo pim triggered-hello-delay** command to restore the system default.

By default, the maximum delay between hello messages is 5 seconds.

**Examples** # Set the maximum delay between hello messages to 3 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim triggered-hello-delay 3
```

## probe-interval

**Syntax** **probe-interval** *interval*  
**undo probe-interval**

**View** PIM view

**Parameters** *interval*: Probe time in seconds, with an effective range of 1 to 3,600.

**Description** Use the **probe-interval** command to configure the probe time, namely the interval at which the DR sends null register messages before the register suppression timer expires.

Use the **undo probe-interval** command to restore the system default.

By default, the probe time is 5 seconds.

**Related commands:** **register-suppression-timeout.**

**Examples** # Set the probe time to 6 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] probe-interval 6
```

## register-policy

**Syntax** **register-policy** *acl-number*

**undo register-policy**

**View** PIM view

**Parameters** *acl-number*: Advanced ACL number, in the range of 3000 to 3999. Only register messages that match the **permit** statement of the ACL can be accepted by the RP.

**Description** Use the **register-policy** command to configure an ACL rule to filter register messages.

Use the **undo register-policy** command to remove the configured register filtering rule.

By default, no register filtering rule is configured.

**Related commands:** **register-suppression-timeout.**

**Examples** # Configure the RP to accept only those register messages for multicast traffic from multicast sources in the range of 10.10.0.0/16 to multicast groups in the range of 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] register-policy 3000
```

## register-suppression-timeout

**Syntax** **register-suppression-timeout** *interval*

**undo register-suppression-timeout**

**View** PIM view

**Parameters** *interval*: Register suppression timeout in seconds, in the range of 1 to 3,600.

**Description** Use the **register-suppression-timeout** command to configure the register suppression timeout time.

Use the **undo register-suppression-timeout** command to restore the system default.

By default, the register suppression timeout time is 60 seconds.

**Related commands:** **probe-interval**, **register-policy**.

**Examples** # Set the register suppression timeout time to 70 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-suppression-timeout 70
```

## register-whole-checksum

**Syntax** **register-whole-checksum**  
**undo register-whole-checksum**

**View** PIM view

**Parameters** None

**Description** Use the **register-whole-checksum** command to configure the router to calculate the checksum based on the entire register message.

Use the **undo register-whole-checksum** command to restore the default configuration.

By default, the checksum is calculated based on the header in the register message.

**Related commands:** **register-policy**, **register-suppression-timeout**.

**Examples** # Configure the router to calculate the checksum based on the entire register message.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-whole-checksum
```

## reset pim control-message counters

**Syntax** **reset pim control-message counters** [ **interface** *interface-type* *interface-number* ]

**View** User view

- Parameters** **interface** *interface-type interface-number*: Specifies to reset the PIM control message counter on a particular interface. If no interface is specified, this command will clear the statistics information of PIM control messages on all interfaces.
- Description** Use the **reset pim control-message counters** command to reset PIM control message counters.
- Examples** # Reset PIM control message counters on all interfaces.  
 <Sysname> reset pim control-message counters

## source-lifetime

- Syntax** **source-lifetime** *interval*  
**undo source-lifetime**
- View** PIM view
- Parameters** *interval*: Multicast source lifetime in seconds, with an effective range of 1 to 65,535.
- Description** Use the **source-lifetime** command to configure the multicast source lifetime.  
 Use the **undo source-lifetime** command to restore the system default.  
 By default, the lifetime of a multicast source is 210 seconds.
- Related commands:** **state-refresh-interval**.
- Examples** # Set the multicast source lifetime to 200 seconds.  
 <Sysname> system-view  
 [Sysname] pim  
 [Sysname-pim] source-lifetime 200

## source-policy

- Syntax** **source-policy** *acl-number*  
**undo source-policy**
- View** PIM view
- Parameters** *acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999.
- Description** Use the **source-policy** command to configure a multicast data filter.



Use the **undo source-policy** command to remove the configured multicast data filter.

By default, no multicast data filter is configured.

Note that:

- If you specify a basic ACL, the device filters all the received multicast packets based on the source address, and discards packets that fail the source address match.
- If you specify an advanced ACL, the device filters all the received multicast packets based on the source and group addresses, and discards packets that fail the match.
- If this command is executed repeatedly, the last configuration will take effect.

**Examples** # Configure the router to accept multicast packets originated from 10.10.1.2 and discard multicast packets originated from 10.10.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.10.1.2 0
[Sysname-acl-basic-2000] rule deny source 10.10.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] source-policy 2000
```

---

## spt-switch-threshold

**Syntax** **spt-switch-threshold infinity** [ **group-policy** *acl-number* [ **order** *order-value* ] ]  
**undo spt-switch-threshold** [ **group-policy** *acl-number* ]

**View** PIM view

**Parameters** **infinity**: Disables RPT-to-SPT switchover.

**group-policy** *acl-number*: Uses this threshold for multicast groups matching the specified multicast policy. In this option, *acl-number* refers to a basic ACL number, in the range of 2000 to 2999. If you do not include this option in your command, the threshold will apply on all multicast groups.

**order** *order-value*: Specifies the order of the ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the ACL in the group-policy list. If you have assigned an *order-value* to a certain ACL, do not specify the same *order-value* for another ACL; otherwise the system will give error information. If you do not specify an *order-value*, the order value of the ACL will remain the same in the group-policy list.

**Description** Use the **spt-switch-threshold** command to configure the RPT-to-SPT switchover parameters.

Use the **undo spt-switch-threshold** command to restore the default configuration.

By default, the device switches to the SPT immediately after it receives the first multicast packet from the RPT.

Note that:

- To adjust the order of an existing ACL in the group-policy list, you can use the *acl-number* argument to specify this ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. The order of the other existing ACLs in the group-policy list will remain unchanged.
- To use an ACL that does not exist in the group-policy list, you can use the *acl-number* argument to specify an ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. If you do not include the **order** *order-value* option in your command, the ACL will be appended to the end of the group-policy list.
- If you use this command multiple times on the same multicast group, the first traffic rate configuration matched in sequence will take effect.
- Once a multicast forwarding entry is created, subsequent multicast data will not be encapsulated in register messages before being forwarded even if a register outgoing interface is available. Therefore, to avoid forwarding failure, do not include the infinity keyword in the **spt-switch-threshold** command on a switch that may become an RP (namely, a static RP or a C-RP).

**Examples** # Disable RPT-to-SPT switchover on a switch that will never become an RP.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold infinity
```

---

## ssm-policy

**Syntax** **ssm-policy** *acl-number*

**undo ssm-policy**

**View** PIM view

**Parameters** *acl-number*: Basic ACL number, in the range of 2000 to 2999.

**Description** Use the **ssm-policy** command to configure the SSM multicast group range.

Use the **undo ssm-policy** command to restore the system default.

By default, the SSM group range is 232.0.0.0/8.

This command allows you to define an address range of permitted or denied multicast sources or groups. If the match succeeds, the multicast mode will be PIM-SSM; otherwise the multicast mode will be PIM-SM.

**Examples** # Configure the SSM group range to be 232.1.0.0/16.

```

<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] ssm-policy 2000

```

## state-refresh-interval

**Syntax** **state-refresh-interval** *interval*

**undo state-refresh-interval**

**View** PIM view

**Parameters** *interval*: State refresh interval in seconds, with an effective range of 1 to 255.

**Description** Use the **state-refresh-interval** command to configure the interval between state refresh messages.

Use the **undo state-refresh-interval** command to restore the system default.

By default, the state refresh interval is 60 seconds.

**Related commands:** **pim state-refresh-capable**, **state-refresh-rate-limit**, **state-refresh-ttl**.

**Examples** # Set the state refresh interval to 70 seconds.

```

<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-interval 70

```

## state-refresh-rate-limit

**Syntax** **state-refresh-rate-limit** *interval*

**undo state-refresh-rate-limit**

**View** PIM view

**Parameters** *interval*: Time to wait before receiving a new refresh message, in seconds and with an effective range of 1 to 65535.

**Description** Use the **state-refresh-rate-limit** command to configure the time the router must wait before receiving a new state refresh message.

Use the **undo state-refresh-rate-limit** command to restore the system default.

By default, the device waits 30 seconds before receiving a new state refresh message.

**Related commands:** `pim state-refresh-capable`, `state-refresh-interval`, `state-refresh-ttl`.

**Examples** # Configure the state refresh interval to 45 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-rate-limit 45
```

## state-refresh-ttl

**Syntax** `state-refresh-ttl ttl-value`

`undo state-refresh-ttl`

**View** PIM view

**Parameters** *ttl-value*: TTL value of state refresh messages, in the range of 1 to 255.

**Description** Use the **state-refresh-ttl** command to configure the TTL value of state refresh messages.

Use the **undo state-refresh-ttl** command to restore the system default.

By default, the TTL value of state refresh messages is 255.

**Related commands:** `pim state-refresh-capable`, `state-refresh-interval`, `state-refresh-rate-limit`.

**Examples** # Configure the device to send PIM state refresh messages with a TTL of 45.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-ttl 45
```

## static-rp

**Syntax** `static-rp rp-address [ acl-number ] [ preferred ]`

`undo static-rp rp-address`

**View** PIM view

**Parameters** *rp-address*: IP address of the static RP to be configured. This address must be a legal unicast IP address, rather than an address on the 127.0.0.0/8 segment.

*acl-number*: Basic ACL number, in the range of 2000 to 2999. If you provide this argument, the configured static RP will serve only those groups that pass the ACL

filtering; otherwise, the configured static RP will serve the all-system group 224.0.0.0/4.

**preferred:** Specifies to give priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP will be given priority, and the static RP takes effect on if no dynamic RP exists in the network or when the dynamic RP fails.

**Description** Use the **static-rp** command to configure a static RP.

Use the **undo static-rp** command to configure a static RP.

By default, no static RP is configured.

Note that:

- PIM-SM or PIM-DM cannot be enabled on an interface that serves as a static RP.
- When the ACL rule applied on a static RP changes, a new RP must be elected for all the multicast groups.
- You can configure multiple static RPs by using this command repeatedly. However, if you carry out this command multiple times and specify the same static RP address or reference the same ACL rule, the last configuration will override the previous one. If multiple static RPs have been configured for the same multicast group, the one with the highest IP address will be chosen to serve the multicast group.
- You can configure up to 50 static RPs on the same device.

**Related commands:** **display pim rp-info, auto-rp enable.**

**Examples** # Configure the interface with the IP address 11.110.0.6 to be a static RP that serves the multicast groups defined in ACL 2001, and give priority to this static RP in the case of static/dynamic RP conflict.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] static-rp 11.110.0.6 2001 preferred
```

---

## timer hello

**Syntax** **timer hello** *interval*

**undo timer hello**

**View** PIM view

**Parameters** *interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

**Description** Use the **timer hello** command to configure the hello interval globally.

Use the **undo timer hello** command to restore the system default.

By default, hello messages are sent at the interval of 30 seconds.

**Related commands:** **pim timer hello.**

**Examples** # Set the global hello interval to 40 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer hello 40
```

## timer join-prune

**Syntax** **timer join-prune** *interval*

**undo timer join-prune**

**View** PIM view

**Parameters** *interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

**Description** Use the **timer join-prune** command to configure the join/prune interval globally.  
Use the **undo timer join-prune** command to restore the system default.  
By default, the join/prune interval is 60 seconds.

**Related commands:** **pim timer join-prune.**

**Examples** # Set the global join/prune interval to 80 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer join-prune 80
```

# 42

## MSDP CONFIGURATION COMMANDS



*The term “router” in this document refers to a router in the generic sense or a Layer 3 switch running MSDP.*

---

### cache-sa-enable

**Syntax** **cache-sa-enable**  
**undo cache-sa-enable**

**View** MSDP view

**Parameters** None

**Description** Use the **cache-sa-enable** command to enable the SA message cache mechanism.

Use the **undo cache-sa-enable** command to disable the SA message cache mechanism.

By default, the SA message cache mechanism is enabled.

**Examples** # Enable the SA message cache mechanism.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] cache-sa-enable
```

---

### display msdp brief

**Syntax** **display msdp brief [ state { connect | down | listen | shutdown | up } ]**

**View** Any view

**Parameters** **state**: Displays the information of MSDP peers in the specified state.

**connect**: Displays the information of MSDP peers in the connecting state.

**down**: Displays the information of MSDP peers in the down state.

**listen**: Displays the information of MSDP peers in the listening state.

**shutdown:** Displays the information of MSDP peers in the deactivated state.

**up:** Displays the information of MSDP peers in the in-session state.

**Description** Use the **display msdp brief** command to view the brief information of MSDP peers.

**Examples** # View the brief information of MSDP peers in all states.

```
<Sysname> display msdp brief
MSDP Peer Brief Information
 Configured Up Listen Connect Shutdown Down
 1 1 0 0 0 0

 Peer's Address State Up/Down time AS SA Count Reset Count
 20.20.20.20 Up 00:00:13 100 0 0
```

**Table 169** Field descriptions of the display msdp brief command

Field	Description
Peer's Address	MSDP peer address
State	MSDP peer status: <ul style="list-style-type: none"> <li>■ Up: Session set up; MSDP peer in session</li> <li>■ Listen: Session set up; local device as server, in listening state</li> <li>■ Connect: Session not set up; local device as client, in connecting state</li> <li>■ Shutdown: Deactivated</li> <li>■ Down: Connection failed</li> </ul>
Up/Down time	Length of time since MSDP peer connection was established/failed
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number.
SA Count	Number of (S, G) entries
Reset Count	MSDP peer connection reset times

## display msdp peer-status

**Syntax** **display msdp peer-status** [ *peer-address* ]

**View** Any view

**Parameters** *peer-address*: Specifies an MSDP peer by its address. If you do not provide this argument, this command will display the detailed status information of all MSDP peers.

**Description** Use the **display msdp peer-status** command to view the detailed MSDP peer status information.

**Related commands:** **peer connect-interface**, **peer description**, **peer mesh-group**, **peer minimum-ttl**, **peer request-sa-enable**, **peer sa-cache-maximum**, **peer sa-policy**, **peer sa-request-policy**.



**Examples** # View the detailed status information of the MSDP peer with the address of 10.110.11.11.

```

<Sysname> display msdp peer-status 10.110.11.11
MSDP Peer 20.20.20.20, AS 100
Description:
Information about connection status:
 State: Up
 Up/down time: 14:41:08
 Resets: 0
 Connection interface: LoopBack0 (20.20.20.30)
 Number of sent/received messages: 867/947
 Number of discarded output messages: 0
 Elapsed time since last connection or counters clear: 14:42:40
Information about (Source, Group)-based SA filtering policy:
 Import policy: none
 Export policy: none
Information about SA-Requests:
 Policy to accept SA-Request messages: none
 Sending SA-Requests status: disable
Minimum TTL to forward SA with encapsulated data: 0
SAs learned from this peer: 0, SA-cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
 Count of RPF check failure: 0
 Incoming/outgoing SA messages: 0/0
 Incoming/outgoing SA requests: 0/0
 Incoming/outgoing SA responses: 0/0
 Incoming/outgoing data packets: 0/0

```

**Table 170** Field descriptions of the display msdp peer-status command

Field	Description
MSDP Peer	MSDP peer address
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number.
State	MSDP peer status: <ul style="list-style-type: none"> <li>■ Up: Session set up; MSDP peer in session</li> <li>■ Listen: Session set up; local device as server, in listening state</li> <li>■ Connect: Session not set up; local device as client, in connecting state</li> <li>■ Shutdown: Deactivated</li> <li>■ Down: Connection failed</li> </ul>
Resets	Number of times the MSDP peer connection is reset
Up/Down time	Length of time since MSDP peer connection was established/failed
Connection interface	Interface and its IP address used for setting up a TCP connection with the remote MSDP peer
Number of sent/received messages	Number of SA messages sent and received through this connection
Number of discarded output messages	Number of discarded outgoing messages
Elapsed time since last connection or counters clear	Time passed since the information of the MSDP peer was last cleared

**Table 170** Field descriptions of the display msdp peer-status command

Field	Description
Information about (Source, Group)-based SA filtering policy	SA message filtering list information <ul style="list-style-type: none"> <li>■ Import policy: Filter list for receiving SA messages from the specified MSDP peer</li> <li>■ Export policy: Filter list for forwarding SA messages from the specified MSDP peer</li> </ul>
Information about SA-Requests	SA requests information <ul style="list-style-type: none"> <li>■ Policy to accept SA-Request messages: Filtering rule for receiving or forwarding SA messages from the specified MSDP peer</li> <li>■ Sending SA-Requests status: Whether enabled to send an SA request message to the designated MSDP peer upon receiving a new Join message</li> </ul>
Minimum TTL to forward SA with encapsulated data	Minimum TTL of multicast packet encapsulated in SA messages
SAs learned from this peer	Number of cached SA messages
SA-cache maximum for the peer	Maximum number of SA messages from the specified MSDP peer that can be cached
Input queue size	Data size cached in the input queue
Output queue size	Data size cached in the output queue
Counters for MSDP message	MSDP peer statistics: <ul style="list-style-type: none"> <li>■ Count of RPF check failure: Number of SA messages discarded due to RPF check failure</li> <li>■ Incoming/outgoing SA messages: Number of SA messages received and sent</li> <li>■ Incoming/outgoing SA requests: Number of SA request received and sent</li> <li>■ Incoming/outgoing SA responses: Number of SA responses received and sent</li> <li>■ Incoming/outgoing data packets: Number of received and sent SA messages encapsulated with multicast data</li> </ul>

## display msdp sa-cache

**Syntax** **display msdp sa-cache** [ *group-address* | *source-address* | *as-number* ] \*

**View** Any view

**Parameters** *group-address*: Multicast group address in the (S, G) entry, in the range of 224.0.1.0 to 239.255.255.255.

*source-address*: Multicast source address in the (S, G) entry.

*as-number*: AS number, in the range of 1 to 65535.

**Description** Use the **display msdp sa-cache** command to view the information of (S, G) entries in the MSDP cache.

Note that:

- This command gives the corresponding output only after the **cache-sa-enable** command is executed.
- If you do not provide a source address, this command will display the information of all sources in the specified multicast group.
- If you do not provide a group address and a source address, this command will display the information of all cached entries.
- If you do not provide an AS number, this command will display the information related to all ASs.

**Related commands:** **cache-sa-enable.**

**Examples** # View the information of (S, G) entries in the MSDP cache.

```
<Sysname> display msdp sa-cache
MSDP Total Source-Active Cache - 5 entries

(Source, Group) Origin RP Pro AS Uptime Expires
(10.10.1.2, 225.1.1.1) 10.10.10.10 BGP 100 00:00:10 00:05:50
(10.10.1.3, 225.1.1.1) 10.10.10.10 BGP 100 00:00:11 00:05:49
(10.10.1.2, 225.1.1.2) 10.10.10.10 BGP 100 00:00:11 00:05:49
(10.10.2.1, 225.1.1.2) 10.10.10.10 BGP 100 00:00:11 00:05:49
(10.10.1.2, 225.1.2.2) 10.10.10.10 BGP 100 00:00:11 00:05:49

MSDP matched 5 entries
```

**Table 171** Field descriptions of the display msdp sa-cache command

Field	Description
(Source, Group)	(S, G) entry: (source address, group address)
Origin RP	Address of the RP that generated the (S, G) entry
Pro	Type of protocol from which the AS number is originated. "?" indicates that the system was unable to obtain the protocol type.
AS	AS number of the origin RP. "?" indicates that the system was unable to obtain the AS number.
Uptime	Length of time for which the cached (S, G) entry has been existing, in hours:minutes:seconds
Expires	Length of time in which the cached (S, G) entry will expire, in hours:minutes:seconds

## display msdp sa-count

**Syntax** **display msdp sa-count** [ *as-number* ]

**View** Any view

**Parameters** *as-number*: AS number, in the range of 1 to 65535.

**Description** Use the **display msdp sa-count** command to view the number of SA messages in the MSDP cache.

This command gives the corresponding output only after the **cache-sa-enable** command is executed.

**Related commands:** **cache-sa-enable.**

**Examples** # View the number of SA messages in the MSDP cache.

```
<Sysname> display msdp sa-count
Number of cached Source-Active entries, counted by Peer
Peer's Address Number of SA
10.10.10.10 5

Number of source and group, counted by AS
AS Number of source Number of group
? 3 3

Total 5 Source-Active entries
```

**Table 172** Field descriptions of the display msdp sa-count command

Field	Description
Number of cached Source-Active entries, counted by Peer	Number of SA messages per peer
Peer's Address	MSDP peer addresses
Number of SA	Number of SA messages from this peer
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number.
Number of source	Number of multicast sources from this AS
Number of group	Number of multicast groups from this AS

## encap-data-enable

**Syntax** **encap-data-enable**

**undo encap-data-enable**

**View** MSDP view

**Parameters** None

**Description** Use the **encap-data-enable** command to enable register message encapsulation in SA messages.

Use the **undo encap-data-enable** command to disable register message encapsulation in SA messages.

By default, an SA message contains only an (S, G) entry. No register message is encapsulated in an SA message.

**Examples** # Enable register message encapsulation in SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] encap-data-enable
```

---

## import-source

**Syntax** **import-source** [ **acl** *acl-number* ]

**undo import-source**

**View** MSDP view

**Parameters** *acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999. A basic ACL is used to filter multicast sources, while an advanced ACL is used to filter multicast sources or multicast groups. If you do not provide this argument in your command, no multicast source information will be advertised.



*During ACL matching, the protocol ID in the ACL rule is not checked.*

**Description** Use the **import-source** command to configure a rule of creating (S, G) entries.

Use the **undo import-source** command to remove any rule of creating (S, G) entries.

By default, when an SA message is created, there are no restrictions on the (S, G) entries to be advertised in it, namely all the (S, G) entries within the domain are advertised in the SA message.

In addition to controlling SA message creation by using this command, you can also configure a filtering rule for forwarding and receiving SA messages by using the **peer sa-policy** command.

**Related commands:** **peer sa-policy**.

**Examples** # Configure the MSDP peer to advertise only the (S, G) entries of multicast sources on the 10.10.0.0/16 subnet and with multicast group address of 225.1.0.0/16 when creating an SA message.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3101] quit
[Sysname] msdp
[Sysname-msdp] import-source acl 3101
```

---

## msdp

**Syntax** **msdp**

**undo msdp**

<b>View</b>	System view
<b>Parameters</b>	None
<b>Description</b>	<p>Use the <b>msdp</b> command to enable MSDP and enter MSDP view.</p> <p>Use the <b>undo msdp</b> command to disable MSDP and remove the configurations performed in MSDP view to free the resources occupied by MSDP.</p> <p>By default, MSDP is disabled.</p>
<b>Examples</b>	<pre># Enable MSDP and enter MSDP view. &lt;Sysname&gt; system-view [Sysname] multicast routing-enable [Sysname] msdp [Sysname-msdp]</pre>

---

## originating-rp

<b>Syntax</b>	<p><b>originating-rp</b> <i>interface-type interface-number</i></p> <p><b>undo originating-rp</b></p>
<b>View</b>	MSDP view
<b>Parameters</b>	<i>interface-type interface-number</i> : Specifies an interface by its type and number.
<b>Description</b>	<p>Use the <b>originating-rp</b> command to configure the address of the specified interface as the RP address of SA messages.</p> <p>Use the <b>undo originating-rp</b> command to restore the system default.</p> <p>By default, the PIM RP address is used as the RP address of SA messages.</p>
<b>Examples</b>	<pre># Specify the IP address of VLAN-interface 100 as the RP address of SA messages. &lt;Sysname&gt; system-view [Sysname] msdp [Sysname-msdp] originating-rp vlan-interface 100</pre>

---

## peer connect-interface

<b>Syntax</b>	<p><b>peer</b> <i>peer-address</i> <b>connect-interface</b> <i>interface-type interface-number</i></p> <p><b>undo peer</b> <i>peer-address</i></p>
<b>View</b>	MSDP view

- Parameters** *peer-address*: MSDP peer address.
- interface-type interface-number*: Specifies an interface by its type and number. The local device will use the IP address of the specified interface as the source IP address when setting up a TCP connection with the remote MSDP peer.
- Description** Use the **peer connect-interface** command to create an MSDP peer connection.
- Use the **undo peer connect-interface** command to remove an MSDP peer connection.
- No MSDP peer connection is created by default.
- Be sure to carry out this command before you use any other **peer** command; otherwise the system will prompt that the peer does not exist.

**Related commands:** **static-rpf-peer**.

- Examples** # Configure the router with the IP address of 125.10.7.6 as the MSDP peer of the local router, with interface VLAN-interface 100 as the local connection port.
- ```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
```

peer description

- Syntax** **peer** *peer-address* **description** *text*
- undo peer** *peer-address* **description**

View MSDP view

- Parameters** *peer-address*: MSDP peer address.
- text*: Descriptive string of 1 to 80 characters, case sensitive.

- Description** Use the **peer description** command to configure the description information for the specified MSDP peer.
- Use the **undo peer description** command to delete the configured description information of the specified MSDP peer.
- By default, an MSDP peer has no description information.

Related commands: **display msdp peer-status**.

- Examples** # Add the descriptive text "Router CstmrA" for the router with the IP address of 125.10.7.6 to indicate that this router is Customer A.

```

<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 description Router CstmrA

```

peer mesh-group

Syntax `peer peer-address mesh-group name`

`undo peer peer-address mesh-group`

View MSDP view

Parameters *peer-address*: MSDP peer address.

name: Mesh group name, a case-sensitive string of 1 to 32 characters.

Description Use the **peer mesh-group** command to configure an MSDP peer as a mesh group member.

Use the **undo peer mesh-group** command to remove an MSDP peer as a mesh group member.

By default, an MSDP peer does not belong to any mesh group.

Examples # Configure the MSDP peer with the IP address of 125.10.7.6 as a member of the mesh group "Grp1".

```

<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 mesh-group Grp1

```

peer minimum-ttl

Syntax `peer peer-address minimum-ttl ttl-value`

`undo peer peer-address minimum-ttl`

View MSDP view

Parameters *peer-address*: MSDP peer address.

ttl-value: Time-to-Live (TTL) value, in the range of 0 to 255.

Description Use the **peer minimum-ttl** command to configure the minimum TTL value of multicast packets encapsulated in SA messages.

Use the **undo peer minimum-ttl** command to restore the default setting.

By default, the minimum TTL value of a multicast packet encapsulated in an SA message is 0.

Related commands: **display msdp peer-status.**

Examples # Set the minimum TTL value of multicast packets to be encapsulated in SA messages to 10 so that only multicast packets whose TTL value is larger than or equal to 10 can be forwarded to the MSDP peer 110.10.10.1.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 110.10.10.1 minimum-ttl 10
```

peer request-sa-enable

Syntax **peer** *peer-address* **request-sa-enable**
undo peer *peer-address* **request-sa-enable**

View MSDP view

Parameters *peer-address*: MSDP peer address.

Description Use the **peer request-sa-enable** command to enable the device to send SA request messages.

Use the **undo peer request-sa-enable** command to disable the device from sending SA request messages.

By default, no SA request message is sent.

Note that before you can enable the device to send SA requests, you must disable the SA message cache mechanism.

Related commands: **cache-sa-enable.**

Examples # Disable the SA message cache mechanism, and enable the router to send an SA request message to the MSDP peer 125.10.7.6 upon receiving a new Join message.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] undo cache-sa-enable
[Sysname-msdp] peer 125.10.7.6 request-sa-enable
```

peer sa-cache-maximum

Syntax **peer** *peer-address* **sa-cache-maximum** *sa-limit*
undo peer *peer-address* **sa-cache-maximum**

View MSDP view

Parameters *peer-address*: MSDP peer address.

sa-limit: Maximum number of SA messages that the device can cache, in the range of 1 to 8,192.

Description Use the **peer sa-cache-maximum** command to configure the maximum number of SA messages that the device can cache.

Use the **undo peer sa-cache-maximum** command to restore the default setting.

By default, the device can cache a maximum of 8,192 SA messages.

Related commands: **display msdp sa-count**, **display msdp peer-status**, **display msdp brief**.

Examples # Allow the device to cache a maximum of 100 SA messages from the MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 sa-cache-maximum 100
```

peer sa-policy

Syntax **peer** *peer-address* **sa-policy** { **import** | **export** } [**acl** *acl-number*]

undo peer *peer-address* **sa-policy** { **import** | **export** }

View MSDP view

Parameters **import**: Specifies to filter SA messages from the specified MSDP peer.

export: Specifies to filter SA messages forwarded to the specified MSDP peer.

peer-address: MSDP peer address.

acl-number: Advanced ACL number, in the range of 3000 to 3999. If you do not provide an ACL number, all SA messages carrying (S, G) entries will be filtered off.

Description Use the **peer sa-policy** command to configure a filtering rule for receiving or forwarding SA messages.

Use the **undo peer sa-policy** command to restore the default setting.

By default, SA messages received or to be forwarded are not filtered, namely, all SA messages are accepted or forwarded.

In addition to controlling SA message receiving and forwarding by using this command, you can also configure a filtering rule for creating SA messages using the **import-source** command.

Related commands: **display msdp peer-status, import-source.**

Examples # Configure a filtering rule so that SA messages will be forwarded to the MSDP peer 125.10.7.6 only if they match ACL 3100.

```
<Sysname> system-view
[Sysname] acl number 3100
[Sysname-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255
destination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

peer sa-request-policy

Syntax **peer** *peer-address* **sa-request-policy** [**acl** *acl-number*]

undo peer *peer-address* **sa-request-policy**

View MSDP view

Parameters *peer-address*: MSDP peer address.

acl-number: Basic ACL number, in the range of 2000 to 2999. If you provide this argument, the SA requests of only the multicast groups that match the ACL will be accepted and other SA requests will be ignored; if you do not provide this argument, all SA requests will be ignored.

Description Use the **peer sa-request-policy** command to configure a filtering rule for SA request messages.

Use the **undo peer sa-request-policy** command to remove the configured SA request filtering rule.

By default, SA request messages are not filtered.

Related commands: **display msdp peer-status.**

Examples # Configure an SA request filtering rule so that SA messages from the MSDP peer 175.58.6.5 will be accepted only if the multicast group address in the SA messages is in the range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] msdp
[Sysname-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

reset msdp peer

Syntax **reset msdp peer** [*peer-address*]

View User view

Parameters *peer-address*: Specifies an MSDP peer by its address. If you do not provide this argument, the TCP connections with all MSDP peers will be reset.

Description Use the **reset msdp peer** command to reset the TCP connection with the specified MSDP peer or the TCP connections with all MSDP peers and clear all the statistics information of the MSDP peer(s).

Related commands: **display msdp peer-status.**

Examples # Reset the TCP connection with the MSDP peer 125.10.7.6 and clear all the statistics information of this MSDP peer.

```
<Sysname> reset msdp peer 125.10.7.6
```

reset msdp sa-cache

Syntax **reset msdp sa-cache** [*group-address*]

View User view

Parameters *group-address*: Address of the multicast group related to which the (S, G) entries are to be cleared from the MSDP cache. The effective range is 224.0.1.0 to 239.255.255.255. If you do not provide this argument, the command will clear all the cached (S, G) entries.

Description Use the **reset msdp sa-cache** command to clear (S, G) entries from the MSDP cache.

Related commands: **cache-sa-enable, display msdp sa-cache.**

Examples # Clear the (S, G) entries related to the multicast group 225.5.4.3 from the MSDP cache.

```
<Sysname> reset msdp sa-cache 225.5.4.3
```

reset msdp statistics

Syntax **reset msdp statistics** [*peer-address*]

View User view

- Parameters** *peer-address*: Address of the MSDP peer of which the statistics information is to be cleared. If you do not provide this argument, the command will clear the statistics information of all MSDP peers.
- Description** Use the **reset msdp statistics** command to clear the statistics information of the specified MSDP peer or all MSDP peers without resetting the MSDP peer(s).
- Examples** # Clear the statistics information of the MSDP peer 125.10.7.6.

```
<Sysname> reset msdp statistics 125.10.7.6
```

shutdown

Syntax **shutdown** *peer-address*
undo shutdown *peer-address*

View MSDP view

Parameters *peer-address*: MSDP peer address.

Description Use the **shutdown** command to deactivate manually the connection with the specified MSDP peer.

Use the **undo shutdown** command to reactivate the connection with the specified MSDP peer.

By default, the connections with all MSDP peers are active.

Related commands: **display msdp peer-status.**

Examples # Deactivate the connection with the MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] shutdown 125.10.7.6
```

static-rpf-peer

Syntax **static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]
undo static-rpf-peer *peer-address*

View MSDP view

Parameters *peer-address*: MSDP peer address.

rp-policy *ip-prefix-name*: Specifies a filtering policy based on the RP address in SA messages, where *ip-prefix-name* is the filtering policy name, a case sensitive string of 1 to 19 characters.

Description Use the **static-rpf-peer** command to configure a static RPF peer.

Use the **undo static-rpf-peer** command to remove a static RPF peer.

No static RPF peer is configured by default.

When you configure multiple static RPF peers, observe the follow rules:

- 1 If you use the **rp-policy** keyword for all the static RPF peers, all the static RPF peers take effect concurrently. SA messages will be filtered as per the configured prefix list and only those SA messages whose RP addresses pass the filtering will be accepted. If multiple static RPF peers use the same filtering policy at the same time, when a peer receives an SA message, it will forward the SA message to the other peers.
- 2 If you use the **rp-policy** keyword for none of the static RPF peers, according to the configuration sequence, only the first static RPF peer whose connection is in the UP state will be activated, and all SA messages from this peer will be accepted while the SA messages from other static RPF peers will be discarded. When this active static RPF peer fails (for example, when the configuration is removed or when the connection is torn down), still the first RPF peer whose connection is in UP state will be selected as the activated RPF peer according to the configuration sequence.

Related commands: **display msdp peer-status**, ip prefix-list.

Examples # Configure static RPF peers.

```
<Sysname> system-view
[Sysname] ip ip-prefix list1 permit 130.10.0.0 16 great-equal 16 les
s-equal 32
[Sysname] msdp
[Sysname-msdp] peer 130.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

timer retry

Syntax **timer retry** *interval*

undo timer retry

View MSDP view

Parameters *interval*: Interval between MSDP peer connection retries, in seconds. The effective range is 1 to 60.

Description Use the **timer retry** command to configure the interval between MSDP peer connection retries.

Use the **undo timer retry** command to restore the default setting.

By default, the interval between MSDP peer connection retries is 30 seconds.

Related commands: **display msdp peer-status.**

Examples # Set the MSDP peer connection retry interval to 60 seconds.

```
<Sysname> system-view  
[Sysname] msdp  
[Sysname-msdp] timer retry 60
```


43

MULTICAST ROUTING CONFIGURATION COMMANDS



The term “router” in this document refers to a router in the generic sense or a Layer 3 switch running an IP multicast routing protocol.

display multicast boundary

Syntax **display multicast boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]

View Any view

Parameters *group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask of the multicast group address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group address, in the range of 4 to 32. The system default is 32.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **display multicast boundary** command to view the multicast boundary information on the specified interface or all interfaces.

Related commands: **multicast boundary**.

Examples # View the multicast boundary information on all interfaces.

```
<Sysname> display multicast boundary
Multicast boundary information
Boundary                Interface
224.1.1.0/24            Vlan1
```

Table 173 Field descriptions of the display multicast boundary command

| Field | Description |
|------------|--|
| Boundary | Multicast group corresponding to the multicast boundary |
| Interface: | Boundary interface corresponding to the multicast boundary |

display multicast forwarding-table

Syntax **display multicast forwarding-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } } | **statistics** | **slot** *slot-id*] * [**port-info**]

View Any view

Parameters *source-address*: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Displays forwarding entries of which the incoming interface is the specified one.

register: Specifies the register interface.

outgoing-interface: Displays forwarding entries of which the outgoing interface is the specified one.

exclude: Displays the routing entries of which the outgoing interface list excludes the specified interface.

include: Displays the routing entries of which the outgoing interface list includes the specified interface.

match: Specifies the routing entries of which the outgoing interface list includes and includes only the specified interface.

statistics: Specifies to display the statistics information of the multicast forwarding table.

slot *slot-id*: Specifies the slot number of an interface module. If you do not specify this option, this command will display the multicast forwarding table information of all modules.

port-info: Specifies to display Layer 2 port information.

Description Use the **display multicast forwarding-table** command to view the multicast forwarding table information.

Related commands: **multicast forwarding-table downstream-limit, multicast forwarding-table route-limit, display multicast routing-table.**

Examples # View the multicast forwarding table information.

```
<Sysname> display multicast forwarding-table
Multicast Forwarding Table
Total 1 entry, 1 matched
00001. (172.168.0.2, 227.0.0.1), MID: 0, Flags: 0x0:0
    Uptime: 00:08:32, Timeout in: 00:03:26
    Incoming interface: Vlan-interface1
    List of 1 outgoing interfaces:
        1: Vlan-interface2
    Matched 38264 packets(1071392 bytes), Wrong If 0 packets
    Forwarded 18696 packets(523488 bytes)
```

Table 174 Field descriptions of display multicast forwarding-table

| Field | Description |
|---|---|
| 00001 | Sequence number of the (S, G) entry |
| (172.168.0.2,227.0.0.1) | An (S, G) entry of the multicast forwarding table |
| MID | (S, G) entry ID. Each (S, G) entry has a unique MID |
| Flags | Current state of the (S, G) entry. Different bits are used to indicate different states of (S, G) entries. Major values of this field are described in Table 175. |
| Uptime | Length of time for which the (S, G) entry has been up, in hours:minutes:seconds |
| Timeout in | Length of time in which the (S, G) entry will expire, in hours:minutes:seconds |
| Incoming interface | Incoming interface of the (S, G) entry |
| List of 1 outgoing interface: | Outgoing interface list |
| 1: Vlan-interface2 | Interface number: outgoing interface name and number |
| Matched 38264 packets (1071392 bytes), Wrong If 0 packets | (S, G)-matched packets (bytes), packets with incoming interface errors |
| Forwarded 18696 packets (523488 bytes) | (S, G)-forwarded packets (bytes) |

Table 175 Major values of the flags field

| Value | Meaning |
|------------|---|
| 0x00000001 | Indicates that a register-stop message must be sent |
| 0x00000002 | Indicates whether the multicast source corresponding to the (S, G) is active |
| 0x00000004 | Indicates a null forwarding entry |
| 0x00000008 | Indicates whether the RP is a PIM domain border router |
| 0x00000010 | Indicates that a register outgoing interface is available |
| 0x00000400 | Identifies a packet to be deleted |
| 0x00008000 | Indicates that the (S, G) entry is in the smoothing process after active/standby switchover |
| 0x00010000 | Indicates that the (S, G) has been updated during the smoothing process |
| 0x00080000 | Indicates that the (S, G) entry has been repeatedly updated and needs to be deleted before a new entry is added |
| 0x00100000 | Indicates that an entry is successfully added |

display multicast routing-table

Syntax **display multicast routing-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } }] *

View Any view

Parameters *source-address*: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Displays multicast routing entries of which the incoming interface is the specified one.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface of PIM-SM.

outgoing-interface: Displays multicast routing entries of which the outgoing interface is the specified one.

exclude: Displays routing entries of which the outgoing interface list excludes the specified interface.

include: Displays routing entries of which the outgoing interface list includes the specified interface.

match: Displays routing entries of which the outgoing interface list includes only the specified interface.

Description Use the **display multicast routing-table** command to view the multicast routing table information.

Related commands: **display multicast forwarding-table.**

Examples # View the routing information in the multicast routing table.

```
<Sysname> display multicast routing-table
Multicast routing table
Total 1 entry
00001. (172.168.0.2, 227.0.0.1)
    Uptime: 00:00:28
```

```

Upstream Interface: Vlan-interface2
List of 2 downstream interfaces
  1: Vlan-interface3
  2: Vlan-interface1

```

Table 176 Field descriptions of display multicast routing-table

| Field | Description |
|---------------------------------|--|
| 00001 | Sequence number of the (S, G) entry |
| (172.168.0.2, 227.0.0.1) | An (S, G) entry of the multicast forwarding table |
| Uptime | Length of time for which the (S, G) entry has been up, in hours:minutes:seconds |
| Upstream interface | Upstream interface the (S, G) entry: multicast packets should arrive at this interface |
| List of 2 downstream interfaces | Downstream interface list: these interfaces need to forward multicast packets |

display multicast routing-table static

Syntax **display multicast routing-table static** [**config**] [*source-address* { *mask-length* | *mask* }]

View Any view

Parameters **config**: Displays the configuration information of static routes.

source-address: Multicast source address.

mask: Mask of the multicast source address.

mask-length: Mask length of the multicast source address, in the range of 0 to 32.

Description Use the **display multicast routing-table static** command to view the information of multicast static routes.

Examples # View all the multicast static routes.

```

<Sysname> display multicast routing-table static
Multicast Routing Table
Routes : 1

Mroute 10.10.0.0/16
  Interface = Vlan-interface1  RPF Neighbor = 10.10.0.254
  Matched routing protocol = <none>, Route-policy = <none>
  Preference = 1, Order = 1
  Running Configuration = ip rpf-route-static 10.10.0.0 16 2.2.2.2 order 1

```

View the configuration information of multicast static routes.

```

<Sysname> display multicast routing-table static config
Multicast Routing Table
Routes : 1

Mroute 10.10.0.0/16,  interface = Vlan-interface1

```

```
Matched routing protocol = <none>, Route-policy = <none>
Preference = 1, Order = 1
```

Table 177 Field descriptions of display multicast routing-table static

| Field | Description |
|--------------------------|--|
| Mroute | Multicast route source address and its mask length |
| Interface | Outgoing interface to the multicast source |
| RPF Neighbor | IP address of the RPF neighbor through which the multicast source is reachable |
| Matched routing protocol | If a protocol is configured, the multicast source address of the route should be the destination address of an entry in unicast routing table. |
| Route-policy | Routing policy. The multicast source address of the route should match the routing policy. |
| Preference | Route preference |
| Order | Sequence number of the route |

display multicast rpf-info

Syntax `display multicast rpf-info source-address [group-address]`

View Any view

Parameters *source-address*: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

Description Use the **display multicast rpf-info** command to view the RPF information of a multicast source.

Related commands: **display multicast routing-table**, **display multicast forwarding-table**.

Examples # View the RPF information of multicast source 192.168.1.55.

```
<Sysname> display multicast rpf-info 192.168.1.55
RPF information about source 192.168.1.55:
  RPF interface: Vlan-interfacel, RPF neighbor: 10.1.1.1
  Referenced route/mask: 192.168.1.0/24
  Referenced route type: igp
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

Table 178 Field descriptions of the display multicast rpf-info command

| Field | Description |
|---|--|
| RPF information about source 192.168.1.55 | Information of the RPF path to multicast source 192.168.1.55 |
| RPF interface | RPF interface |
| RPF neighbor | IP address of the RPF neighbor |
| Referenced route/mask | Referenced route and its mask length |

Table 178 Field descriptions of the display multicast rpf-info command

| Field | Description |
|-----------------------|--|
| Referenced route type | Type of the referenced route, which can be any of the following: <ul style="list-style-type: none"> ■ igp: unicast route (IGP) ■ egp: unicast route (BGP) ■ unicast (direct): unicast route (directly connected) ■ unicast: other unicast route (such as unicast static route) ■ multicast static: multicast static route |
| Route selection rule | Rule for RPF route selection, which can be based on the preference of the routing protocol or based on the longest match on the destination address |
| Load splitting rule | Status of the load splitting rule (enabled/disabled) |

ip rpf-route-static

Syntax **ip rpf-route-static** *source-address* { *mask* | *mask-length* } [*protocol* [*process-id*]] [**route-policy** *policy-name*] { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*] [**order** *order-number*]

undo ip rpf-route-static *source-address* { *mask* | *mask-length* } [*protocol* [*process-id*]] [**route-policy** *policy-name*]

View System view

Parameters *source-address*: Multicast source address.

mask: Mask of the multicast source address.

mask-length: Mask length of the multicast source address, in the range of 0 to 32.

protocol: Routing protocol, which can have any of the following values:

- **bgp**: Specifies the BGP protocol.
- **isis**: Specifies the IS-IS protocol.
- **ospf**: Specifies the OSPF protocol.
- **rip**: Specifies the RIP protocol.

process-id: Process number of the unicast routing protocol, in the range of 1 to 65535. This argument must be provided if IS-IS, OSPF or RIP is the specified unicast routing protocol.

policy-name: Name of the multicast route match rule, a string of 1 to 19 characters.

rpf-nbr-address: Specifies an RPF neighbor by the IP address.

interface-type interface-number: Specifies an RPF neighbor by the interface type and interface number. The interface type must not be Ethernet, GigabitEthernet, Loopback or VLAN-interface.

preference: Route preference, in the range of 1 to 255 and defaulting to 1.

order-number: Match order for routes on the same segment, in the range of 1 to 100.

Description Use the **ip rpf-route-static** command to configure a multicast static route.

Use the **undo ip rpf-route-static** command to delete a multicast static route from the multicast static routing table.

By default, no multicast static route is configured.

Note that:

- The arguments *source-address { mask | mask-length }, protocol* and *policy-name* are critical elements in multicast static route configuration. The variation of any of these three arguments results in a different configuration.
- In the configuration, you can use the **display multicast routing-table static** command to check whether the multicast static route information contains this configuration. If you find a match, modify the corresponding fields without changing the configuration sequence; otherwise, add a multicast static route.
- When configuring a multicast static route, you can specify an RPF neighbor only by providing an IP address (*rpf-nbr-address*) rather than an interface (*interface-type interface-number*) if the interface type of that router is Ethernet, GigabitEthernet, Loopback or VLAN-interface; instead, you can specify an RPF neighbor only by providing an address (*rpf-nbr-address*).
- Because outgoing interface iteration may fail or the specified interface may be in the down state, the multicast static route configured with this command may fail to take effect. Therefore, we recommend that you use the **display multicast routing-table static** command after you configure a multicast static route to check whether the route has been successfully configured or whether the route has taken effect.

Related commands: **display multicast routing-table static.**

Examples # Configure a multicast static route.

```
<Sysname> system-view
[Sysname] ip rpf-route-static 1.0.0.0 255.0.0.0 rip 1 route-policy map1 11.0.0.1
```

mtracert

Syntax **mtracert** *source-address* [[*last-hop-router-address*] *group-address*]

View Any view

Parameters *source-address*: Specifies a multicast source address.

group-address: Specifies a multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

last-hop-router-address: Specifies a last-hop router address, which is the IP address of the local router by default.

Description Use the **mtracert** command to trace the path down which the multicast traffic from a given multicast source flows to the last-hop router.

Note that if the *last-hop-router-address* argument is given in the command to trace the path for a specific (S, G) multicast stream, the interface corresponding to the last-hop router address must be the outgoing interface for the (S, G) multicast stream; otherwise the multicast traceroute will fail.

Examples # Trace the path down which the (6.6.6.6, 225.2.1.1) multicast traffic flows from the multicast source to the last-hop router with the (S, G) outgoing interface address of 5.5.5.8.

```
<Sysname> mtracert 6.6.6.6 5.5.5.8 225.2.1.1
Type Ctrl+C to quit mtrace facility
Tracing reverse path of (6.6.6.6, 225.2.1.1) from last-hop router (5.5.5.8) to source via mult
icast routing-table

-1 5.5.5.8
  Incoming interface address: 4.4.4.8
  Previous-hop router address: 4.4.4.7
  Input packet count on incoming interface: 17837
  Output packet count on outgoing interface: 0
  Total number of packets for this source-group pair: 8000
  Protocol: PIM
  Forwarding TTL: 0
  Forwarding code: No error

-2 4.4.4.7
  Incoming interface address: 6.6.6.7
  Previous-hop router address: 0.0.0.0
  Input packet count on incoming interface: 2
  Output packet count on outgoing interface: 259
  Total number of packets for this source-group pair: 8100
  Protocol: PIM
  Forwarding TTL: 0
  Forwarding code: No error
```

Table 179 Field descriptions of the mtracert command

| Field | Description |
|--|---|
| last-hop router | Last-hop router |
| (6.6.6.6, 225.2.1.1) | The (S, G) multicast stream for which the forwarding path is being traced |
| -1 5.5.5.8 | The (S, G) outgoing interface address of each hop, starting from the last-hop router |
| Incoming interface address | The address of the interface on which the (S, G) packets arrive |
| Previous-hop router address | The IP address of the router from which this router receives packets from this source |
| Input packet count on incoming interface | The total number of multicast packets received on the incoming interface |
| Output packet count on outgoing interface | The total number of multicast packets transmitted on the outgoing interface |
| Total number of packets for this source-group pair | The total number of packets from the specified source forwarded by this router to the specified group |

Table 179 Field descriptions of the mtracert command

| Field | Description |
|-----------------|--|
| Protocol | The multicast routing protocol in use between this router and the previous hop router |
| Forwarding TTL | The minimum TTL that a packet is required to have before it can be forwarded over the outgoing interface |
| Forwarding code | Forwarding code |

multicast boundary

Syntax **multicast boundary** *group-address* { *mask* | *mask-length* }

undo multicast boundary { *group-address* { *mask* | *mask-length* } | **all** }

View Interface view

Parameters *group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group address.

mask-length: Mask length of the multicast group address, in the range of 4 to 32.

all: Specifies to remove all forwarding boundaries configured on the interface.

Description Use the **multicast boundary** command to configure a multicast forwarding boundary.

Use the **undo multicast boundary** command to remove a multicast forwarding boundary.

By default, no multicast forwarding boundary is configured.

Note that:

- A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified range. If the destination address of a multicast packet matches the set boundary condition, the packet will not be forwarded.
- If an interface needs to act as a forwarding boundary for multiple multicast groups, just carry out this command on the interface once for each group.
- Assume that Set A and Set B are both multicast forwarding boundary sets to be configured, and B is a subset of A. If A has been configured on an interface, it is not allowed to configure B on the interface; if B has been configured on the interface before A is configured, the previously configured B will be removed.

Related commands: **display multicast boundary.**

Examples # Configure VLAN-interface 100 to be the forwarding boundary of multicast group 239.2.0.0/16.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] multicast boundary 239.2.0.0 16
```

multicast forwarding-table downstream-limit

Syntax **multicast forwarding-table downstream-limit** *limit*
undo multicast forwarding-table downstream-limit

View System view

Parameters *limit*: Maximum number of downstream nodes (namely, the maximum number of outgoing interfaces) for a single route in the multicast forwarding table. The value ranges from 0 to the maximum allowable number.

Description Use the **multicast forwarding-table downstream-limit** command to configure the maximum number of downstream nodes for a single route in the multicast forwarding table.

Use the **undo multicast forwarding-table downstream-limit** command to restore the system default.

By default, the maximum number of downstream nodes for a single route in the multicast forwarding table is 128.

Related commands: **display multicast forwarding-table.**

Examples # Set the maximum number of downstream nodes for a single route in the multicast forwarding table to 120.

```
<Sysname> system-view
[Sysname] multicast forwarding-table downstream-limit 120
```

multicast forwarding-table route-limit

Syntax **multicast forwarding-table route-limit** *limit*
undo multicast forwarding-table route-limit

View System view

Parameters *limit*: Maximum number of route entries in the multicast forwarding table. The value ranges 0 to the maximum allowable number.

Description Use the **multicast forwarding-table route-limit** command to configure the maximum number of route entries in the multicast forwarding table.

Use the **undo multicast forwarding-table route-limit** command to restore the maximum number of route entries in the multicast forwarding table to the system default.

By default, the maximum number of route entries in the multicast forwarding table is 1000.

Related commands: **display multicast forwarding-table.**

Examples # Set the maximum number of routing entries in the multicast forwarding table to 200.

```
<Sysname> system-view
[Sysname] multicast forwarding-table route-limit 200
```

multicast load-splitting

Syntax **multicast load-splitting { source | source-group }**

undo multicast load-splitting

View System view

Parameters **source:** Specifies to implement per-source load splitting.

source-group: Specifies to implement per-source and per-group load splitting simultaneously.

Description Use the **multicast load-splitting** command to enable load splitting of multicast traffic.

Use the **undo multicast load-splitting** command to disable load splitting of multicast traffic.

By default, load splitting of multicast traffic is disabled.

Examples # Enable per-source load splitting of multicast traffic.

```
<Sysname> system-view
[Sysname] multicast load-splitting source
```

multicast longest-match

Syntax **multicast longest-match**

undo multicast longest-match

View System view

Parameters None

Description Use the **multicast longest-match** command to configure route selection based on the longest match, namely based on the mask length.

Use the **undo multicast longest-match** command to remove the configuration of route selection based on the longest match.

By default, routes are selected according to the order of route entries.

Examples # Configure route selection based on the longest match.

```
<Sysname> system-view
[Sysname] multicast longest-match
```

multicast routing-enable

Syntax **multicast routing-enable**
undo multicast routing-enable

View System view

Parameters None

Description Use the **multicast routing-enable** command to enable IP multicast routing.

Use the **undo multicast routing-enable** command to disable IP multicast routing.

IP multicast routing is disabled by default.

Note that:

- You must enable IP multicast routing before you can carry out other Layer 3 multicast commands.
- The device does not forward any multicast packets before IP multicast routing is enabled.

Examples # Enable IP multicast routing.

```
<Sysname> system-view
[Sysname] multicast routing-enable
```

reset multicast forwarding-table

Syntax **reset multicast forwarding-table** { { *source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View User view

- Parameters**
- source-address*: Multicast source address.
 - group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.
 - mask*: Mask of the multicast group/source address, 255.255.255.255 by default.
 - mask-length*: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.
 - incoming-interface**: Specifies to clear multicast forwarding entries of which the incoming interface is the specified one.
 - interface-type interface-number*: Specifies an interface by its type and number.
 - register**: Specifies the register interface of PIM-SM.
 - all**: Specifies to clear all the forwarding entries from the multicast forwarding table.

Description Use the **reset multicast forwarding-table** command to clear the multicast forwarding table information.

When a forwarding entry is deleted from the multicast forwarding table, the corresponding route entry is also deleted from the multicast routing table.

Related commands: **reset multicast routing-table, display multicast routing-table, display multicast forwarding-table.**

Examples # Clear the multicast forwarding entries related to multicast group 225.5.4.3 from the multicast forwarding table.

```
<Sysname> reset multicast forwarding-table 225.5.4.3
```

reset multicast routing-table

- Syntax** **reset multicast routing-table** { { *source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }
- View** User view
- Parameters**
- source-address*: Multicast source address.
 - group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.
 - mask*: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Specifies the incoming interface of multicast routing entries.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface.

all: Specifies to clear all the routing entries from the multicast routing table.

Description Use the **reset multicast routing-table** command to clear multicast routing entries from the multicast routing table.

When a route entry is deleted from the multicast routing table, the corresponding forwarding entry is also deleted from the multicast forwarding table.

Related commands: **reset multicast forwarding-table, display multicast routing-table, display multicast forwarding-table.**

Examples # Clear the route entries related to multicast group 225.5.4.3 from the multicast routing table.

```
<Sysname> reset multicast routing-table 225.5.4.3
```


44

802.1X CONFIGURATION COMMANDS

display dot1x

Syntax `display dot1x [sessions | statistics] [interface interface-list]`

View Any view

Parameters **sessions**: Displays 802.1x session information.

statistics: Displays 802.1x statistics.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **display dot1x** command to display information about 802.1x, including session information, statistics, or configuration.

With both the **sessions** keyword and the **statistics** keyword not provided, this command displays 802.1x configuration information.

Related commands: **reset dot1x statistics, dot1x, dot1x retry, dot1x max-user, dot1x port-control, dot1x port-method, dot1x timer.**

Examples # Display 802.1x configuration information.

```
<Sysname> display dot1x
Equipment 802.1X protocol is enabled
CHAP authentication is enabled
Proxy trap checker is disabled
Proxy logoff checker is disabled
EAD quick deploy is enabled
Configuration: Transmit Period 30 s, Handshake Period 15 s
                  Quiet Period 60 s, Quiet Period Timer is disabled
                  Supp Timeout 30 s, Server Timeout 100 s
                  The maximal retransmitting times 3
EAD quick deploy configuration:
                  URL: http://192.168.0.38
                  Free IP: 192.168.0.0 255.255.255.0
                  EAD timeout: 30 m
```

Total maximum 802.1x user resource number is 2048 per slot

```

Total current used 802.1x resource number is 0

Ethernet2/0/1 is link-up
 802.1X protocol is disabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 Handshake is disabled
 The port is an authenticator
 Authenticate Mode is Auto
 Port Control Type is Mac-based
 Guest VLAN: 0
 Max on-line user number is 256
 EAPOL Packet: Tx 0, Rx 0
 Sent EAP Request/Identity Packets : 0
   EAP Request/Challenge Packets: 0
   EAP Success Packets: 0, Fail Packets: 0
 Received EAPOL Start Packets : 0
   EAPOL LogOff Packets: 0
   EAP Response/Identity Packets : 0
   EAP Response/Challenge Packets: 0
   Error Packets: 0

Controlled User(s) amount to 0

```

Table 180 Field descriptions of the display dot1x command

| Field | Description |
|--|--|
| Equipment 802.1X protocol is enabled | Indicates whether 802.1x is enabled |
| CHAP authentication is enabled | Indicates whether CHAP authentication is enabled |
| Proxy trap checker is disabled | Indicates whether the device is configured to send a trap packet when detecting that a user is trying to login through a proxy |
| Proxy logoff checker is disabled | Indicates whether the device is configured to get offline any user trying to login through a proxy |
| EAD quick deploy is enabled | Indicates whether EAD quick deployment is enabled |
| Transmit Period | Setting of the username request timeout timer |
| Handshake Period | Setting of the handshake timer |
| Quiet Period | Setting of the quiet timer |
| Quiet Period Timer is disabled | Indicates whether the quiet timer is enabled |
| Supp Timeout | Setting of the supplicant timeout timer |
| Server Timeout | Setting of the server timeout timer |
| The maximal retransmitting times | Maximum number of attempts for the authenticator to send authentication requests to the supplicant |
| EAD quick deploy configuration | EAD quick deployment configurations |
| URL | Redirect URL for IE users |
| Free IP | Accessible network segment |
| EAD timeout | EAD rule timeout time |
| Total maximum 802.1x user resource number per slot | Maximum number of supplicants supported per board |
| Total current used 802.1x resource number | Total number of online users |
| Ethernet2/0/1 is link-up | Status of port Ethernet 2/0/1 |
| 802.1X protocol is disabled | Indicates whether 802.1x is enabled on the port |
| Proxy trap checker is disabled | Indicates whether the port is configured to send a trap packet when detecting that a user is trying to login through a proxy |

Table 180 Field descriptions of the display dot1x command

| Field | Description |
|-----------------------------------|--|
| Proxy logoff checker is disabled | Indicates whether the port is configured to get offline any user trying to login through a proxy |
| Handshake is disabled | Indicates whether handshake is enabled on the port |
| The port is an authenticator | Role of the port |
| Authenticate Mode is Auto | Access control mode for the port |
| Port Control Type is Mac-based | Access control method for the port |
| Guest VLAN | Guest VLAN configured for the port. The value of 0 means that no guest VLAN is configured. |
| Max on-line user number | Maximum number of users supported on the port |
| EAPOL Packet | Number of EAPOL packets received (Tx) or sent (Rx) |
| Sent EAP Request/Identity Packets | Number of EAP Request/Identity packets sent |
| EAP Request/Challenge Packets | Number of EAP Request/Challenge packets sent |
| EAP Success Packets | Number of EAP Success packets sent |
| Received EAPOL Start Packets | Number of EAPOL Start packets received |
| EAPOL LogOff Packets | Number of EAPOL LogOff packets received |
| EAP Response/Identity Packets | Number of EAP Response/Identity packets received |
| EAP Response/Challenge Packets | Number of EAP Response/Challenge packets received |
| Error Packets | Number of erroneous packets received |
| Controlled User(s) amount | Number of controlled users on the port |

dot1x

Syntax In system view:

```
dot1x [ interface interface-list ]
```

```
undo dot1x [ interface interface-list ]
```

In Ethernet interface view:

```
dot1x
```

```
undo dot1x
```

View System view, interface view

Parameters **interface** *interface-list*: Specifies a port list, which can contain multiple ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x** command in system view to enable 802.1x globally.

Use the **undo dot1x** command in system view to disable 802.1x globally.

Use the **dot1x interface** *interface-list* command in system view or the **dot1x** command in interface view to enable 802.1x for specified ports.

Use the **undo dot1x interface** *interface-list* command in system view or the **undo dot1x** command in interface view to disable 802.1x for specified ports.

By default, 802.1x is neither enabled globally nor enabled for any port.

Note that:

- 802.1x must be enabled both globally in system view and for the intended ports in system view or interface view. Otherwise, it does not function.
- You can configure 802.1x parameters either before or after enabling 802.1x.

Related commands: **display dot1x.**

Examples # Enable 802.1x for ports Ethernet 2/0/1, and Ethernet 2/0/5 to Ethernet 2/0/7.

```
<Sysname> system-view
[Sysname] dot1x interface Ethernet2/0/1 Ethernet2/0/5 to Ethernet2/0/7
```

Or

```
<Sysname> system-view
[Sysname] interface Ethernet2/0/1
[Sysname-Ethernet2/0/1] dot1x
[Sysname-Ethernet2/0/1] quit
[Sysname] interface Ethernet2/0/5
[Sysname-Ethernet2/0/5] dot1x
[Sysname-Ethernet2/0/5] quit
[Sysname] interface Ethernet2/0/6
[Sysname-Ethernet2/0/6] dot1x
[Sysname-Ethernet2/0/6] quit
[Sysname] interface Ethernet2/0/7
[Sysname-Ethernet2/0/7] dot1x
```

Enable 802.1x globally.

```
<Sysname> system-view
[Sysname] dot1x
```

dot1x authentication-method

Syntax **dot1x authentication-method** { **chap** | **eap** | **pap** }

undo dot1x authentication-method

View System view

Parameters **chap**: Authenticates supplicants using CHAP.

eap: Authenticates supplicants using EAP.

pap: Authenticates supplicants using PAP.

Description Use the **dot1x authentication-method** command to set the 802.1x authentication method.

Use the **undo dot1x authentication-method** command to restore the default.

By default, CHAP is used.

- The password authentication protocol (PAP) transports passwords in plain text.
- The challenge handshake authentication protocol (CHAP) transports only usernames over the network. Compared with PAP, CHAP provides better security.
- With EAP relay authentication, the authenticator encapsulates 802.1x user information in the EAP attributes of RADIUS packets and sends the packets to the RADIUS server for authentication; it does not need to repackage the EAP packets into standard RADIUS packets for authentication. In this case, you can configure the **user-name-format** command but it does not take effect. Currently, the device supports these EAP modes: EAP-TLS, EAP-TTLS, EAP-MD5, and PEAP. For more information refer to **user-name-format** on page 824.

Note that:

- Local authentication supports only PAP and CHAP.
- For RADIUS authentication, the RADIUS server must be configured accordingly to support PAP, CHAP, or EAP authentication.

Related commands: **display dot1x.**

Examples # Set the 802.1x authentication method to PAP.

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

dot1x guest-vlan

Syntax In system view:

dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan [**interface** *interface-list*]

In Ethernet interface view:

dot1x guest-vlan *vlan-id*

undo dot1x guest-vlan

View System view, Ethernet interface view

Parameters *vlan-id*: ID of the VLAN to be specified as the guest VLAN, in the range 1 to 4094.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description Use the **dot1x guest-vlan** command to configure the guest VLAN for specified or all ports.

Use the **undo dot1x guest-vlan** command to remove the guest VLAN(s) configured for specified or all ports.

By default, a port is configured with no guest VLAN.

In system view, this command configures guest VLAN for all ports with *interface-list* not provided, and configures guest VLAN for specified with *interface-list* provided.

In Ethernet interface view, you cannot specify the *interface-list* argument and can only configure guest VLAN for the current port.

For the guest VLAN feature to take effect on a port, make sure that:

- 802.1x is enabled.
- The port access control method is set to **portbased**. When the port access control method is **macbased**, you can configure a guest VLAN but your configuration will not take effect.
- The port access control mode is set to **auto**.
- The 802.1x multicast trigger function is enabled.
- The link type of the port is set to **access**.

Note that:

- Do not delete a VLAN that has been configured as a guest VLAN.
- You can specify a tagged VLAN as the guest VLAN for a Hybrid port, but the guest VLAN does not take effect. Similarly, if a guest VLAN for a Hybrid port is in operation, you cannot configure the guest VLAN to carry tags.

Examples # Specify port Ethernet 2/0/1 to use VLAN 999 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 999 interface Ethernet2/0/1
```

Specify ports Ethernet 2/0/2 to Ethernet 2/0/5 to use VLAN 10 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 10 interface Ethernet2/0/2 to Ethernet2/0/5
```

Specify all ports to use VLAN 7 as their guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 7
```

Specify port Ethernet 2/0/7 to use VLAN 3 as its guest VLAN.

```
<Sysname> system-view
[Sysname] interface Ethernet2/0/7
[Sysname-Ethernet2/0/7] dot1x guest-vlan 3
```

dot1x handshake

Syntax **dot1x handshake**

undo dot1x handshake

View Interface view

Parameters None

Description Use the **dot1x handshake** command to enable the online user handshake function so that the device can periodically send handshake messages to the client to check whether a user is online.

Use the **undo dot1x handshake** command to disable the function.

By default, the function is enabled.

Note that the 802.1x proxy detection function depends on the online user handshake function. Be sure to enable handshake before enabling proxy detection and to disable proxy detection before disabling handshake.

Examples # Enable online user handshake.

```
<Sysname> system-view
[Sysname] interface Ethernet2/0/4
[Sysname-Ethernet2/0/4] dot1x handshake
```

dot1x max-user

Syntax In system view:

dot1x max-user *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

In Ethernet interface view:

dot1x max-user *user-number*

undo dot1x max-user

View System view, Ethernet interface view

Parameters *user-number*: Maximum number of users to be supported simultaneously. The valid range is from 1 to 1024.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description Use the **dot1x max-user** command to set the maximum number of users to be supported simultaneously for specified or all ports.

Use the **undo dot1x max-user** command to restore the default.

By default, the maximum number of concurrent users supported on a port is 1024.

With no interface specified, the command sets the threshold for all ports.

Related commands: **display dot1x.**

Examples # Configure port Ethernet 2/0/1 to support up to 32 concurrent users.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface Ethernet2/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface Ethernet2/0/1
[Sysname-Ethernet2/0/1] dot1x max-user 32
```

dot1x multicast-trigger

Syntax **dot1x multicast-trigger**
undo dot1x multicast-trigger

View Interface view

Parameters None

Description Use the **dot1x multicast-trigger** command to enable the multicast trigger function of 802.1x to send multicast trigger messages to the clients periodically.

Use the **undo dot1x multicast-trigger** command to disable this function.

By default, the multicast trigger function is enabled.

Related commands: **display dot1x.**

Examples # Disable the multicast trigger function for port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] undo dot1x multicast-trigger
```

dot1x port-control

Syntax In system view:

```
dot1x port-control { authorized-force | auto | unauthorized-force }
[ interface interface-list ]
```

```
undo dot1x port-control [ interface interface-list ]
```

In Ethernet interface view:

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

```
undo dot1x port-control
```

View System view, Ethernet interface view

Parameters **authorized-force**: Places the specified or all ports in the state of authorized, allowing users of the ports to access the network without authentication.

auto: Places the specified or all ports in the state of unauthorized initially to allow only EAPOL frames to pass, and turns the ports into the state of authorized to allow access to the network after the users pass authentication. This is the most common choice.

unauthorized-force: Places the specified or all ports in the state of unauthorized, denying any access requests from users of the ports.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description Use the **dot1x port-control** command to set the access control mode for specified or all ports.

Use the **undo dot1x port-control** command to restore the default.

The default access control mode is **auto**.

Related commands: **display dot1x.**

Examples # Set the access control mode of port Ethernet 2/0/1 to **unauthorized-force**.

```
<Sysname> system-view
[Sysname] dot1x port-control unauthorized-force interface Ethernet2/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface Ethernet2/0/1
[Sysname-Ethernet2/0/1] dot1x port-control unauthorized-force
```

dot1x port-method

Syntax In system view:

dot1x port-method { **macbased** | **portbased** } [**interface** *interface-list*]

undo dot1x port-method [**interface** *interface-list*]

In Ethernet interface view:

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

View System view, Ethernet interface view

Parameters **macbased**: Specifies to use the **macbased** authentication method. With this method, each user of a port must be authenticated separately, and when an authenticated user goes offline, no other users are affected.

portbased: Specifies to use the **portbased** authentication method. With this method, after the first user of a port passes authentication, all other users of the port can access the network without authentication, and when the first user goes offline, all other users get offline at the same time.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description Use the **dot1x port-method** command to set the access control method for specified or all ports.

Use the **undo dot1x port-method** command to restore the default.

The default access control method is **macbased**.

Related commands: **display dot1x.**

Examples # Set the access control method to **portbased** for port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] dot1x port-method portbased interface Ethernet2/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface Ethernet2/0/1
[Sysname-Ethernet2/0/1] dot1x port-method portbased
```

dot1x quiet-period

Syntax **dot1x quiet-period**
undo dot1x quiet-period

View System view

Parameters None

Description Use the **dot1x quiet-period** command to enable the quiet timer function.
Use the **undo dot1x quiet-period** command to disable the function.
By default, the function is disabled.
After a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in the period dictated by the quiet timer.

Related commands: **display dot1x, dot1x timer.**

Examples # Enable the quiet timer.

```
<Sysname> system-view
[Sysname] dot1x quiet-period
```

dot1x retry

Syntax **dot1x retry** *max-retry-value*
undo dot1x retry

View System view

Parameters *max-retry-value*: Maximum number of attempts to send an authentication request to a supplicant, in the range 1 to 10.

Description Use the **dot1x retry** command to set the maximum number of attempts to send an authentication request to a supplicant.

Use the **undo dot1x retry** command to restore the default.

By default, the authenticator can send an authentication request to a supplicant for up to twice.

Note that after sending an authentication request to a supplicant, the authenticator may retransmit the request if it does not receive any response at an interval specified by the username request timeout timer or supplicant timeout timer. The number of retransmission attempts is one less than the value set by this command.

Related commands: **display dot1x.**

Examples # Set the maximum number of attempts to send an authentication request to a supplicant as 9.

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

dot1x supp-proxy-check

Syntax In system view:

```
dot1x supp-proxy-check { logoff | trap } [ interface interface-list ]
```

```
undo dot1x supp-proxy-check { logoff | trap } [ interface interface-list ]
```

In Ethernet interface view:

```
dot1x supp-proxy-check { logoff | trap }
```

```
undo dot1x supp-proxy-check { logoff | trap }
```

View System view, Ethernet interface view

Parameters **logoff**: Gets offline any user trying to login through a proxy.

trap: Sends a trap to the network management system when detecting that a user is trying to login through a proxy.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x supp-proxy-check** command to enable detection and control of users logging in through proxies for specified or all ports.

Use the **undo dot1x supp-proxy-check** command to disable the function for specified or all ports.

By default, the function is disabled.

Note that:

- This function requires the cooperation of the 802.1x client program by 3Com.
- In system view, this command enables detection and control of users' login for all ports with *interface-list* not provided, and enables detection and control of users' login for specified with *interface-list* provided.
- In Ethernet interface view, you cannot specify the *interface-list* argument and can only enable detection and control of users' login for the current port.
- This function must be enabled both globally in system view and for the intended ports in system view or Ethernet interface view. Otherwise, it does not work.

Related commands: **display dot1x.**

Examples # Configure ports Ethernet 2/0/1 to Ethernet 2/0/8 to get offline users trying to login through proxies.

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check logoff
[Sysname] dot1x supp-proxy-check logoff interface Ethernet2/0/1 to Ethernet2/0/8
```

Configure port Ethernet 2/0/9 to send a trap packet when detecting that a user is trying to login through a proxy.

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] dot1x supp-proxy-check trap interface Ethernet2/0/9
```

Or

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] interface Ethernet2/0/9
[Sysname-Ethernet2/0/9] dot1x supp-proxy-check trap
```

dot1x timer

Syntax **dot1x timer** { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **server-timeout** | **supp-timeout** | **tx-period** }

View System view

Parameters *handshake-period-value*: Setting for the handshake timer in seconds. It ranges from 5 to 1024 and defaults to 15.

quiet-period-value: Setting for the quiet timer in seconds. It ranges from 10 to 120 and defaults to 60.

server-timeout-value: Setting for the server timeout timer in seconds. It ranges from 100 to 300 and defaults to 100.

supp-timeout-value: Setting for the supplicant timeout timer in seconds. It ranges from 10 to 120 and defaults to 30.

tx-period-value: Setting for the username request timeout timer in seconds. It ranges from 10 to 120 and defaults to 30.

Description Use the **dot1x timer** command to set 802.1x timers.

Use the **undo dot1x timer** command to restore the defaults.

Several timers are used in the 802.1x authentication process to guarantee that the supplicants, the authenticators, and the RADIUS server interact with each other in a reasonable manner. You can use this command to set these timers:

- Handshake timer (handshake-period): After a supplicant passes authentication, the authenticator sends to the supplicant handshake requests at this interval to check whether the supplicant is online. If the authenticator receives no response after sending the allowed maximum number of handshake requests, it considers that the supplicant is offline.
- Quiet timer (quiet-period): When a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in this period of time.
- Server timeout timer (server-timeout): Once an authenticator sends a RADIUS Access-Request packet to the authentication server, it starts this timer. If this timer expires but it receives no response from the server, it retransmits the request.
- Supplicant timeout timer (supp-timeout): Once an authenticator sends an EAP-Request/MD5 Challenge frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request.
- Username request timeout timer (tx-period): Once an authenticator sends an EAP-Request/Identity frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request. In addition, to be compatible with clients that do not send EAPOL-Start requests unsolicitedly, the device multicasts EAP-Request/Identity frame periodically to detect the clients, with the multicast interval defined by tx-period.

Generally, it is unnecessary to change the timers unless in some special or extreme network environments.

Related commands: **display dot1x.**

Examples # Set the server timeout timer to 150 seconds.
 <Sysname> system-view
 [Sysname] dot1x timer server-timeout 150

reset dot1x statistics

Syntax **reset dot1x statistics** [**interface** *interface-list*]

View User view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **reset dot1x statistics** command to clear 802.1x statistics.

With the **interface** *interface-list* argument specified, the command clears 802.1x statistics on the specified ports. With the argument unspecified, the command clears global 802.1x statistics and 802.1x statistics on all ports.

Related commands: **display dot1x.**

Examples # Clear 802.1x statistics on port Ethernet 2/0/1.
 <Sysname> reset dot1x statistics interface Ethernet2/0/1

45

EAD FAST DEPLOYMENT CONFIGURATION COMMANDS

dot1x free-ip

Syntax **dot1x free-ip** *ip-address* { *mask-address* | *mask-length* }
undo dot1x free-ip { *ip-address* { *mask* | *mask-length* } | **all** }

View System view

Parameters *ip-address*: IP address of the freely accessible network segment, also called a free IP.

mask: Mask of the freely accessible network segment.

mask-length: Length of the mask of the freely accessible network segment.

Description Use the **dot1x free-ip** command to configure a freely accessible network segment, that is, a network segment that users can access before passing 802.1x authentication.

Use the **undo dot1x free-ip** command to remove one or all freely accessible network segments.

By default, no freely accessible network segment is configured.

Note that:

- The free IP function is mutually exclusive with the global MAC authentication function and the port security function.
- The free IP function is effective only when the port access control mode is **auto**.
- The maximum number of freely accessible network segments varies by device.

Related commands: **display dot1x**.

Examples # Configure 192.168.0.0 as a freely accessible network segment.

```
<Sysname> system-view  
[Sysname] dot1x free-ip 192.168.0.0 24
```

dot1x timer ead-timeout

Syntax **dot1x timer ead-timeout** *ead-timeout-value*

undo dot1x timer ead-timeout

View System view

Parameters *ead-timeout-value*: EAD rule timeout time, in the range 1 minute to 1440 minutes.

Description Use the **dot1x timer ead-timeout** command to set the EAD rule timeout time.

Use the **undo dot1x timer ead-timeout** command to restore the default.

By default, the timeout time is 30 minutes.

Related commands: **display dot1x.**

Examples # Set the EAD rule timeout time to 5 minutes.

```
<Sysname> system-view
[Sysname] dot1x timer ead-timeout 5
```

dot1x url

Syntax **dot1x url** *url-string*

undo dot1x [*url-string*]

View System view

Parameters *url-string*: Redirect URL, a case-sensitive string of 1 to 64 characters in the format `http://string`.

Description Use the **dot1x url** command to configure a URL to which the system redirects users' HTTP access before they pass 802.1x authentication.

Use the **undo dot1x url** command to remove the redirect URL.

By default, no redirect URL is defined.

Note that:

- The redirect URL and the free IP must be in the same network segment; otherwise, the URL may be inaccessible.
- You can configure the **dot1x url** command for more than once but only the last one takes effect.

Related commands: **display dot1x, dot1x free-ip.**

Examples # Configure the redirect URL as http://192.168.0.1.
<Sysname> system-view
[Sysname] dot1x url http://192.168.0.1

46

MAC AUTHENTICATION CONFIGURATION COMMANDS

display mac-authentication

Syntax `display mac-authentication [interface interface-list]`

View Any view

Parameter `interface interface-list`: Specifies an Ethernet port list, in the format of { `interface-type interface-number [to interface-type interface-number]` }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the `to interface-type interface-number` portion comprises only one port. With an interface range, the end interface number and the start interface number must be of the same type and the former must be greater than the latter.

Description Use the `display mac-authentication` command to display global MAC authentication information or MAC authentication information about specified ports.

Examples # Display global MAC authentication information.

```
<Sysname> display mac-authentication
MAC address authentication is enabled.
User name format is MAC address, like xxxxxxxxxxxxxx
Fixed username:mac
Fixed password:not configured
    Offline detect period is 300s
    Quiet period is 60s.
    Server response timeout value is 100s
    the max allowed user number is 2048 per slot
    Current user number amounts to 0
    Current domain: not configured, use default domain

Silent Mac User info:
      MAC ADDR                From Port          Port Index
Ethernet2/0/1 is link-up
  MAC address authentication is Enabled
  Authenticate success: 0, failed: 0
  Current online user number is 0
MAC ADDR          Authenticate state          AuthIndex
.....(omitted)
```

Table 181 Field descriptions of the display mac-authentication command

| Field | Description |
|--|---|
| MAC address authentication is Enabled | Whether MAC authentication is enabled |
| User name format is MAC address, like xxxxxxxxxxxx | The username is in format of MAC address, like xxxxxxxxxxxx |
| Fixed username: | Fixed username |
| Fixed password: | Password of the fixed username |
| Offline detect period | Setting of the offline detect timer |
| Quiet period | Setting of the quiet timer |
| Server response timeout value | Setting of the server timeout timer |
| the max allowed user number | Maximum number of users each slot in the device supports |
| Current user number amounts to | Total number of online users |
| Current domain: not configured, use default domain | Currently used ISP domain |
| Silent Mac User info | Information on users who are kept silent after failing MAC authentication |
| Ethernet2/0/1 is link-up | Status of the link on port Ethernet 2/0/1 |
| MAC address authentication is Enabled | Whether MAC authentication is enabled on port Ethernet 2/0/1 |
| Authenticate success: 0, failed: 0 | MAC authentication statistics, including the number of successful authentication attempts and that of unsuccessful authentication attempts |
| Current online user number | Number of online users on the port |
| MAC ADDR | Online user MAC address |
| Authenticate state | User status. Possible values are: <ul style="list-style-type: none"> ■ CONNECTING: The user is logging in. ■ SUCCESS: The user has passed the authentication. ■ FAILURE: The user failed the authentication. ■ LOGOFF: The user has logged off. |
| AuthIndex | Authenticator Index |

mac-authentication

Syntax `mac-authentication [interface interface-list]`

`undo mac-authentication [interface interface-list]`

View System view, Ethernet interface view

Parameters `interface interface-list`: Specifies an Ethernet port list, in the format of `{ interface-type interface-number [to interface-type interface-number] }&<1-10>`, where `&<1-10>` indicates that you can specify up to 10 port ranges. A port range defined without the `to interface-type interface-number` portion comprises only one port.

Description Use the **mac-authentication** command to enable MAC authentication globally or for one or more ports.

Use the **undo mac-authentication** command to disable MAC authentication globally or for one or more ports.

By default, MAC authentication is neither enabled globally nor enabled on any port.

Note that:

- In system view, if you provide the *interface-list* argument, the command enables MAC authentication for the specified ports; otherwise, the command enables MAC authentication globally. In Ethernet interface view, the command enables MAC authentication for the port without requiring the *interface-list* argument.
- You can configure MAC authentication parameters globally or for specified ports either before or after enabling MAC authentication. If no MAC authentication parameters are configured before MAC authentication is enabled globally, the default values are used.
- You can enable MAC authentication for ports before enabling it globally. However, MAC authentication begins to function only after you also enable it globally.

Examples # Enable MAC authentication globally.

```
<Sysname> system-view
[Sysname] mac-authentication
Mac-auth is enabled globally.
```

Enable MAC authentication for port Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] mac-authentication interface Ethernet 2/0/1
Mac-auth is enabled on port Ethernet2/0/1.
```

Or

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] mac-authentication
Mac-auth is enabled on port Ethernet2/0/1.
```

mac-authentication domain

Syntax **mac-authentication domain** *isp-name*

undo mac-authentication domain

View System view

- Parameters** *isp-name*: ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain any forward slash (/), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>), and @.
- Description** Use the **mac-authentication domain** command to specify the ISP domain for MAC authentication.
- Use the **undo mac-authentication domain** command to restore the default.
- By default, the default ISP domain (system) is used.
- Examples** # Specify the ISP domain for MAC authentication as domain1.
- ```
<Sysname> systme-view
[Sysname] mac-authentication domain domain1
```

## mac-authentication timer

- Syntax** **mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }
- undo mac-authentication timer** { **offline-detect** | **quiet** | **server-timeout** }
- View** System view
- Parameters** **offline-detect** *offline-detect-value*: Specifies the offline detect interval, in the range 60 to 65,535 seconds.
- quiet** *quiet-value*: Specifies the quiet period, in the range 1 to 3,600 seconds.
- server-timeout** *server-timeout-value*: Specifies the server timeout period, in the range 100 to 300 seconds.
- Description** Use the **mac-authentication timer** command to set the MAC authentication timers.
- Use the **undo mac-authentication timer** command to restore the defaults.
- By default, the offline detect interval is 300 seconds, the quiet period is 60 seconds, and the server timeout period is 100 seconds.
- The following timers function in the process of MAC authentication:
- Offline detect timer: At this interval, the device checks to see whether an online user has gone offline. Once detecting that a user becomes offline, the device sends to the RADIUS server a stop accounting notice.
  - Quiet timer: Whenever a user fails MAC authentication, the device does not initiate any MAC authentication of the user during such a period.
  - Server timeout timer: During authentication of a user, if the device receives no response from the RADIUS server in this period, it assumes that its connection



to the RADIUS server has timed out and forbids the user from accessing the network.

**Related commands:** **display mac-authentication.**

**Examples** # Set the server timeout timer to 150 seconds.

```
<Sysname> systme-view
[Sysname] mac-authentication timer server-timeout 150
```

---

## mac-authentication user-name-format

**Syntax** **mac-authentication user-name-format** { **fixed** [ **account** *name* ] [ **password** { **cipher** | **simple** } *password* ] | **mac-address** [ **with-hyphen** | **without-hyphen** ] }

**undo mac-authentication user-name-format**

**View** System view

**Parameters** **fixed:** Uses the MAC authentication username type of fixed username.

**account** *name:* Specifies the fixed username. The *name* argument is a case-insensitive string of 1 to 55 characters and defaults to mac.

**password** { **cipher** | **simple** } *password:* Specifies the password for the fixed username. Using the **cipher** keyword displays the password in cipher text. Using the **simple** keyword displays the password in plain text. In the former case, the password can be either a string of 1 to 63 characters in plain text or a string of 24 or 88 characters in cipher text. In the latter case, the password must be a string of 1 to 63 characters in plain text.

**mac-address:** Adopts the user's source MAC address as the username, which is case-insensitive.

**with-hyphen:** Indicates that the MAC address must include "-", like xx-xx-xx-xx-xx-xx. The letters in the address must be in lower case.

**without-hyphen:** Indicates that the MAC address must not include "-", like xxxxxxxxxxxx. The letters in the address must be in lower case.

**Description** Use the **mac-authentication user-name-format** command to configure the username and password for MAC authentication.

Use the **undo mac-authentication user-name-format** command to restore the default.

By default, a user's source MAC address is used as the username and password, and the MAC address does not contain hyphen "-".

Note that:

- When the user's source MAC address is used as the username, the password is also that MAC address.
- In cipher display mode, a password in plain text with no more than 16 characters will be encrypted into a password in cipher text with 24 characters, and a password in plain text with 16 to 63 characters will be encrypted into a password in cipher text with 88 characters. For a password with 24 characters, the system will determine whether it can decrypt the password. If so, it treats the password as a cipher-text one. Otherwise, it treats it as a plain-text one.

**Related commands:** **display mac-authentication.**

**Examples** # Configure the username for MAC authentication as abc, and the password displayed in plain text as xyz.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

---

## reset mac-authentication statistics

**Syntax** **reset mac-authentication statistics** [ **interface** *interface-list* ]

**View** User view

**Parameters** **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

**Description** Use the **reset mac-authentication statistics** command to clear MAC authentication statistics.

Note that:

- If you do not specify the *interface-list* argument, the command clears the global MAC authentication statistics and the MAC authentication statistics on all ports.
- If you specify the *interface-list* argument, the command clears the MAC authentication statistics on the specified ports.

**Related commands:** **display mac-authentication.**

**Examples** # Clear MAC authentication statistics on Ethernet 2/0/1.

```
<Sysname> reset mac-authentication statistics interface Ethernet2/0/1
```

# 47

## AAA CONFIGURATION COMMANDS

---

### access-limit

**Syntax** `access-limit { disable | enable max-user-number }`  
`undo access-limit`

**View** ISP domain view

**Parameters** **disable**: Specifies that the system do not limit the number of accessing users in the current ISP domain.

**enable** *max-user-number*: Specifies that the system limit the number of accessing users in the current ISP domain. *max-user-number* is the maximum number of accessing users in the current ISP domain. The valid range is from 1 to 4096.

**Description** Use the **access-limit enable** command to set the maximum number of accessing users allowed by an ISP domain.

Use the **undo access-limit** or **access-limit disable** command to remove the limitation.

By default, there is no limit to the amount of supplicants in an ISP domain.

As the supplicants may compete for network resources, setting a proper limit to the amount of accessing users helps in providing a reliable system performance.

**Examples** # Set a limit of 500 supplicants for ISP domain aabbcc.net.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] access-limit enable 500
```

---

### accounting default

**Syntax** `accounting default { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }`  
`undo accounting default`

**View** ISP domain view

**Parameters** **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local accounting.

**none**: Does not perform any accounting.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **accounting default** command to specify the default accounting scheme for all types of users.

Use the **undo accounting default** command to restore the default.

By default, the accounting scheme is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The accounting scheme specified with the **accounting default** command is for all types of users and has a priority lower than that for a specific access mode.
- Local accounting is only for managing the local user connection number; it does not provide the statistics function. The local user connection number management is only for local accounting; it does not affect local authentication and authorization.
- With the access mode of login, accounting is not supported for FTP services.

**Related commands:** **authentication default, authorization default, hwtacacs scheme, radius scheme.**

**Examples** # Configure the default ISP domain **system** to use the local accounting scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting default local
```

# Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for all types of users and to use the local accounting scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting default radius-scheme rd local
```

---

**accounting lan-access**

**Syntax** **accounting lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [ **local** ] }

**undo accounting lan-access**

**View** ISP domain view

**Parameters** **local**: Performs local accounting.

**none**: Does not perform any accounting.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **accounting lan-access** command to specify the accounting scheme for LAN access users.

Use the **undo accounting lan-access** command to restore the default.

By default, the default accounting scheme is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

**Related commands:** **accounting default, radius scheme.**

**Examples** # Configure the default ISP domain **system** to use the local accounting scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting lan-access local
```

# Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for LAN access users and to use the local accounting scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting lan-access radius-scheme rd local
```

---

**accounting login**

**Syntax** **accounting login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] | **local** | **none** | **radius-scheme** *radius-scheme-name* [ **local** ] }

**undo accounting login**

**View** ISP domain view

**Parameters** **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local accounting.

**none**: Does not perform any accounting.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **accounting login** command to specify the accounting scheme for login users.

Use the **undo accounting login** command to restore the default.

By default, the default accounting scheme is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

**Related commands:** **accounting default**, **hwtacacs scheme**, **radius scheme**.

**Examples** # Configure the default ISP domain **system** to use the local accounting scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login local
```

# Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for login users and to use the local accounting scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login radius-scheme rd local
```

---

## accounting optional

**Syntax** **accounting optional**

**undo accounting optional**

**View** ISP domain view

**Parameters** None

**Description** Use the **accounting optional** command to enable the accounting optional feature.

Use the **undo accounting optional** command to disable the feature.

By default, the feature is disabled.

Note that:

- With the **accounting optional** command configured, a user that will be disconnected otherwise can use the network resources even when there is no available accounting server or the communication with the current accounting server fails. This command is normally used when authentication is required but accounting is not.
- If you configure the **accounting optional** command for a domain, the device does not send real-time accounting updates for users of the domain any more after accounting fails.
- With the **accounting optional** command configured, the limit on the number of local user connections configured by the **attribute access-limit** command is not effective.

**Examples** # Enable the accounting optional feature for users in domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] accounting optional
```

## accounting portal

**Syntax** **accounting portal** { **none** | **radius-scheme** *radius-scheme-name* }

**undo accounting portal**

**View** ISP domain view

**Parameters** **none**: Does not perform any accounting.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **accounting portal** command to specify the accounting scheme for portal users.

Use the **undo accounting portal** command to restore the default.

By default, the default accounting scheme is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

**Related commands:** **accounting default**, **radius scheme**.

**Examples** # In the default ISP domain **system**, specify the accounting scheme for portal users to RADIUS scheme, with the name **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting portal radius-scheme rd
```

---

**attribute**

**Syntax** **attribute** { **access-limit** *max-user-number* | **idle-cut** *minute* | **ip** *ip-address* | **location** { [ **nas-ip** *ip-address* ] **port** *slot-number subslot-number port-number* } | **mac** *mac-address* | **vlan** *vlan-id* } \*

**undo attribute** { **access-limit** | **idle-cut** | **ip** | **location** | **mac** | **vlan** } \*

**View** Local user view

**Parameters** **access-limit** *max-user-number*: Specifies the maximum number of concurrent users that can log in using the current username, which ranges from 1 to 1024.

**idle-cut** *minute*: Configures the idle cut function. The idle cut period ranges from 1 to 120, in minutes.

**ip** *ip-address*: Specifies the IP address of the user.

**location**: Specifies the port binding attribute of the user.

**nas-ip** *ip-address*: Specifies the IP address of the port of the remote access server bound by the user. The default is 127.0.0.1, that is, the device itself. This keyword and argument combination is required only when the user is bound to a remote port.

**port** *slot-number subslot-number port-number*: Specifies the port to which the user is bound. The value of *slot-number* and *subslot-number* both range from 0 to 15. The value of *port-number* ranges from 0 to 255. The ports bounded are determined by port number, regardless of port type.

**mac** *mac-address*: Specifies the MAC address of the user in the format of *H-H-H*.

**vlan** *vlan-id*: Specifies the VLAN to which the user belongs. The *vlan-id* argument is an integer in the range 1 to 4094.

**Description** Use the **attribute** command to set some of the attributes for a LAN access user.

Use the **undo attribute** command to remove the configuration.

Note that:

- The **attribute access-limit** command for local users is effective only after local accounting scheme is configured.
- The **attribute ip** command for local users is applicable only to the authentication supporting IP address upload, for example, 802.1x authentication. If this command is configured for the authentication that does not support IP address upload, for example, MAC authentication, local authentication may fail.
- The **idle-cut** command in user interface view applies to lan-access users only.

**Related commands:** **display local-user**.



**Examples** # Set the IP address of local user user1 to 10.110.50.1.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] attribute ip 10.110.50.1
```

---

## authentication default

**Syntax** **authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] | **local** | **none** | **radius-scheme** *radius-scheme-name* [ **local** ] }

**undo authentication default**

**View** ISP domain view

**Parameters** **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local authentication.

**none**: Does not perform any authentication.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **authentication default** command to specify the default authentication scheme for all types of users.

Use the **undo authentication default** command to restore the default.

By default, the authentication scheme is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The authentication scheme specified with the **authentication default** command is for all types of users and has a priority lower than that for a specific access mode.

**Related commands:** **authorization default**, **accounting default**, **hwtacacs scheme**, **radius scheme**.

**Examples** # Configure the default ISP domain **system** to use the local authentication scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication default local
```

# Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for all types of users and to use the local authentication scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication default radius-scheme rd local
```

---

## authentication lan-access

**Syntax** **authentication lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [ **local** ] }

**undo authentication lan-access**

**View** ISP domain view

**Parameters** **local**: Performs local authentication.

**none**: Does not perform any authentication.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **authentication lan-access** command to specify the authentication scheme for LAN access users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication scheme is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

**Related commands:** **authentication default**, **radius scheme**.

**Examples** # Configure the default ISP domain **system** to use the local authentication scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication lan-access local
```

# Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for LAN access users and to use the local authentication scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication lan-access radius-scheme rd local
```

---

**authentication login**

**Syntax** **authentication login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] | **local** | **none** | **radius-scheme** *radius-scheme-name* [ **local** ] }

**undo authentication login**

**View** ISP domain view

**Parameters** **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local authentication.

**none**: Does not perform any authentication.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **authentication login** command to specify the authentication scheme for login users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication scheme is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

**Related commands:** **authentication default, hwtacacs scheme, radius scheme.**

**Examples** # Configure the default ISP domain **system** to use the local authentication scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login local
```

# Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for login users and to use the local authentication scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login radius-scheme rd local
```

---

**authentication portal**

**Syntax** **authentication portal** { **none** | **radius-scheme** *radius-scheme-name* }

**undo authentication portal**

**View** ISP domain view

**Parameters** **none**: Does not perform any authentication.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **authentication portal** command to specify the authentication scheme for portal users.

Use the **undo authentication portal** command to restore the default.

By default, the default authentication scheme is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

**Related commands:** **authentication default, radius scheme.**

**Examples** # In the default ISP domain **system**, specify the authentication scheme for portal users to RADIUS scheme, with the name **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication portal radius-scheme rd
```

## authorization command

**Syntax** **authorization command hwtacacs-scheme** *hwtacacs-scheme-name*

**undo authorization command**

**View** ISP domain view

**Parameters** **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **authorization command** command to specify the authorization scheme for command line users.

Use the **undo authorization command** command to restore the default.

By default, the default authorization scheme is used for command line users.

Note that the HWTACACS scheme specified for the current ISP domain must have been configured.

**Related commands:** **authorization default, hwtacacs scheme.**

**Examples** # Configure the default ISP domain **system** to use HWTACACS authorization scheme **hw** for command line users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization command hwtacacs-scheme hw
```

---

## authorization default

**Syntax** **authorization default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] | **local** | **none** | **radius-scheme** *radius-scheme-name* [ **local** ] }

**undo authorization default**

**View** ISP domain view

**Parameters** **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local authorization.

**none**: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **authorization default** command to specify the authorization scheme for all types of users.

Use the **undo authorization default** command to restore the default.

By default, the authorization scheme for all types of users is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The authorization scheme specified with the **authorization default** command is for all types of users and has a priority lower than that for a specific access mode.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. In addition, if a RADIUS authorization fails, the error message returned to the NAS says that the server is not responding.

**Related commands:** **authentication default**, **accounting default**, **hwtacacs scheme**, **radius scheme**.

**Examples** # Configure the default ISP domain **system** to use the local authorization scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default local
```

# Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for all types of users and to use the local authorization scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default radius-scheme rd local
```

---

## authorization lan-access

**Syntax** **authorization lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [ **local** ] }

**undo authorization lan-access**

**View** ISP domain view

**Parameters** **local**: Performs local authorization.

**none**: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **authorization lan-access** command to specify the authorization scheme for LAN access users.

Use the **undo authorization lan-access** command to restore the default.

By default, the default authorization scheme is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

**Related commands:** **authorization default**, **radius scheme**.

**Examples** # Configure the default ISP domain **system** to use the local authorization scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization lan-access local
```

# Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for LAN access users and to use the local authorization scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization lan-access radius-scheme rd local
```

---

## authorization login

**Syntax** **authorization login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] | **local** | **none** | **radius-scheme** *radius-scheme-name* [ **local** ] }

**undo authorization login**

**View** ISP domain view

**Parameters** **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local authorization.

**none**: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **authorization login** command to specify the authorization scheme for login users.

Use the **undo authorization login** command to restore the default.

By default, the default authorization scheme is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

**Related commands:** **authorization default**, **hwtacacs scheme**, **radius scheme**.

**Examples** # Configure the default ISP domain **system** to use the local authorization scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login local
```

# Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for login users and to use the local authorization scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login radius-scheme rd local
```

---

**authorization portal**

**Syntax** **authorization portal** { **none** | **radius-scheme** *radius-scheme-name* }

**undo authorization portal**

**View** ISP domain view

**Parameters** **none**: None authorization, which means the user is trusted completely. Here, the user is assigned with the default privilege.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description** Use the **authorization portal** command to specify the authorization scheme for portal users.

Use the **undo authorization portal** command to restore the default.

By default, the default authorization scheme is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

**Related commands:** **authorization default**, **radius scheme**.

**Examples** # In the default ISP domain **system**, specify the authorization scheme for portal users to RADIUS scheme, with the name **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization portal radius-scheme rd
```

---

**cut connection**

**Syntax** **cut connection** { **access-type** { **dot1x** | **mac-authentication** | **portal** } | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id* } [ **slot** *slot-number* ]

**View** System view

**Parameters** **access-type**: Specifies user connections of an access mode.

- **dot1x**: Specifies 802.1x authentication user connections.
- **mac-authentication**: Specifies MAC authentication user connections.
- **portal**: Specifies portal authentication user connections.

**all**: Specifies all user connections.



**domain** *isp-name*: Specifies all user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a string of 1 to 24 characters.

**interface** *interface-type interface-number*: Specifies all user connections of an interface.

**ip** *ip-address*: Specifies a user connection by IP address.

**mac** *mac-address*: Specifies a user connection by MAC address. The MAC address must be in the format of *H-H-H*.

**ucibindex** *ucib-index*: Specifies a user connection by connection index. The value range is from 0 to 4294967295.

**user-name** *user-name*: Specifies a user connection by username.

**vlan** *vlan-id*: Specifies all user connections in a VLAN. The VLAN ID ranges from 1 to 4094.

**slot** *slot-number*: Specifies the connections on a slot.

**Description** Use the **cut connection** command to tear down the specified connections forcibly.

At present, this command applies to only LAN access and portal user connections.

**Related commands:** **display connection, service-type.**

**Examples** # Tear down all connections in ISP domain aabbcc.net.

```
<Sysname> system-view
[Sysname] cut connection domain aabbcc.net
```

---

## display connection

**Syntax** **display connection** [ **access-type** { **dot1x** | **mac-authentication** | **portal** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id* ] [ **slot** *slot-number* ]

**View** Any view

**Parameters** **access-type** { **dot1x** | **mac-authentication** | **portal** }: Specifies user connections of an access mode, that is, 802.1x user connections, MAC authentication user connections, or portal authentication user connections.

**domain** *isp-name*: Specifies all user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a case-insensitive string of 1 to 24 characters.

**interface** *interface-type interface-number*: Specifies all user connections of an interface.

**ip** *ip-address*: Specifies all user connections using the specified IP address.

**mac** *mac-address*: Specifies all user connections using the specified MAC address. The MAC address must be in the format of *H-H-H*.

**ucibindex** *ucib-index*: Specifies all user connections using the specified connection index. The value range is from 0 to 4294967295.

**user-name** *user-name*: Specifies all user connections using the specified username. The *user-name* argument is a case-sensitive string of 1 to 80 characters.

**vlan** *vlan-id*: Specifies all user connections in a VLAN. The VLAN ID ranges from 1 to 4094.

**slot** *slot-number*: Specifies the connections on a slot.

**Description** Use the **display connection** command to display information about specified or all AAA user connections.

This command does not apply to FTP user connections.

**Related commands:** **cut connection**.

**Examples** # Display information about all AAA user connections.

```
<Sysname> display connection
```

```
Index=1 ,Username=telnet@system
```

```
IP=10.0.0.1
```

```
Total 1 connection(s) matched.
```

**Table 182** Field descriptions of the display connection command

Field	Description
Index	Index number
Username	Username of the connection, in the format <i>username@domain</i>
IP	IP address of the user
Total 1 connection(s) matched.	Total number of user connections

---

## display domain

**Syntax** **display domain** [ *isp-name* ]

**View** Any view

**Parameters** *isp-name*: Name of an existing ISP domain, a string of 1 to 24 characters.

**Description** Use the **display domain** command to display the configuration information of a specified ISP domain or all ISP domains.

**Related commands:** **access-limit, domain, state.**

**Examples** # Display the configuration information of all ISP domains.

```
<Sysname> display domain
0 Domain = aabbcc
 State = Active
 Access-limit = Disable
 Accounting method = Required
 Default authentication scheme : local
 Default authorization scheme : local
 Default accounting scheme : local
 Lan-access authentication scheme : radius=test, local
 Lan-access authorization scheme : hwtacacs=hw, local
 Lan-access accounting scheme : local
 Domain User Template:
 Idle-cut = Disable
 Self-service = Disable

1 Domain = system
 State = Active
 Access-limit = Disable
 Accounting method = Required
 Default authentication scheme : local
 Default authorization scheme : local
 Default accounting scheme : local
 Domain User Template:
 Idle-cut = Disable
 Self-service = Disable

Default Domain Name: system
Total 2 domain(s)
```

**Table 183** Field descriptions of the display domain command

Field	Description
Domain	Domain name
State	Status of the domain (active or block)
Access-limit	Access limit (disabled)
Accounting method	Accounting method (either required or optional)
Default authentication scheme	Default authentication scheme
Default authorization scheme	Default authorization scheme
Default accounting scheme	Default accounting scheme
Authentication scheme	Authentication scheme
Authorization scheme	Authentication scheme
Accounting scheme	Accounting scheme
Domain User Template	Template for users in the domain
Idle-cut	Whether idle cut is enabled
Self-service	Whether self service is enabled
Total 2 domain(s).	2 ISP domains in total

---

**display local-user**

**Syntax** **display local-user** [ **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id* ] [ **slot** *slot-number* ]

**View** Any view

**Parameters** **idle-cut** { **disable** | **enable** }: Specifies local users with the idle cut function disabled or enabled.

**service-type**: Specifies the local users of a type.

- **ftp** refers to users using FTP;
- **lan-access** refers to users accessing the network through an Ethernet, such as 802.1x users;
- **ssh** refers to users using SSH;
- **telnet** refers to users using Telnet;
- **terminal** refers to users logging in through the console port or AUX port.

**state** { **active** | **block** }: Specifies all local users in the state of active or block. A local user in the state of active can access network services, while a local user in the state of blocked cannot.

**user-name** *user-name*: Specifies all local users using the specified username. The username is a case-sensitive string of 1 to 55 characters.

**vlan** *vlan-id*: Specifies all local users in a VLAN. The VLAN ID ranges from 1 to 4094.

**slot** *slot-number*: Specifies all local users in the slot where the interface module is inserted.

**Description** Use the **display local-user** command to display information about specified or all local users.

**Related commands:** **local-user**.

**Examples** # Display the information of local user **bbb** on the module installed on slot 1.

```
<Sysname> display local-user user-name bbb slot 0
Slot: 0
The contents of local user bbb:
State: Active
ServiceType: lan-access
Idle-cut: Disable
Access-limit: Enable Current AccessNum: 100
Bind location: Disable
Vlan ID: Disable
IP address: Disable
MAC address: Disable
```

```
User Privilege: 0
Total 1 local user(s) matched.
```

**Table 184** Field descriptions of display local-user (for distributed device)

Field	Description
Slot	Slot number of the card
State	Status of the local user, active or block
ServiceType	Service types that the user can use (ftp, lan-access, ssh, telnet, terminal)
Idle-cut	Whether idle cut is enabled
Access-limit	Accessing user connection limit
Current AccessNum	Number of users currently accessing network services, either for all modules or for a specified module.
Bind location	Whether bound with a port
VLAN ID	VLAN to which the user belongs
IP address	IP address of the user
MAC address	MAC address of the user
User Privilege	Local user privilege
Total 1 local user(s) matched.	1 local user in total

---

## domain

**Syntax** **domain** *isp-name*

**undo domain** *isp-name*

**View** System view

**Parameters** *isp-name*: ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain any forward slash (/), colon (:), asterisk (\*), question mark (?), less-than sign (<), greater-than sign (>), and @.

**Description** Use the **domain** *isp-name* command to create an ISP domain and/or enter ISP domain view.

Use the **domain default** command to specify the default ISP domain and enter ISP domain view.

Use the **undo domain** command to remove an ISP domain.

By default, the system uses the domain of system. You can view its settings by executing the **display domain** command.

If the specified ISP domain does not exist, the system will create a new ISP domain. All the ISP domains are in the active state when they are created.

**Related commands:** **access-limit**, **state**, **display domain**.

**Examples** # Create ISP domain aabbcc.net, and enter ISP domain view.

```

<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net]

```

---

## domain default

**Syntax** `domain default { disable | enable isp-name }`

**View** System view

**Parameters** **disable**: Disables the configured default ISP domain.

**enable**: Enables the configured default ISP domain.

*isp-name*: Name of the ISP, a string of 1 to 24 characters.

**Description** Use the **domain default** command to manually configure the system default ISP domain.

By default, the default domain is named system.

Note that:

- There must be only one default ISP domain.
- When configure a default domain, this domain must have existed.
- The default domain configured cannot be deleted unless you cancel it as a default domain first.

**Related commands:** **state, display domain.**

**Examples** # Create a new ISP domain named **aabbcc.net**, and configure it as the default ISP domain.

```

<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] quit
[Sysname] domain default enable aabbcc.net

```

---

## idle-cut

**Syntax** `idle-cut { disable | enable minute }`

**View** ISP domain view

**Parameters** **disable**: Disables the idle cut function.

**enable** *minute*: Enables the idle cut function. The *minute* argument refers to the allowed idle duration, in the range 1 to 120 minutes.

**Description** Use the **idle-cut** command to enable or disable the idle cut function.  
By default, the function is disabled.

**Related commands:** **domain.**

**Examples** # Enable the idle cut function and set the idle threshold to 50 minutes for ISP domain aabbcc.net.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] idle-cut enable 50
```

## level

**Syntax** **level** *level*

**undo level**

**View** Local user view

**Parameters** *level*: Priority level for the user, which can be 0 for visit level, 1 for monitor level, 2 for system level, and 3 for manage level. A smaller number means a lower priority.

**Description** Use the **level** command to set the priority level of a user.

Use the **undo level** command to restore the default.

By default, the user priority is 0.

Note that:

- If you specify not to perform authentication or use password authentication, the level of the commands that a user can use after logging in depends on the priority of the user interface. For details about the authentication, refer to command **authentication-mode** on page 60.
- If you specify an authentication method that requires the username and password, the level of the commands that a user can use after logging in depends on the priority of the user. For an SSH user using RSA public key authentication, the commands that can be used depend on the level configured on the user interface.

**Related commands:** **local-user.**

**Examples** # Set the level of user user1 to 3.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] level 3
```

---

**local-user**

**Syntax** **local-user** *user-name*

**undo local-user** { *user-name* | **all** [ **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } ] }

**View** System view

**Parameters** *user-name*: Name for the local user, a case-sensitive string of 1 to 55 characters. It cannot include the domain name and cannot contain any back slash (\), vertical bar (|), forward slash (/), colon (:), asterisk (\*), question mark (?), less-than sign (<), greater-than sign (>) or @. In addition, it cannot be **a**, **al**, or **all**.

**all**: Specifies all users.

**service-type**: Specifies the users of a type.

- **ftp** refers to users using FTP;
- **lan-access** refers to users accessing the network through an Ethernet, such as 802.1x users;
- **ssh** refers to users using SSH;
- **telnet** refers to users using Telnet;
- **terminal** refers to users logging in through the console port or AUX port

**Description** Use the **local-user** command to add a local user and enter local user view.

Use the **undo local-user** command to remove the specified local users.

By default, no local user is configured.

**Related commands:** **display local-user**, **service-type**.

**Examples** # Add a local user named **user1**.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1]
```

---

**local-user password-display-mode**

**Syntax** **local-user password-display-mode** { **auto** | **cipher-force** }

**undo local-user password-display-mode**

**View** System view



**Parameters** **auto**: Displays the password of an accessing user based on the configuration of the user by using the **password** command.

**cipher-force**: Displays the passwords of all accessing users in cipher text.

**Description** Use the **local-user password-display-mode** command to set the password display mode for all local users.

Use the **undo local-user password-display-mode** command to restore the default.

The default mode is **auto**.

With the **cipher-force** mode configured:

- A local user password is always displayed in cipher text, regardless of the configuration of the **password** command.
- If you use the **save** command to save the configuration, all existing local user passwords will still be displayed in cipher text after the device restarts, even if you restore the display mode to **auto**.

**Related commands:** **display local-user, password.**

**Examples** # Specify to display the passwords of all accessing users in cipher text.  
`[Sysname] local-user password-display-mode cipher-force`

## password

**Syntax** **password** { **cipher** | **simple** } *password*

**undo password**

**View** Local user view

**Parameters** **cipher**: Specifies to display the password in cipher text.

**simple**: Specifies to display the password in plain text.

*password*: Password for the local user.

- In plain text, it must be a string of 1 to 63 characters that contains no blank space, for example, aabbcc.
- In cipher text, it must be a string of 24 or 88 characters, for example, \_(TT8F]Y5SQ=^Q'MAF4<1!!.
- With the **simple** keyword, you must specify the password in plain text. With the **cipher** keyword, you can specify the password in either plain or cipher text.

**Description** Use the **password** command to configure a password for a local user.

Use the **undo password** command to delete the password of a local user.

Note that:

- With the **local-user password-display-mode cipher-force** command configured, the password is always displayed in cipher text, regardless of the configuration of the **password** command.
- With the **cipher** keyword specified, a password of up to 16 characters in plain text will be encrypted into a password of 24 characters in cipher text, and a password of 16 to 63 characters in plain text will be encrypted into a password of 88 characters in cipher text. For a password of 24 characters, if the system can decrypt the password, the system treats it as a password in cipher text. Otherwise, the system treats it as a password in plain text.

**Related commands:** **display local-user.**

**Examples** # Set the password of user1 to 123456 and specify to display the password in plain text.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password simple 123456
```

## self-service-url

**Syntax** **self-service-url** { **disable** | **enable** *url-string* }

**undo self-service-url**

**View** ISP domain view

**Parameters** **disable**: Disable the self-service server localization function.

**enable** *url-string*: Enable the self-service server localization function. The *url-string* argument refers to the URL of the self-service server for changing user password. The URL is a string of 1 to 64 characters that starts with `http://` and cannot contain any question mark.

**Description** Use the **self-service-url enable** command to enable the self-service server localization function and specify the URL of the self-service server for changing user password.

Use the **self-service-url disable** command or the **undo self-service-url** command to disable the self-service server localization function.

By default, the function is disabled.

Note that:

- A self-service RADIUS server, for example, CAMS, is required for the self-service server localization function. With the self-service function, a user can manage

and control his or her accounting information or module number. A server with self-service software is a self-service server.

- After you configure the **self-service-url enable** command, a user can locate the self-service server by selecting [Service/Change Password] from the 802.1x client. The client software automatically launches the default browser, IE or Netscape, and opens the URL page of the self-service server for changing the user password. A user can change his or her password through the page.
- Only authenticated users can select [Service/Change Password] from the 802.1x client. The option is gray and unavailable for unauthenticated users.

**Examples** # Enable the self-service server localization function and specify the URL of the self-service server for changing user password to `http://10.153.89.94/selfservice/modPasswd1x.jsp|userName` for the default ISP domain **system**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] self-service-url enable http://10.153.89.94/selfservice/modPasswd1x.jsp|userName
```

---

## service-type

**Syntax** **service-type** { **lan-access** | { **ssh** | **telnet** | **terminal** } \* [ **level** *level* ] }

**undo service-type** { **lan-access** | { **ssh** | **telnet** | **terminal** } \* }

**View** Local user view

**Parameters** **lan-access**: Authorizes the user to use the Ethernet to access the network. The user can be, for example, an 802.1x user.

**ssh**: Authorizes the user to use the SSH service.

**telnet**: Authorizes the user to use the Telnet service.

**terminal**: Authorizes the user to use the terminal service, allowing the user to login from the console or AUX port.

**level** *level*: Sets the user level of a Telnet, terminal, or SSH user. The *level* argument is an integer in the range 0 to 3 and defaults to 0.

**Description** Use the **service-type** command to specify the service types that a user can use.

Use the **undo service-type** command to delete one or all service types configured for a user.

By default, a user is authorized with no service.

**Related commands:** **service-type ftp**.

**Examples** # Authorize user user1 to use the Telnet service.

```

<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type telnet

```

---

## service-type ftp

**Syntax** **service-type ftp**

**undo service-type ftp**

**View** Local user view

**Parameters** None

**Description** Use the **service-type ftp** command to authorize a user to use the FTP service.  
Use the **undo service-type ftp** command to disable a user from using the FTP service.

By default, no service is authorized to a user and anonymous access to FTP service is not allowed. If you authorize a user to use the FTP service but do not specify a directory that the user can access, the user can access the root directory of the device by default.

**Related commands:** **work-directory**, **service-type**.

**Examples** # Authorize user user1 to use the FTP service.  
[Sysname-luser-user1] service-type ftp

---

## state

**Syntax** **state { active | block }**

**View** ISP domain view, local user view

**Parameters** **active:** Places the current ISP domain or local user in the active state, allowing the users in the current ISP domain or the current local user to request network services.

**block:** Places the current ISP domain or local user in the blocked state, preventing users in the current ISP domain or the current local user from requesting network services.

**Description** Use the **state** command to configure the status of the current ISP domain or local user.

By default, an ISP domain is active when created. So does a local user.

By blocking an ISP domain, you disable users of the domain that are offline from requesting network services. Note that the online users are not affected.

By blocking a user, you disable the user from requesting network services. No other users are affected.

**Related commands:** **domain.**

**Examples** # Place the current ISP domain aabbcc.net to the state of blocked.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] state block
```

# Place the current user user1 to the state of blocked.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-user-user1] state block
```

## work-directory

**Syntax** **work-directory** *directory-name*

**undo work-directory**

**View** Local user view

**Parameters** *directory-name*: Name of the directory that FTP/SFTP users are authorized to access, a case-insensitive string of 1 to 135 characters.

**Description** Use the **work-directory** command to specify the directory accessible to FTP/SFTP users.

Use the **undo work-directory** command to restore the default.

By default, FTP/SFTP users can access the root directory of the device.

Note that:

- The specified directory accessible to users must exist.
- If you use a file system command to delete the specified directory, FTP/SFTP users will no longer access the directory.
- If the specified directory carries with information about the slot where the secondary module is inserted, FTP/SFTP users cannot log in after primary-to-secondary switching. It is not recommended to carry with slot information when you specify a work directory.

**Examples** # Specify the directory accessible to FTP/SFTP users.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] work-directory flash:
```

# 48

## RADIUS CONFIGURATION COMMANDS

---

### data-flow-format

**Syntax** `data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet { giga-packet | kilo-packet | mega-packet | one-packet } }*`

`undo data-flow-format { data | packet }`

**View** RADIUS scheme view

**Parameters** **data:** Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

**packet:** Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

**Description** Use the **data-flow-format** command to specify the unit for data flows or packets to be sent to a RADIUS server.

Use the **undo data-flow-format** command to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

**Related commands:** **display radius scheme.**

**Examples** # Define RADIUS scheme radius1 to send data flows and packets destined for the RADIUS server in kilobytes and kilo-packets.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

---

### display radius scheme

**Syntax** `display radius scheme [ radius-scheme-name ] [ slot slot-number ]`

**View** Any view

**Parameters** *radius-scheme-name*: RADIUS scheme name.

**slot slot-number**: Specifies the slot where the interface module is inserted.

**Description** Use the **display radius scheme** command to display the configuration information of a specified RADIUS scheme or all RADIUS schemes.

**Related commands:** **radius scheme.**

**Examples** # Display the configurations of all RADIUS schemes.

```
<Sysname> display radius scheme

SchemeName = radius1
Index=0 Type=extended
Primary Auth IP = 1.1.1.1 Port = 1812 State = active
Primary Acct IP = 1.1.1.1 Port = 1813 State = active
Second Auth IP = 0.0.0.0 Port = 1812 State = block
Second Acct IP = 0.0.0.0 Port = 1813 State = block
Auth Server Encryption Key= Not configured
Acct Server Encryption Key= Not configured
Interval for timeout(second) =3
Retransmission times for timeout =3
Interval for realtime accounting(minute) =12
Retransmission times of realtime-accounting packet =5
Retransmission times of stop-accounting packet =500
Quiet-interval(min) =5
Username format =without-do
main
Data flow unit =Byte
Packet unit =one

Total 1 RADIUS scheme(s)
```

**Table 185** Field descriptions of the display radius scheme command

Field	Description
SchemeName	Name of the RADIUS scheme
Index	Index number of the RADIUS scheme
Type	Type of the RADIUS server
Primary Auth IP/ Port/ State	IP address/access port number/current status of the primary authentication server: (active or block)
Primary Acct IP/ Port/ State	IP address/access port number/current status of the primary accounting server: (active or block)
Second Auth IP/ Port/ State	IP address/access port number/current status of the secondary authentication server: (active or block)
Second Acct IP/ Port/ State	IP address/access port number/current status of the secondary accounting server: (active or block)
Auth Server Encryption Key	Shared key of the authentication server
Acct Server Encryption Key	Shared key of the accounting server
Interval for timeout(second)	timeout time in seconds
Retransmission times for timeout	Times of retransmission in case of timeout
Interval for realtime accounting (minute)	Interval for realtime accounting in minutes
Retransmission times of realtime-accounting packet	Retransmission times of realtime-accounting packet



**Table 185** Field descriptions of the display radius scheme command

Field	Description
Retransmission times of stop-accounting packet	Retransmission times of stop-accounting packet
Quiet-interval(min)	Quiet interval for the primary server
Username format	Format of the username
Data flow unit	Unit of data flows
Packet unit	Unit of packets
Total 1 RADIUS scheme(s)	1 RADIUS scheme in total

---

## display radius statistics

**Syntax** `display radius statistics [ slot slot-number ]`

**View** Any view

**Parameters** `slot slot-number`: Specifies the slot where the interface module is inserted.

**Description** Use the **display radius statistics** command to display statistics about RADIUS packets.

**Related commands:** `radius scheme`.

**Examples** # Display statistics about RADIUS packets.

```
<Sysname> display radius statistics
Slot 0:state statistic(total=4096):
 DEAD = 4096 AuthProc = 0 AuthSucc = 0
 AcctStart = 0 RLTSend = 0 RLWait = 0
 AcctStop = 0 OnLine = 0 Stop = 0

Received and Sent packets statistic:
Sent PKT total = 0 Received PKT total = 0
RADIUS received packets statistic:
Code = 2 Num = 0 Err = 0
Code = 3 Num = 0 Err = 0
Code = 5 Num = 0 Err = 0
Code = 11 Num = 0 Err = 0

Running statistic:
RADIUS received messages statistic:
Normal auth request Num = 0 Err = 0 Succ = 0
EAP auth request Num = 0 Err = 0 Succ = 0
Account request Num = 0 Err = 0 Succ = 0
Account off request Num = 0 Err = 0 Succ = 0
PKT auth timeout Num = 0 Err = 0 Succ = 0
PKT acct_timeout Num = 0 Err = 0 Succ = 0
Realtime Account timer Num = 0 Err = 0 Succ = 0
PKT response Num = 0 Err = 0 Succ = 0
Session ctrl pkt Num = 0 Err = 0 Succ = 0
Normal author request Num = 0 Err = 0 Succ = 0
```

```

Set policy result Num = 0 Err = 0 Succ = 0
RADIUS sent messages statistic:
Auth accept Num = 0
Auth reject Num = 0
EAP auth replying Num = 0
Account success Num = 0

Account failure Num = 0
Server ctrl req Num = 0
RecError_MSG_sum = 0
SndMSG_Fail_sum = 0
Timer_Err = 0
Alloc_Mem_Err = 0
State Mismatch = 0
Other_Error = 0

No-response-acct-stop packet = 0
Discarded No-response-acct-stop packet for buffer overflow = 0

```

**Table 186** Field descriptions of display radius statistics command

Field	Description
state statistic(total=4096)	state statistic
DEAD	The state of idle
AuthProc	The state of waiting for authentication
AuthSucc	The state of authenticated
AcctStart	The state of accounting start
RLTSend	The state of sending real-time accounting packets
RLTWait	The state of waiting for real-time accounting
AcctStop	The state of accounting waiting stopped
OnLine	The state of online
Stop	The state of stop
Received and Sent packets statistic	Number of packets sent and received
Sent PKT total	Number of packets sent
Received PKT total	Number of packets received
RADIUS received packets statistic	Statistic of packets received by RADIUS
Code	Type of packet
Num	Total number of packets
Err	Number of error packets
Running statistic	Statistics of running packets
RADIUS received messages statistic	Number of messages received by RADIUS
Normal auth request	Number of normal authentication requests
EAP auth request	Number of EAP authentication requests
Account request	Number of accounting requests
Account off request	Number of stop-accounting requests
PKT auth timeout	Number of authentication timeout packets
PKT acct_timeout	Number of accounting timeout packets
Realtime Account timer	Number of realtime accounting requests
PKT response	Number of PKT responses

**Table 186** Field descriptions of display radius statistics command

Field	Description
Session ctrl pkt	Number of session control packets
Normal author request	Number of normal authorization packets
Succ	Number of successful packets
Set policy result	Number of responses to the Set policy packets
RADIUS sent messages statistic	Number of messages that have been sent by RADIUS
Auth accept	Number of accepted authentication packets
Auth reject	Number of rejected authentication packets
EAP auth replying	Number of replying packets of EAP authentication
Account success	Number of accounting succeeded packets
Account failure	Number of accounting failed packets
Server ctrl req	Number of server control requests
RecError_MSG_sum	Number of received packets in error
SndMSG_Fail_sum	Number of packets that failed to be sent out
Timer_Err	Number of timer errors
Alloc_Mem_Err	Number of memory errors
State Mismatch	Number of errors for mismatching status
Other_Error	Number of errors of other types
No-response-acct-stop packet	Number of times that no response was received for stop-accounting packets
Discarded No-response-acct-stop packet for buffer overflow	Number of stop-accounting packets that were buffered but then discarded due to full memory

## display stop-accounting-buffer

**Syntax** **display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [ **slot** *slot-number* ]

**View** Any view

**Parameters** **radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**session-id** *session-id*: Specifies a session by its ID. The ID is a string of 1 to 50 characters.

**time-range** *start-time stop-time*: Specifies a time range by its start time and end time in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

**user-name** *user-name*: Specifies a user by the user name, which is a case-sensitive string of 1 to 80 characters.

**slot** *slot-number*: Specifies the slot where the interface module is inserted.

**Description** Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device by scheme, session ID, time range, user name, or slot.

Note that if receiving no response after sending a stop-accounting request to a RADIUS server, the device buffers the request and retransmits it. You can use the **retry stop-accounting** command to set the number of allowed transmission attempts.

**Related commands:** **reset stop-accounting-buffer, stop-accounting-buffer enable, retry stop-accounting.**

**Examples** # Display information about the buffered stop-accounting requests from 0:0:0 to 23:59:59 on August 31, 2006.

```
<Sysname> display stop-accounting-buffer time-range 0:0:0-08/31/2006 23:59:59-08/31/2006
Total find 0 record (0)
```

## key

**Syntax** **key { accounting | authentication } string**

**undo key { accounting | authentication }**

**View** RADIUS scheme view

**Parameters** **accounting:** Sets the shared key for RADIUS accounting packets.

**authentication:** Sets the shared key for RADIUS authentication/authorization packets.

*string:* Shared key, a case-sensitive string of 1 to 16 characters.

**Description** Use the **key** command to set the shared key for RADIUS authentication/authorization or accounting packets.

Use the **undo key** command to restore the default.

By default, no shared key is configured.

Note that:

- You must ensure that the same shared key is set on the device and the RADIUS server.
- If authentication/authorization and accounting are performed on two servers with different shared keys, you must set separate shared key for each on the device.

**Related commands:** **display radius scheme.**

**Examples** # Set the shared key for authentication/authorization packets to hello for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key authentication hello
```

# Set the shared key for accounting packets to ok for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting ok
```

---

## nas-ip

**Syntax** **nas-ip** *ip-address*

**undo nas-ip**

**View** RADIUS scheme view

**Parameters** *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

**Description** Use the **nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure. The address of a loopback interface is recommended.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.

**Related commands:** **radius nas-ip**.

**Examples** # Set the IP address for the device to use as the source address of the RADIUS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] nas-ip 10.1.1.1
```

---

## primary accounting

**Syntax** **primary accounting** *ip-address* [ *port-number* ]

**undo primary accounting**

**View** RADIUS scheme view

**Parameters** *ip-address*: IP address of the primary accounting server.

*port-number*: UDP port number of the primary accounting server, which ranges from 1 to 65535.

**Description** Use the **primary accounting** command to configure the IP address and UDP port of the primary RADIUS accounting server.

Use the **undo primary accounting** command to restore the defaults.

By default, the default IP address is 0.0.0.0, and the default port number 1813.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.

**Related commands:** **key, radius scheme, state.**

**Examples** # Set the IP address of the primary accounting server for RADIUS scheme radius1 to 10.110.1.2 and the UDP port of the server to 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813
```

---

## primary authentication

**Syntax** **primary authentication** *ip-address* [ *port-number* ]

**undo primary authentication**

**View** RADIUS scheme view

**Parameters** *ip-address*: IP address of the primary authentication/authorization server.

*port-number*: UDP port number of the primary authentication/authorization server, which ranges from 1 to 65535.

**Description** Use the **primary authentication** command to configure the IP address and UDP port of the primary RADIUS authentication/authorization server.

Use the **undo primary authentication** command to restore the defaults.

By default, the default IP address is 0.0.0.0, and the default port number 1812.

Note that:

- After creating a RADIUS scheme, you are supposed to configure the IP address and UDP port of each RADIUS server (primary/secondary authentication/authorization or accounting server). The configuration of RADIUS servers is at your discretion except that there must be at least one authentication/authorization server and one accounting server. Besides, ensure that the RADIUS service port settings on the device are consistent with the port settings on the RADIUS servers.
- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.

**Related commands:** **key, radius scheme, state.**

**Examples** # Set the IP address of the primary authentication/authorization server for RADIUS scheme radius1 to 10.110.1.1 and the UDP port of the server to 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812
```

## radius client

**Syntax** **radius client enable**

**undo radius client**

**View** System view

**Parameters** None

**Description** Use the **radius client enable** command to enable the listening port of the RADIUS client.

Use the **undo radius client** command to disable the listening port of the RADIUS client.

By default, the listening port is enabled.

Note that when the listening port of the RADIUS client is disabled:

- The RADIUS client can either accept authentication, authorization or accounting requests or process timer messages. However, it fails to transmit and receive packets to and from the RADIUS server.

- The end account packets of online users cannot be sent out and buffered. This may cause that the RADIUS server still has the user record after a user goes offline for a period of time.
- The authentication, authorization and accounting turn to the local scheme after the RADIUS request fails if the RADIUS scheme and the local authentication, authorization and accounting scheme are configured.
- The buffered accounting packets cannot be sent out and will be deleted from the buffer when the configured maximum number of attempts is reached.

**Examples** # Enable the listening port of the RADIUS client.

```
<Sysname> system-view
[Sysname] radius client enable
```

---

## radius nas-ip

**Syntax** **radius nas-ip** *ip-address*

**undo radius nas-ip**

**View** System view

**Parameters** *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

**Description** Use the **radius nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo radius nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.

**Related commands:** **nas-ip**.



**Examples** # Set the IP address for the device to use as the source address of the RADIUS packets to 129.10.10.1.

```
<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1
```

## radius scheme

**Syntax** **radius scheme** *radius-scheme-name*  
**undo radius scheme** *radius-scheme-name*

**View** System view

**Parameters** *radius-scheme-name*: RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

**Description** Use the **radius scheme** command to create a RADIUS scheme and enter RADIUS scheme view.

Use the **undo radius scheme** command to delete a RADIUS scheme.

By default, no RADIUS scheme is defined.

Note that:

- The RADIUS protocol is configured scheme by scheme. Every RADIUS scheme must at least specify the IP addresses and UDP ports of the RADIUS authentication/authorization/accounting servers and the parameters necessary for a RADIUS client to interact with the servers.
- A RADIUS scheme can be referenced by more than one ISP domain at the same time.
- You cannot remove the RADIUS scheme being used by online users with the **undo radius scheme** command.

**Related commands:** **key**, **retry realtime-accounting**, **timer realtime-accounting**, **stop-accounting-buffer enable**, **retry stop-accounting**, **server-type**, **state**, **user-name-format**, **retry**, **display radius scheme**, **display radius statistics**.

**Examples** # Create a RADIUS scheme named **radius1** and enter RADIUS scheme view.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

## radius trap

**Syntax** **radius trap** { **accounting-server-down** | **authentication-server-down** }  
**undo radius trap** { **accounting-server-down** | **authentication-server-down** }

**View** System view

**Parameters** **accounting-server-down**: RADIUS trap for accounting servers.  
**authentication-server-down**: RADIUS trap for authentication servers.

**Description** Use the **radius trap** command to enable the RADIUS trap function.  
 Use the **undo radius trap** command to disable the function.  
 By default, the RADIUS trap function is disabled.

Note that:

- If a NAS sends an accounting or authentication request to the RADIUS server but gets no response, the NAS retransmits the request. With the RADIUS trap function enabled, when the NAS transmits the request for half of the specified maximum number of transmission attempts, it sends a trap message; when the NAS transmits the request for the specified maximum number, it sends another trap message.
- If the specified maximum number of transmission attempts is odd, the half of the number refers to the smallest integer greater than the half of the number.

**Examples** # Enable the RADIUS trap function for accounting servers.

```
<Sysname> system-view
[Sysname] radius trap accounting-server-down
```

## reset radius statistics

**Syntax** **reset radius statistics** [ **slot** *slot-number* ]

**View** User view

**Parameters** **slot** *slot-number*: Specifies the slot where the interface module is inserted.

**Description** Use the **reset radius statistics** command to clear RADIUS statistics.

**Related commands:** **display radius scheme**.

**Examples** # Clear RADIUS statistics.

```
<Sysname> reset radius statistics
```

## reset stop-accounting-buffer

**Syntax** **reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [ **slot** *slot-number* ]

<b>View</b>	User view
<b>Parameters</b>	<p><b>radius-scheme</b> <i>radius-scheme-name</i>: Specifies a RADIUS scheme by its name, a string of 1 to 32 characters.</p> <p><b>session-id</b> <i>session-id</i>: Specifies a session by its ID, a string of 1 to 50 characters.</p> <p><b>time-range</b> <i>start-time stop-time</i>: Specifies a time range by its start time and end time in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.</p> <p><b>user-name</b> <i>user-name</i>: Specifies a user name based on which to reset the stop-accounting buffer. The username is a case-sensitive string of 1 to 80 characters.</p> <p><b>slot</b> <i>slot-number</i>: Specifies the slot where the interface module is inserted.</p>
<b>Description</b>	Use the <b>reset stop-accounting-buffer</b> command to clear the buffered stop-accounting requests, which get no responses.
<b>Related commands:</b>	<b>stop-accounting-buffer enable, retry stop-accounting, display stop-accounting-buffer.</b>
<b>Examples</b>	<pre># Clear the buffered stop-accounting requests for user user0001@aabbcc.net. &lt;Sysname&gt; reset stop-accounting-buffer user-name user0001@aabbcc.net  # Clear the buffered stop-accounting requests in the time range from 0:0:0 to 23:59:59 on August 31, 2006.  &lt;Sysname&gt; reset stop-accounting-buffer time-range 0:0:0-08/31/2006 2 3:59:59-08/31/2006</pre>

---

## retry

<b>Syntax</b>	<p><b>retry</b> <i>retry-times</i></p> <p><b>undo retry</b></p>
<b>View</b>	RADIUS scheme view
<b>Parameters</b>	<i>retry-times</i> : Maximum number of retransmission attempts, in the range 1 to 20.
<b>Description</b>	<p>Use the <b>retry</b> command to set the maximum number of RADIUS retransmission attempts.</p> <p>Use the <b>undo retry</b> command to restore the default.</p> <p>The default value for the <i>retry-times</i> argument is 3.</p> <p>Note that:</p>

- Because RADIUS uses UDP packets to transmit data, the communication is not reliable. If the device does not receive a response to its request from the RADIUS server within the response time-out time, it will retransmit the RADIUS request. If the number of retransmission attempts exceeds the limit but the device still receives no response from the RADIUS server, the device regards that the authentication fails.
- The maximum number of retransmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

**Related commands:** **radius scheme**, **timer response-timeout**.

**Examples** # Set the maximum number of RADIUS request transmission attempts to 5 for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

---

## retry realtime-accounting

**Syntax** **retry realtime-accounting** *retry-times*

**undo retry realtime-accounting**

**View** RADIUS scheme view

**Parameters** *retry-times*: Maximum number of accounting request transmission attempts. It ranges from 1 to 255 and defaults to 5.

**Description** Use the **retry realtime-accounting** command to set the maximum number of accounting request transmission attempts.

Use the **undo retry realtime-accounting** command to restore the default.

Note that:

- A RADIUS server usually checks whether a user is online by a timeout timer. If it receives from the NAS no real-time accounting packet for a user in the timeout period, it considers that there may be line or device failure and stops accounting for the user. This may happen when some unexpected failure occurs. In this case, the NAS is required to disconnect the user in accordance. This is done by the maximum number of accounting request transmission attempts. Once the limit is reached but the NAS still receives no response, the NAS disconnects the user.
- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 3 (set with the **retry** command), and the real-time accounting interval is 12 minutes (set with the **timer realtime-accounting** command), and the maximum number of accounting request transmission attempts is 5 (set with the **retry realtime-accounting** command). In such a case, the device

generates an accounting request every 12 minutes, and retransmits the request when receiving no response within 3 seconds. The accounting is deemed unsuccessful if no response is received within 3 requests. Then the device sends a request every 12 minutes, and if for 5 times it still receives no response, the device will cut the user connection.

**Related commands:** **radius scheme, timer realtime-accounting.**

**Examples** # Set the maximum number of accounting request transmission attempts to 10 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname -radius-radius1] retry realtime-accounting 10
```

## retry stop-accounting

**Syntax** **retry stop-accounting** *retry-times*

**undo retry stop-accounting**

**View** RADIUS scheme view

**Parameters** *retry-times*: Maximum number of stop-accounting request transmission attempts. It ranges from 10 to 65,535 and defaults to 500.

**Description** Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 5 (set with the **retry** command), and the maximum number of stop-accounting request transmission attempts is 20 (set with the **retry stop-accounting** command). This means that for each stop-accounting request, if the device receives no response within 3 seconds, it will initiate a new request. If still no responses are received within 5 renewed requests, the stop-accounting request is deemed unsuccessful. Then the device will temporarily store the request in the device and resend a request and repeat the whole process described above. Only when 20 consecutive attempts fail will the device discard the request.

**Related commands:** **reset stop-accounting-buffer, radius scheme, display stop-accounting-buffer.**

**Examples** # Set the maximum number of stop-accounting request transmission attempts to 1,000 for RADIUS scheme radius1.

```

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000

```

---

## secondary accounting

**Syntax** **secondary accounting** *ip-address* [ *port-number* ]

**undo secondary accounting**

**View** RADIUS scheme view

**Parameters** *ip-address*: IP address of the secondary accounting server, in dotted decimal notation. The default is 0.0.0.0.

*port-number*: UDP port number of the secondary accounting server, which ranges from 1 to 65535 and defaults to 1813.

**Description** Use the **secondary accounting** command to configure the IP address and UDP port of the secondary RADIUS accounting server.

Use the **undo secondary accounting** command to restore the defaults.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.

**Related commands:** **key**, **radius scheme**, **state**.

**Examples** # Set the IP address of the secondary accounting server for RADIUS scheme radius1 to 10.110.1.1 and the UDP port of the server to 1813.

```

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813

```

---

## secondary authentication

**Syntax** **secondary authentication** *ip-address* [ *port-number* ]

**undo secondary authentication**

**View** RADIUS scheme view

**Parameters** *ip-address*: IP address of the secondary authentication/authorization server, in dotted decimal notation. The default is 0.0.0.0.

*port-number*: UDP port number of the secondary authentication/authorization server, which ranges from 1 to 65535 and defaults to 1812.

**Description** Use the **secondary authentication** command to configure the IP address and UDP port of the secondary RADIUS authentication/authorization server.

Use the **undo secondary authentication** command to restore the defaults.

Note that:

- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.

**Related commands:** **key, radius scheme, state.**

**Examples** # Set the IP address of the secondary authentication/authorization server for RADIUS scheme radius1 to 10.110.1.2 and the UDP port of the server to 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

## security-policy-server

**Syntax** **security-policy-server** *ip-address*

**undo security-policy-server** { *ip-address* | **all** }

**View** RADIUS scheme view

**Parameters** *ip-address*: IP address of a security policy server.

**all**: All IP addresses

**Description** Use the **security-policy-server** command to specify a security policy server.

Use the **undo security-policy-server** command to remove one or all security policy servers.

By default, no security policy server is specified.

Note that:

- If more than one interface of the device is enabled with Portal, the interfaces may use different security policy servers. You can specify up to eight security policy servers for a RADIUS scheme.
- The specified security policy server must be a security policy server or RADIUS server that is correctly configured and working normally. Otherwise, the device will regard it as an illegal server.

**Examples** # For RADIUS scheme **radius1**, set the IP address of a security policy server to 10.110.1.2.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] security-policy-server 10.110.1.2
```

---

## server-type

**Syntax** **server-type** { **extended** | **standard** }

**undo server-type**

**View** RADIUS scheme view

**Parameters** **extended**: Specifies the extended RADIUS server (generally CAMS), which requires the RADIUS client and RADIUS server to interact according to the procedures and packet formats provisioned by the private RADIUS protocol.

**standard**: Specifies the standard RADIUS server, which requires the RADIUS client end and RADIUS server to interact according to the regulation and packet format of the standard RADIUS protocol (RFC 2865/2866 or newer).

**Description** Use the **server-type** command to specify the RADIUS server type supported by the device.

Use the **undo server-type** command to restore the default.

By default, the supported RADIUS server type is **standard**.

**Related commands:** **radius scheme**.

**Examples** # Set the RADIUS server type of RADIUS scheme radius1 to standard.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] server-type standard
```

---

## state

**Syntax** **state** { **primary** | **secondary** } { **accounting** | **authentication** } { **active** | **block** }

**View** RADIUS scheme view

**Parameters** **primary**: Sets the status of the primary RADIUS server.

**secondary**: Sets the status of the secondary RADIUS server.

**accounting**: Sets the status of the RADIUS accounting server.



**authentication:** Sets the status of the RADIUS authentication/authorization server.

**active:** Sets the status of the RADIUS server to **active**, namely the normal operation state.

**block:** Sets the status of the RADIUS server to **block**.

**Description** Use the **state** command to set the status of a RADIUS server.

By default, every RADIUS server configured with an IP address in the RADIUS scheme is in the state of active.

Note that:

- When a primary server, authentication/authorization server or accounting server, fails, the device automatically turns to the secondary server.
- Once the primary server fails, the primary server turns into the state of block, and the device turns to the secondary server. In this case, if the secondary server is available, the device triggers the primary server quiet timer. After the quiet timer times out, the status of the primary server is active again and the status of the secondary server remains the same. If the secondary server fails, the device restores the status of the primary server to active immediately.
- If the primary server has resumed, the device turns to use the primary server and stops communicating with the secondary server. After accounting starts, the communication between the client and the secondary server remains unchanged.
- If both the primary server and the secondary server are in the state of active or blocked, the device sends the packets only to the primary server.
- If one server is in the active state while the other is blocked, the switchover will not take place even if the active server is not reachable.

**Related commands:** **radius scheme, primary authentication, secondary authentication, primary accounting, secondary accounting.**

**Examples** # Set the status of the secondary server in RADIUS scheme radius1 to **active**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication active
```

## stop-accounting-buffer enable

**Syntax** **stop-accounting-buffer enable**  
**undo stop-accounting-buffer enable**

**View** RADIUS scheme view

**Parameters** None

**Description** Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the RADIUS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

**Related commands:** **reset stop-accounting-buffer, radius scheme, display stop-accounting-buffer.**

**Examples** # In RADIUS scheme radius1, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

## timer quiet

**Syntax** **timer quiet** *minutes*

**undo timer quiet**

**View** RADIUS scheme view

**Parameters** *minutes*: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

**Description** Use the **timer quiet** command to set the quiet timer for the primary server, that is, the duration that the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

**Related commands:** **display radius scheme.**

**Examples** # Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] timer quiet 10
```

---

**timer realtime-accounting**

**Syntax** **timer realtime-accounting** *minutes*

**undo timer realtime-accounting**

**View** RADIUS scheme view

**Parameters** *minutes*: Real-time accounting interval in minutes, must be a multiple of 3 and in the range 3 to 60, with the default value being 12.

**Description** Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the RADIUS accounting server periodically. This command is for setting the interval.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the RADIUS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

**Table 187** Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

**Related commands:** **retry realtime-accounting**, **radius scheme**.

**Examples** # Set the real-time accounting interval to 51 minutes for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

---

**timer response-timeout**

**Syntax** **timer response-timeout** *seconds*

**undo timer response-timeout**

<b>View</b>	RADIUS scheme view
<b>Parameters</b>	<i>seconds</i> : RADIUS server response timeout period in seconds. It ranges from 1 to 10 and defaults to 3.
<b>Description</b>	Use the <b>timer response-timeout</b> command to set the RADIUS server response timeout timer.  Use the <b>undo timer</b> command to restore the default.  Note that: <ul style="list-style-type: none"> <li>■ If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request (authentication/authorization or accounting request), it has to resend the request so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.</li> <li>■ A proper value for the RADIUS server response timeout timer can help improve the system performance. Set the timer based on the network conditions.</li> <li>■ The maximum total number of all types of retransmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.</li> </ul>

**Related commands:** **radius scheme, retry.**

**Examples** # Set the RADIUS server response timeout timer to 5 seconds for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

---

## user-name-format

<b>Syntax</b>	<b>user-name-format { with-domain   without-domain }</b>
<b>View</b>	RADIUS scheme view
<b>Parameters</b>	<b>with-domain:</b> Includes the ISP domain name in the username sent to the RADIUS server.  <b>without-domain:</b> Excludes the ISP domain name from the username sent to the RADIUS server.
<b>Description</b>	Use the <b>user-name-format</b> command to specify the format of the username to be sent to a RADIUS server.  By default, the ISP domain name is included in the username.  Note that:

- A username is generally in the format of `userid@isp-name`, of which `isp-name` is used by the device to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the device must remove the domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a RADIUS server.
- If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the RADIUS scheme to more than one ISP domain, thus avoiding the confused situation where the RADIUS server regards two users in different ISP domains but with the same `userid` as one.

**Related commands:** `radius scheme`.

**Examples** # Specify the device to include the domain name in the username sent to the RADIUS servers for the RADIUS scheme `radius1`.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```



# 49

## HWTACACS CONFIGURATION COMMANDS

---

### data-flow-format

**Syntax** **data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }\*

**undo data-flow-format** { **data** | **packet** }

**View** HWTACACS scheme view

**Parameters** **data**: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

**packet**: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

**Description** Use the **data-flow-format** command to specify the unit for data flows or packets to be sent to a HWTACACS server.

Use the **undo data-flow-format** command to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

**Related commands:** **display hwtacacs**.

**Examples** # Define HWTACACS scheme **hwt1** to send data flows and packets destined for the TACACS server in kilobytes and kilo-packets.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname- hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo
-packet
```

---

### display hwtacacs

**Syntax** **display hwtacacs** [ *hwtacacs-scheme-name* [ **statistics** ] ] [ **slot** *slot-number* ]

**View** Any view

**Parameters** *hwtacacs-scheme-name*: HWTACACS scheme name.

**statistics:** Displays complete statistics about the HWTACACS server.

**slot *slot-number*:** Specifies the slot where the interface module is inserted.

**Description** Use the **display hwtacacs** command to display configuration information or statistics of the specified or all HWTACACS schemes.

Note that:

- If no HWTACACS scheme is specified, the command will display the configuration information of all HWTACACS schemes.
- If no slot number is specified, the command will display the configuration information of the HWTACACS scheme on the main processing unit (MPU).

**Related commands:** **hwtacacs scheme.**

**Examples** # Display configuration information about HWTACACS scheme gy.

```
<Sysname> display hwtacacs gy

HWTACACS-server template name : gy
Primary-authentication-server : 172.31.1.11:49
Primary-authorization-server : 172.31.1.11:49
Primary-accounting-server : 172.31.1.11:49
Secondary-authentication-server : 0.0.0.0:0
Secondary-authorization-server : 0.0.0.0:0
Secondary-accounting-server : 0.0.0.0:0
Current-authentication-server : 172.31.1.11:49
Current-authorization-server : 172.31.1.11:49
Current-accounting-server : 172.31.1.11:49
NAS-IP-address : 0.0.0.0
key authentication : 790131
key authorization : 790131
key accounting : 790131
Quiet-interval(min) : 5
Realtime-accounting-interval(min) : 12
Response-timeout-interval(sec) : 5
Acct-stop-PKT retransmit times : 100
Domain-included : Yes
Data traffic-unit : B
Packet traffic-unit : one-packet

```

**Table 188** Field descriptions of the display hwtacacs command

Field	Description
HWTACACS-server template name	Name of the HWTACACS scheme
Primary-authentication-server	Primary authentication server
Primary-authorization-server	Primary authorization server
Primary-accounting-server	Primary accounting server
Secondary-authentication-server	Secondary authentication server
Secondary-authorization-server	Secondary authorization server
Secondary-accounting-server	Secondary accounting server
Current-authentication-server	Currently used authentication server
Current-authorization-server	Currently used authorization server
Current-accounting-server	Currently used accounting server



**Table 188** Field descriptions of the display hwtacacs command

Field	Description
NAS-IP-address	NAS-IP address
key authentication	Key for authentication
key authorization	Key for authorization
key accounting	Key for accounting
Quiet-interval	Quiet interval for the primary server
Realtime-accounting-interval	Real-time accounting interval
Response-timeout-interval	Server response timeout period
Acct-stop-PKT retransmit times	Number of stop-accounting packet transmission retries
Domain-included	Whether a user name includes the domain name
Data traffic-unit	Unit for data flows
Packet traffic-unit	Unit for data packets

---

## display stop-accounting-buffer

**Syntax** **display stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name*  
[ **slot** *slot-number* ]

**View** Any view

**Parameters** **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies a HWTACACS scheme by its name, a string of 1 to 32 characters.

**slot** *slot-number*: Specifies the slot where the interface module is inserted.

**Description** Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device by scheme, session ID, time range, user name, or slot.

**Related commands:** **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **retry stop-accounting**.

**Examples** # Display information about the buffered stop-accounting requests for HWTACACS scheme hwt1.

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1
Total 0 record(s) Matched
```

---

## hwtacacs nas-ip

**Syntax** **hwtacacs nas-ip** *ip-address*

**undo hwtacacs nas-ip**

**View** System view

- Parameters** *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.
- Description** Use the **hwtacacs nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.
- Use the **undo hwtacacs nas-ip** command to remove the configuration.
- By default, the source IP address of a packet sent to the server is the IP address of the outbound port.
- Note that:
- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
  - If you configure the command for more than one time, the last configuration takes effect.
  - The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

**Related commands:** **nas-ip**.

**Examples** # Set the IP address for the device to use as the source address of the HWTACACS packets to **129.10.10.1**.

```
<Sysname> system-view
[Sysname] hwtacacs nas-ip 129.10.10.1
```

---

## hwtacacs scheme

- Syntax** **hwtacacs scheme** *hwtacacs-scheme-name*
- undo hwtacacs scheme** *hwtacacs-scheme-name*
- View** System view
- Parameters** *hwtacacs-scheme-name*: HWTACACS scheme name, a case-insensitive string of 1 to 32 characters.
- Description** Use the **hwtacacs scheme** command to create an HWTACACS scheme and enter HWTACACS scheme view.
- Use the **undo hwtacacs scheme** command to delete an HWTACACS scheme.
- By default, no HWTACACS scheme exists.

**Examples** # Create an HWTACACS scheme named hwt1 and enter HWTACACS scheme view.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1]
```

## key

**Syntax** **key** { **accounting** | **authentication** | **authorization** } *string*  
**undo key** { **accounting** | **authentication** | **authorization** } *string*

**View** HWTACACS scheme view

**Parameters** **accounting**: Sets the shared key for HWTACACS accounting packets.  
**authentication**: Sets the shared key for HWTACACS authentication packets.  
**authorization**: Sets the shared key for HWTACACS authorization packets.  
*string*: Shared key, a string of 1 to 16 characters.

**Description** Use the **key** command to set the shared key for HWTACACS authentication, authorization, or accounting packets.

Use the **undo key** command to remove the configuration.

By default, no shared key is configured.

**Related commands:** **display hwtacacs**.

**Examples** # Set the shared key for HWTACACS accounting packets to **hello** for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting hello
```

## nas-ip

**Syntax** **nas-ip** *ip-address*  
**undo nas-ip**

**View** HWTACACS scheme view

**Parameters** *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

**Description** Use the **nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

**Related commands:** **hwtacacs nas-ip**.

**Examples** # Set the IP address for the device to use as the source address of the HWTACACS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

## primary accounting

**Syntax** **primary accounting** *ip-address* [ *port-number* ]

**undo primary accounting**

**View** HWTACACS scheme view

**Parameters** *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

**Description** Use the **primary accounting** command to specify the primary HWTACACS accounting server.

Use the **undo primary accounting** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

**Examples** # Configure the primary accounting server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme test1
[Sysname-hwtacacs-test1] primary accounting 10.163.155.12 49
```

---

## primary authentication

**Syntax** **primary authentication** *ip-address* [ *port-number* ]

**undo primary authentication**

**View** HWTACACS scheme view

**Parameters** *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

**Description** Use the **primary authentication** command to specify the primary HWTACACS authentication server.

Use the **undo primary authentication** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

**Related commands:** **display hwtacacs.**

**Examples** # Set the primary authentication server.

```

<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49

```

---

## primary authorization

**Syntax** **primary authorization** *ip-address* [ *port-number* ]

**undo primary authorization**

**View** HWTACACS scheme view

**Parameters** *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

**Description** Use the **primary authorization** command to specify the primary HWTACACS authorization server.

Use the **undo primary authorization** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

**Related commands:** **display hwtacacs.**

**Examples** # Configure the primary authorization server.

```

<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49

```

---

## reset hwtacacs statistics

**Syntax** **reset hwtacacs statistics** { **accounting** | **all** | **authentication** | **authorization** } [ *slot slot-number* ]

**View** User view

**Parameters**

- accounting**: Clears HWTACACS accounting statistics.
- all**: Clears all HWTACACS statistics.
- authentication**: Clears HWTACACS authentication statistics.
- authorization**: Clears HWTACACS authorization statistics.
- slot** *slot-number*: Clears HWTACACS statistics on the interface module in the specified slot.

**Description** Use the **reset hwtacacs statistics** command to clear HWTACACS statistics.

**Related commands:** **display hwtacacs**.

**Examples**

```
Clear all HWTACACS statistics.
<Sysname> reset hwtacacs statistics all
```

## reset stop-accounting-buffer

**Syntax** **reset stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name* [ **slot** *slot-number* ]

**View** User view

**Parameters** **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies a HWTACACS scheme by its name, a string of 1 to 32 characters.

**slot** *slot-number*: Specifies the slot where the interface module is inserted.

**Description** Use the **reset stop-accounting-buffer** command to clear the buffered stop-accounting requests that get no responses.

**Related commands:** **stop-accounting-buffer enable**, **retry stop-accounting**, **display stop-accounting-buffer**.

**Examples**

```
Clear the buffered stop-accounting requests for HWTACACS scheme hwt1.
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

## retry stop-accounting

**Syntax** **retry stop-accounting** *retry-times*  
**undo retry stop-accounting**

**View** HWTACACS scheme view

**Parameters** *retry-times*: Maximum number of stop-accounting request transmission attempts. It ranges from 1 to 300 and defaults to 100.

**Description** Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

**Related commands:** **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

**Examples** # Set the maximum number of stop-accounting request transmission attempts to 50.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 50
```

## secondary accounting

**Syntax** **secondary accounting** *ip-address* [ *port-number* ]

**undo secondary accounting**

**View** HWTACACS scheme view

**Parameters** *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

**Description** Use the **secondary accounting** command to specify the secondary HWTACACS accounting server.

Use the **undo secondary accounting** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

**Examples** # Configure the secondary accounting server.



```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49
```

---

## secondary authentication

**Syntax** **secondary authentication** *ip-address* [ *port-number* ]

**undo secondary authentication**

**View** HWTACACS scheme view

**Parameters** *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

**Description** Use the **secondary authentication** command to specify the secondary HWTACACS authentication server.

Use the **undo secondary authentication** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

**Related commands:** **display hwtacacs.**

**Examples** # Configure the secondary authentication server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49
```

---

## secondary authorization

**Syntax** **secondary authorization** *ip-address* [ *por-number t* ]

**undo secondary authorization**

**View** HWTACACS scheme view

**Parameters** *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

**Description** Use the **secondary authorization** command to specify the secondary HWTACACS authorization server.

Use the **undo secondary authorization** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

**Related commands:** **display hwtacacs.**

**Examples** # Configure the secondary authorization server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49
```

## stop-accounting-buffer enable

**Syntax** **stop-accounting-buffer enable**

**undo stop-accounting-buffer enable**

**View** HWTACACS scheme view

**Parameters** None

**Description** Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the HWTACACS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

**Related commands:** **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

**Examples** # In HWTACACS scheme **hwt1**, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

## timer quiet

**Syntax** **timer quiet** *minutes*

**undo timer quiet**

**View** HWTACACS scheme view

**Parameters** *minutes*: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

**Description** Use the **timer quiet** command to set the quiet timer for the primary server, that is, the duration that the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

**Related commands:** **display hwtacacs**.

**Examples** # Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet 10
```

## timer realtime-accounting

**Syntax** **timer realtime-accounting** *minutes*

**undo timer realtime-accounting**

- View** HWTACACS scheme view
- Parameters** *minutes*: Real-time accounting interval in minutes. It is a multiple of 3 in the range 3 to 60 and defaults to 12.
- Description** Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. This command is for setting the interval.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the HWTACACS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

**Table 189** Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

- Examples** # Set the real-time accounting interval to 51 minutes for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

---

## timer response-timeout

- Syntax** **timer response-timeout** *seconds*
- undo timer response-timeout**
- View** HWTACACS scheme view
- Parameters** *seconds*: HWTACACS server response timeout period in seconds. It ranges from 1 to 300 and defaults to 5.
- Description** Use the **timer response-timeout** command to set the HWTACACS server response timeout timer.

Use the **undo timer** command to restore the default.

As HWTACACS is based on TCP, the timeout of the server response timeout timer and/or the TCP timeout timer will cause the device to be disconnected from the HWTACACS server.

**Related commands:** **display hwtacacs.**

**Examples** # Set the HWTACACS server response timeout timer to 30 seconds for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

## user-name-format

**Syntax** **user-name-format** { **with-domain** | **without-domain** }

**View** HWTACACS scheme view

**Parameters** **with-domain:** Includes the ISP domain name in the username sent to the HWTACACS server.

**without-domain:** Excludes the ISP domain name from the username sent to the HWTACACS server.

**Description** Use the **user-name-format** command to specify the format of the username to be sent to a HWTACACS server.

By default, the ISP domain name is included in the username.

Note that:

- A username is generally in the format of `userid@isp-name`, of which `isp-name` is used by the device to determine the ISP domain to which a user belongs. Some earlier HWTACACS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a HWTACACS server, the device must remove the domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a HWTACACS server.
- If a HWTACACS scheme defines that the username is sent without the ISP domain name, do not apply the HWTACACS scheme to more than one ISP domain, thus avoiding the confused situation where the HWTACACS server regards two users in different ISP domains but with the same `userid` as one.

**Related commands:** **hwtacacs scheme.**

**Examples** # Specify the device to include the ISP domain name in the username sent to the HWTACACS servers for the HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

# 50

## WEB AUTHENTICATION CONFIGURATION COMMANDS

---

### display portal acl

**Syntax** `display portal acl { all | dynamic | static } interface interface-type  
interface-number`

**View** Any view

**Parameters** **all**: Displays all portal access control lists (ACLs), including dynamic ones and static ones.

**dynamic**: Displays dynamic portal ACLs, namely, ACLs generated after a user passes portal authentication.

**static**: Displays static portal ACLs, namely, ACLs generated by related configurations.

**interface *interface-type interface-number***: Displays the ACLs on the specified interface.

**Description** Use the **display portal acl** command to display the ACLs on a specified interface.

**Examples** # Display all ACLs on interface Vlan-interface 2.

```
<Sysname> display portal acl all interface Vlan-interface 2
Vlan-interface 2 portal ACL rule:
```

```
Rule 0
Inbound interface = Ethernet2/0/3
Type = static
Action = permit
Source:
 IP = 0.0.0.0
 Mask = 0.0.0.0
 MAC = 0000-0000-0000
 Interface = any
 VLAN = 2
Destination:
 IP = 192.168.0.111
 Mask = 255.255.255.255
```

```
Rule 1
Inbound interface = Ethernet2/0/4
Type = static
Action = permit
```

```

Source:
 IP = 0.0.0.0
 Mask = 0.0.0.0
 MAC = 0000-0000-0000
 Interface = any
 VLAN = 2
Destination:
 IP = 192.168.0.111
 Mask = 255.255.255.255

```

**Table 190** Field descriptions of the display portal acl command

Field	Description
Rule	Sequence number of the generated ACL, which is numbered from 0 in ascending order
Inbound interface	Interface to which portal ACLs are bound
Type	Type of the portal ACL
Action	Match action in the portal ACL
Source	Source information in the portal ACL
IP	Source IP address in the portal ACL
Mask	Subnet mask of the source IP address in the portal ACL
MAC	Source MAC address in the portal ACL
Interface	Source interface in the portal ACL
VLAN	Source VLAN in the portal ACL
Destination	Destination information in the portal ACL
IP	Destination IP address in the portal ACL
Mask	Subnet mask of the destination IP address in the portal ACL

## display portal connection statistics

**Syntax** `display portal connection statistics { all | interface interface-type interface-number }`

**View** Any view

**Parameters** **all**: Specifies all interfaces.

**interface** *interface-type* *interface-number*: Specifies an interface by its type and number.

**Description** Use the **display portal connection statistics** command to display portal connection statistics on a specified interface or all interfaces.

**Examples** # Display portal connection statistics on interface Vlan-interface 2.

```

<Sysname> display portal connection statistics interface Vlan-interface 2
-----Interface: Vlan-interface 2-----
User state statistics:
State-Name User-Num
VOID 0
DISCOVERED 0
WAIT_AUTHEN_ACK 0

```



WAIT_AUTHOR_ACK	0		
WAIT_LOGIN_ACK	0		
WAIT_ACL_ACK	0		
WAIT_NEW_IP	0		
WAIT_USERIPCHANGE_ACK	0		
ONLINE	1		
WAIT_LOGOUT_ACK	0		
WAIT_LEAVING_ACK	0		
Message statistics:			
Msg-Name	Total	Err	Discard
MSG_AUTHEN_ACK	3	0	0
MSG_AUTHOR_ACK	3	0	0
MSG_LOGIN_ACK	3	0	0
MSG_LOGOUT_ACK	2	0	0
MSG_LEAVING_ACK	0	0	0
MSG_CUT_REQ	0	0	0
MSG_AUTH_REQ	3	0	0
MSG_LOGIN_REQ	3	0	0
MSG_LOGOUT_REQ	2	0	0
MSG_LEAVING_REQ	0	0	0
MSG_ARPPKT	0	0	0
MSG_TMR_REQAUTH	1	0	0
MSG_TMR_AUTHEN	0	0	0
MSG_TMR_AUTHOR	0	0	0
MSG_TMR_LOGIN	0	0	0
MSG_TMR_LOGOUT	0	0	0
MSG_TMR_LEAVING	0	0	0
MSG_TMR_NEWIP	0	0	0
MSG_TMR_USERIPCHANGE	0	0	0
MSG_PORT_REMOVE	0	0	0
MSG_VLAN_REMOVE	0	0	0
MSG_IF_REMOVE	6	0	0
MSG_L3IF_SHUT	0	0	0
MSG_IP_REMOVE	0	0	0
MSG_ALL_REMOVE	1	0	0
MSG_IFIPADDR_CHANGE	0	0	0
MSG_SOCKET_CHANGE	8	0	0

**Table 191** Field descriptions of display portal connection statistics

Field	Description
User state statistics	Statistics on portal users
State-Name	Name of a user state
User-Num	Number of users
VOID	Number of users in void state
DISCOVERED	Number of users in discovered state
WAIT_AUTHEN_ACK	Number of users in wait_authen_ack state
WAIT_AUTHOR_ACK	Number of users in wait_author_ack state
WAIT_LOGIN_ACK	Number of users in wait_login_ack state
WAIT_ACL_ACK	Number of users in wait_acl_ack state
WAIT_NEW_IP	Number of users in wait_new_ip state
WAIT_USERIPCHANGE_ACK	Number of users wait_useripchange_ack state
ONLINE	Number of users in online state
WAIT_LOGOUT_ACK	Number of users in wait_logout_ack state
WAIT_LEAVING_ACK	Number of users in wait_leaving_ack state
Message statistics	Statistics on messages
Msg-Name	Message type

**Table 191** Field descriptions of display portal connection statistics

Field	Description
Total	Total number of messages
Err	Number of erroneous messages
Discard	Number of discarded messages
MSG_AUTHEN_ACK	Authentication acknowledgment message
MSG_AUTHOR_ACK	Authorization acknowledgment message
MSG_LOGIN_ACK	Accounting acknowledgment message
MSG_LOGOUT_ACK	Accounting-stop acknowledgment message
MSG_LEAVING_ACK	Leaving acknowledgment message
MSG_CUT_REQ	Cut request message
MSG_AUTH_REQ	Authentication request message
MSG_LOGIN_REQ	Accounting request message
MSG_LOGOUT_REQ	Accounting-stop request message
MSG_LEAVING_REQ	Leaving request message
MSG_ARPPKT	ARP message
MSG_TMR_REQAUTH	Authentication request timeout message
MSG_TMR_AUTHEN	Authentication timeout message
MSG_TMR_AUTHOR	Authorization timeout message
MSG_TMR_LOGIN	Accounting-start timeout message
MSG_TMR_LOGOUT	Accounting-stop timeout message
MSG_TMR_LEAVING	Leaving timeout message
MSG_TMR_NEWIP	Public IP update timeout message
MSG_TMR_USERIPCHANGE	User IP change timeout message
MSG_PORT_REMOVE	Users-of-a-Layer-2-port-removed message
MSG_VLAN_REMOVE	VLAN user removed message
MSG_IF_REMOVE	Users-of-a-Layer-3-interface-removed message
MSG_L3IF_SHUT	Layer 3 interface shutdown message
MSG_IP_REMOVE	User-with-an-IP-removed message
MSG_ALL_REMOVE	All-users-removed message
MSG_IFIPADDR_CHANGE	Interface IP address change message
MSG_SOCKET_CHANGE	Socket change message

---

## display portal free-rule

**Syntax** `display portal free-rule [ rule-number ]`

**View** Any view

**Parameters** *rule-number*: Number of a portal-free rule, in the range 0 to 31.

**Description** Use the **display portal free-rule** command to display information about a specified portal-free rule or all portal-free rules.

**Related commands:** **portal free-rule.**

**Examples** # Display information about portal-free rule 1.

```
<Sysname> display portal free-rule 1
Rule-Number 1:
Source:
 IP = 2.2.2.0
 Mask = 255.255.255.0
 MAC = 0000-0000-0000
 Interface = any
 Vlan = 0
Destination:
 IP = 0.0.0.0
 Mask = 0.0.0.0
```

**Table 192** Field descriptions of the display portal free-rule command

Field	Description
Rule-Number	Number of the portal-free rule
Source	Source information in the portal-free rule
IP	Source IP address in the portal-free rule
Mask	Subnet mask of the source IP address in the portal-free rule
MAC	Source MAC address in the portal-free rule
Interface	Source interface in the portal-free rule
Vlan	Source VLAN in the portal-free rule
Destination	Destination information in the portal-free rule
IP	Destination IP address in the portal-free rule
Mask	Subnet mask of the destination IP address in the portal-free rule

---

## display portal interface

**Syntax** **display portal interface** *interface-type interface-number*

**View** Any view

**Parameters** *interface-type interface-number*: Specifies an interface by its type and number.

**Description** Use the **display portal interface** command to display the portal configuration of an interface.

**Examples** # Display the portal configuration of interface Vlan-interface 2.

```
<Sysname> display portal interface Vlan-interface 2
Interface portal configuration:
Vlan-interface 2: Portal running
Portal server: servername
Authentication type: Direct
Authentication network:
address = 0.0.0.0 mask = 0.0.0.0
```

**Table 193** Field descriptions of the display portal interface command

Field	Description
Interface portal configuration	Portal configuration on the interface
Vlan-interface 2	Status of the portal feature on the interface
Portal server	Portal server referenced by the interface
Authentication type	Authentication mode enabled on the interface
Authentication network address	Information of the portal authentication subnet IP address of the portal authentication subnet
mask	Subnet mask of the IP address of the portal authentication subnet

---

## display portal server

**Syntax** `display portal server [ server-name ]`

**View** Any view

**Parameters** *server-name*: Name of a portal server, a case-sensitive string of 1 to 32 characters.

**Description** Use the **display portal server** command to display information about a specified portal server or all portal servers.

**Related commands:** **portal server**.

**Examples** # Display information about portal server aaa.

```
<Sysname> display portal server aaa
Portal server:
 1)aaa:
 IP = 192.168.0.111
 Key = portal
 Port = 50100
 URL = http://192.168.0.111/portal
```

**Table 194** Field descriptions of the display portal server command

Field	Description
1)	Number of the portal server
aaa	Name of the portal server
IP	IP address of the portal server
Key	Key for portal authentication
Port	Listening port on the portal server
URL	Address the packets are to be redirected to

## display portal server statistics

**Syntax** `display portal server statistics { all | interface interface-type interface-number }`

**View** Any view

**Parameters** **all**: Specifies all interfaces.

**interface** *interface-type interface-number*: Specifies an interface by its type and name.

**Description** Use the **display portal server statistics** command to display portal server statistics on a specified interface or all interfaces.

Note that with the **all** keyword specified, the command displays portal server statistics by interface and therefore statistics about a portal server referenced by more than one interface may be displayed repeatedly.

**Examples** # Display portal server statistics on Vlan-interface 2.

```
<Sysname> display portal server statistics interface Vlan-interface 2
-----Interface: Vlan-interface 2-----
Server name: st
Invalid packets: 0
Pkt-Name Total Discard Checkerr
REQ_CHALLENGE 3 0 0
ACK_CHALLENGE 3 0 0
REQ_AUTH 3 0 0
ACK_AUTH 3 0 0
REQ_LOGOUT 1 0 0
ACK_LOGOUT 1 0 0
AFF_ACK_AUTH 3 0 0
NTF_LOGOUT 1 0 0
REQ_INFO 6 0 0
ACK_INFO 6 0 0
NTF_USERDISCOVER 0 0 0
NTF_USERIPCHANGE 0 0 0
AFF_NTF_USERIPCHANGE 0 0 0
ACK_NTF_LOGOUT 1 0 0
```

**Table 195** Field descriptions of the display portal server statistics command

Field	Description
Interface	Interface referencing the portal server
Server name	Name of the portal server
Invalid packets	Number of invalid packets
Pkt-Name	Packet type
Total	Total number of packets
Discard	Number of discarded packets
Checkerr	Number of erroneous packets
REQ_CHALLENGE	Challenge request message the portal server sends to the access device
ACK_CHALLENGE	Challenge acknowledgment message the access device sends to the portal server

**Table 195** Field descriptions of the display portal server statistics command

Field	Description
REQ_AUTH	Authentication request message the portal server sends to the access device
ACK_AUTH	Authentication acknowledgment message the access device sends to the portal server
REQ_LOGOUT	Logout request message the portal server sends to the access device
ACK_LOGOUT	Logout acknowledgment message the access device sends to the portal server
AFF_ACK_AUTH	Affirmation message the portal server sends to the access device after receiving an authentication acknowledgement message
NTF_LOGOUT	Forced logout notification message the access device sends to the portal server
REQ_INFO	Information request message
ACK_INFO	Information acknowledgment message
NTF_USERDISCOVER	User discovery notification message the portal server sends to the access device
NTF_USERIPCHANGE	User IP change notification message the access device sends to the portal server
AFF_NTF_USERIPCHANGE	User IP change success notification message the portal server sends to the access device
ACK_NTF_LOGOUT	Forced logout acknowledgment message from the portal server

---

## display portal tcp-cheat statistics

**Syntax** `display portal tcp-cheat statistics`

**View** Any view

**Parameters** None

**Description** Use the **display portal tcp-cheat statistics** command to display TCP spoofing statistics.

**Examples** # Display TCP spoofing statistics.

```
<Sysname> display portal tcp-cheat statistics
TCP Cheat Statistic:
Total Opens: 0
Reset Connections: 0
Current Opens: 0
Packets Received: 0
Packets Sent: 0
Packets Retransmitted: 0
Packets Dropped: 0
HTTP Packets Sent: 0
Connection State:
 SYN_RECV: 0
 ESTABLISHED: 0
 CLOSE_WAIT: 0
```

```

LAST_ACK: 0
FIN_WAIT_1: 0
FIN_WAIT_2: 0
CLOSING: 0

```

**Table 196** Description on fields of the display portal tcp-cheat statistics command

Field	Description
TCP Cheat Statistic	TCP spoofing statistics
Total Opens	Total number of opened connections
Resets Connections	Number of connections reset through RST packets
Current Opens	Number of connections currently being setting up
Packets Received	Number of received packets
Packets Sent	Number of sent packets
Packets Retransmitted	Number of retransmitted packets
Packets Dropped	Number of dropped packets
HTTP Packets Sent	Number of HTTP packets sent
Connection State	Statistics of connections in various state
ESTABLISHED	Number of connections in ESTABLISHED state
CLOSE_WAIT	Number of connections in CLOSE_WAIT state
LAST_ACK	Number of connections in LAST-ACK state
FIN_WAIT_1	Number of connections in FIN_WAIT_1 state
FIN_WAIT_2	Number of connections in FIN_WAIT_2 state
CLOSING	Number of connections in CLOSING state

## display portal user

**Syntax** `display portal user { all | interface interface-type interface-number }`

**View** Any view

**Parameters** **all**: Specifies all interfaces.

**interface** *interface-type interface-number*: Specifies an interface by its type and name.

**Description** Use the **display portal user** command to display information about portal users on a specified interface or all interfaces.

**Examples** # Display information about portal users on all interfaces.

```

<Sysname> display portal user all
Index:2
State:ONLINE
SubState:INVALID
MAC IP Vlan Interface

000d-88f8-0eab 2.2.2.2 2 Vlan-interface 2
Total 1 user(s) matched, 1 listed.

```

**Table 197** Field descriptions of the display portal user command

Field	Description
Index	Index of the portal user
State	Current status of the portal user
SubState	Current sub-status of the portal user
MAC	MAC address of the portal user
IP	IP address of the portal user
Vlan	VLAN to which the portal user belongs
Interface	Interface to which the portal user is attached
Total 1 user(s) matched, 1 listed	Total number of portal users

---

## portal auth-network

**Syntax** `portal auth-network network-address { mask-length | mask }`

**undo portal auth-network** { `network-address` | **all** }

**View** Interface view

**Parameters** *network-address*: IP address of the authentication subnet.

*mask-length*: Length of the subnet mask, in the range of 0 to 32.

*mask*: Subnet mask, in dotted decimal notation.

**all**: Specifies all authentication subnets.

**Description** Use the **portal auth-network** command to configure a portal authentication subnet.

Use the **undo portal auth-network** command to remove a specified portal authentication subnet or all portal authentication subnets.

Note that this command is only applicable for Layer 3 authentication. The portal authentication subnet for direct authentication is any source IP address, and the portal authentication subnet for re-DHCP authentication is the one determined by the private IP address of the interface.

By default, the portal authentication subnet is 0.0.0.0/0, meaning that users in all subnets are to be authenticated.

**Examples** # Configure a portal authentication subnet of 10.10.10.0/24.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] portal auth-network 10.10.10.0 24
```



---

**portal delete-user**

**Syntax** **portal delete-user** { *ip-address* | **all** | **interface** *interface-type interface-number* }

**View** System view

**Parameters** *ip-address*: IP address of a user.

**all**: Logs out all users.

**interface** *interface-type interface-number*: Logs out all users on the specified interface.

**Description** Use the **portal delete-user** command to log out users.

**Related commands:** **display portal user**.

**Examples** # Log out user 1.1.1.1.  

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

---

**portal free-rule**

**Syntax** **portal free-rule** *rule-number* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } } | **any** } } | **source** { **any** | [ **interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } } | **any** } | **mac** *mac-address* | **vlan** *vlan-id* ] \* } } \*

**undo portal free-rule** { *rule-number* | **all** }

**View** System view

**Parameters** *rule-number*: Number for the portal-free rule, in the range 0 to 31.

**any**: Imposes no limitation on the previous keyword.

**ip** *ip-address*: Specifies an IP address.

**mask** { *mask-length* | *netmask* }: Specifies the mask of the IP address, which can be in dotted decimal notation or an integer in the range 0 to 32.

**interface** *interface-type interface-number*: Specifies a source interface.

**mac** *mac-address*: Specifies a source MAC address in the format of H-H-H.

**vlan** *vlan-id*: Specifies a source VLAN ID. The value range is from 1 to 4094.

**all**: Specifies all portal-free rules.

**Description** Use the **portal free-rule** command to configure a portal-free rule and specify the source filtering condition and/or destination filtering condition.

Use the **undo portal free-rule** command to remove a specified portal-free rule or all portal-free rules.

**Related commands:** **display portal free-rule.**



- *If you specify both the source IP and source MAC address information in a portal-free rule, the IP address must be a host address with a mask of 32 bits; otherwise, the specified MAC address will be neglected.*
- *You cannot configure two portal-free rules with the same filtering conditions. Otherwise, the device will prompt that the portal-free rule already exists.*

**Examples** # Configure a portal-free rule, allowing any packet whose source IP address is 10.10.10.1/24 and source interface is Vlan-interface 2 to bypass portal authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 15 source ip 10.10.10.1 mask 24 interface
Vlan-interface 2 destination ip any
```

## portal server

**Syntax** **portal server** *server-name* **ip** *ip-address* [ **key** *key-string* | **port** *port-id* | **url** *url-string* ] \*

**undo portal server** *server-name* [ **key** | **port** | **url** ]

**View** System view

**Parameters** *server-name*: Name of the portal server, a case-sensitive string of 1 to 32 characters.

*ip-address*: IP address of the portal server.

*key-string*: Shared key for communication with the portal server, a case-sensitive string of 1 to 16 characters.

*port-id*: Destination port number used when the device sends a message to the portal server unsolicitedly, in the range 1 to 65534. The default is 50100.

*url-string*: Uniform resource locator (URL) to which HTTP packets are to be redirected, in the *http://ip-address* format. The default of *ip-address* is the IP address of the portal server.

**Description** Use the **portal server** command to configure a portal server.

Use the **undo portal server** command to remove a portal server, restore the default destination port number or URL, or delete the shared key.

By default, no portal server is configured.

Using the **undo portal server** *server-name* command, you remove the specified portal server if the specified portal server exists and there is no user on the interfaces referencing the portal server.

**Related commands:** **display portal server.**



**CAUTION:**

- *If the portal feature is enabled on an interface, you cannot remove the **portal server** that the interface references. If there are users on this interface, you cannot modify the parameters of the **portal server**.*
- *You must disable portal authentication on an interface before removing the **portal server** applied to the interface.*

**Examples** # Configure portal server pts, setting the IP address to 192.168.0.111, the key to portal, and the redirection URL to http://192.168.0.111/portal.

```
<Sysname> system-view
[Sysname] portal server pts ip 192.168.0.111 key portal url http://192.168.0.111/portal
```

---

## portal server method

**Syntax** **portal server** *server-name* **method** { **direct** | **layer3** | **redhcp** }

**undo portal**

**View** Interface view

**Parameters** *server-name*: Name of the portal server, a case-sensitive string of 1 to 32 characters.

**method**: Specifies the authentication mode to be used.

**direct**: Direct authentication.

**layer3**: Layer 3 authentication.

**redhcp**: Re-DHCP authentication.

**Description** Use the **portal server** command to enable portal authentication on an interface, and specify the portal server to be referenced and the authentication mode and service type.

Use the **undo portal** command to disable portal authentication on an interface.

By default, portal authentication is disabled on an interface.

Note that the portal server to be referenced must exist.

**Related commands:** **display portal server.**

**Examples** # Enable portal authentication on interface VLAN-interface 100, setting the portal server to **pts**, the authentication mode to **direct**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal server pts method direct
```

## reset portal connection statistics

**Syntax** **reset portal connection statistics** { **all** | **interface** *interface-type interface-number* }

**View** User view

**Parameters** **all**: Specifies all interfaces.

**interface** *interface-type interface-number*: Specifies an interface by its type and number.

**Description** Use the **reset portal connection statistics** command to clear portal connection statistics on a specified interface or all interfaces.

**Examples** # Clear portal connection statistics on interface Vlan-interface 2.

```
<Sysname> reset portal connection statistics interface Vlan-interface 2
```

## reset portal server statistics

**Syntax** **reset portal server statistics** { **all** | **interface** *interface-type interface-number* }

**View** User view

**Parameters** **all**: Specifies all interfaces.

**interface** *interface-type interface-number*: Specifies an interface by its type and number.

**Description** Use the **reset portal server statistics** command to clear portal server statistics on a specified interface or all interfaces.

**Examples** # Clear portal server statistics on interface Vlan-interface 2.

```
<Sysname> reset portal server statistics interface Vlan-interface 2
```

---

**reset portal tcp-cheat statistics**

**Syntax** `reset portal tcp-cheat statistics`

**View** User view

**Parameters** None

**Description** Use the **reset portal tcp-cheat statistics** command to clear TCP spoofing statistics.

**Examples** # Clear TCP spoofing statistics.  
`<Sysname> reset portal tcp-cheat statistics`



# 51

## SSH CONFIGURATION COMMANDS

---

### display public-key local

**Syntax** `display public-key local rsa public`

**View** Any view

**Parameters** `rsa`: Displays the public key(s) of RSA local key pair(s).

**Description** Use the **display public-key local** command to display the information about the public key(s) of the local key pair(s).

**Related commands:** `public-key local create`.

**Examples** # Display the public key information of RSA local key pair(s).

```
<Sysname> display public-key local rsa public
```

```
=====
```

```
Time of Key pair created: 19:59:16 2006/10/25
```

```
Key name: HOST_KEY
```

```
Key type: RSA Encryption Key
```

```
=====
```

```
Key code:
```

```
30819F300D06092A864886F70D010101050003818D0030818902818100BC4C392A97
```

```
734A633BA0F1DB01F84EB51228EC86ADE1DBA597E0D9066FDC4F04776CEA3610D257
```

```
8341F5D049143656F1287502C06D39D39F28F0F5CBA630DA8CD1C16ECE8A7A65282F
```

```
2407E8757E7937DCCDB5DB620CD1F471401B7117139702348444A2D8900497A87B8D
```

```
5F13D61C4DEFA3D14A7DC07624791FC1D226F62DF3020301
```

```
0001
```

```
=====
```

```
Time of Key pair created: 19:59:17 2006/10/25
```

```
Key name: SERVER_KEY
```

```
Key type: RSA Encryption Key
```

```
=====
```

```
Key code:
```

```
307C300D06092A864886F70D0101010500036B003068026100C51AF7CA926962284A
```

```
4654B2AACC7B2AE12B2B1EABFAC1CDA97E42C3C10D7A70D1012BF23ADE5AC4E7AAB1
```

```
32CFB6453B27E054BFAA0A85E113FBDE751EE0ECECF659529E857CF8C211E2A03FD8F
```

```
10C5BEC162B2989ABB5D299D1E4E27A13C7DD10203010001
```

**Table 198** Description on fields of the display public-key local command

Field	Description
Time of Key pair created	Time when the key pair is created
Key name	Name of the key
Key type	Type of the key
Key code	Code of the key

---

## display public-key peer

**Syntax** `display public-key peer [ brief | name publickey-name ]`

**View** Any view

**Parameters** **brief**: Displays brief information about all public keys of remote ends.  
**name *publickey-name***: Specifies a public key of a remote end by its name, which is a string of 1 to 64 characters.

**Description** Use the **display public-key peer** command to display information about specified or all public keys of remote ends.

With neither the **brief** keyword nor the **name *publickey-name*** combination specified, the command displays detailed information about all public keys of remote ends.

**Related commands:** **public-key peer**.

**Examples** # Display detailed information about the public key named **idrsa**.

```
<Sysname> display public-key peer name idrsa
=====
Key name : idrsa
Key type : RSA
Key module : 1024
=====
Key Code:
30819D300D06092A864886F70D010101050003818B00308187028181009C46A87102
16CEC0C01C7CE136BA76C79AA6040E79F9E305E453998C7ADE8276069410803D5974
F708496947AB39B3F39C5CE56C95B6AB7442D56393BF241F99A639DD02D9E29B1F5C
1FD05CC1C44FBD6CFFB58BE6F035FAA2C596B27D1231D159846B7CB9A7757C5800FA
DA9FD72F65672F4A549EE99F63095E11BD37789955020123
```

**Table 199** Description on fields of the display public-key peer name command

Field	Description
Key name	Name of the key
Key type	Type of the key
Key module	Module of the key
Key code	Code of the key



# Display brief information about all public keys of remote ends.

```
<Sysname> display public-key peer brief
Type Module Name

RSA 1024 idrsa
```

**Table 200** Field descriptions of the display public-key peer brief command

Field	Description
Type	Type of the key
Module	Number of bits in the key
Name	Name of the peer public key

---

## display sftp client source

**Syntax** **display sftp client source**

**View** Any view

**Parameters** None

**Description** Use the **display sftp client source** command to display the source IP address or source interface currently set for the SFTP client.

If neither source IP address nor source interface is specified for the SFTP client, "You didn't specify the source" will be displayed.

**Related commands:** **sftp client source.**

**Examples** # Display the source IP address of the SFTP client.

```
<Sysname> display sftp client source
The source IP address you specified is 192.168.0.1
```

---

## display ssh client source

**Syntax** **display ssh client source**

**View** Any view

**Parameters** None

**Description** Use the **display ssh client source** command to display the source IP address or source interface currently set for the SSH client.

If neither source IP address nor source interface is specified for the SSH client, "You didn't specify the source" will be displayed.

**Related commands:** **ssh client source.**

**Examples** # Display the source IP address of the SSH client.

```
<Sysname> display ssh client source
The source IP address you specified is 192.168.0.1
```

---

## display ssh server

**Syntax** **display ssh server { status | session }**

**View** Any view

**Parameters** **status:** Displays the status information of the SSH server.

**session:** Displays the session information of the SSH server.

**Description** Use the **display ssh server** command to display the status information or session information of an SSH server.

**Related commands:** **ssh server authentication-retries, ssh server rekey-interval, ssh server authentication-timeout, ssh server enable, ssh server compatible-ssh1x enable.**

**Examples** # Display the status information of the SSH server.

```
<Sysname> display ssh server status
SSH Server: Disable
SSH version : 1.99
SSH authentication-timeout : 60 second(s)
SSH server key generating interval : 0 hour(s)
SSH Authentication retries : 3 time(s)
SFTP Server: Disable
SFTP Server Idle-Timeout: 10 minute(s)
```

**Table 201** Description on fields of the display ssh server status command

Field	Description
SSH Server	Whether the SSH server function is enabled
SSH version	SSH protocol version
	When the SSH server supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.0.
SSH authentication-timeout	Authentication timeout period
SSH server key generating interval	SSH server key pair update interval
SSH Authentication retries	Maximum number of SSH authentication attempts
SFTP Server	Whether the SFTP server function is enabled
SFTP Server Idle-Timeout	SFTP connection idle timeout period

# Display the session information of the SSH server.

```
<Sysname> display ssh server session
Conn Ver Encry State Retry SerType Username
VTY 0 2.0 DES Established 0 SFTP client001
```

**Table 202** Description on fields of the display ssh server session command

Field	Description
Conn	Connected VTY channel
Ver	SSH server protocol version
Encry	Encryption algorithm
State	Status of the session, including: Init, Ver-exchange, Keys-exchange, Auth-request, Serv-request, Established, Disconnected
Retry	Number of authentication attempts
SerType	Service type (SFTP, Stelnet)
Username	Name of a user during login

## display ssh server-info

**Syntax** `display ssh server-info`

**View** Any view

**Parameters** None

**Description** Use the **display ssh server-info** command to display the mappings between host public keys and SSH servers saved on a client.

**Examples** # Display the mappings between host public keys and SSH servers saved on the client.

```
<Sysname> display ssh server-info
Server Name(IP) Server public key name

192.168.0.1 abc_key01
192.168.0.2 abc_key02
```

**Table 203** Descriptions on fields of the display ssh server-info command

Field	Description
Server Name(IP)	Name or IP address of the server
Server public key name	Name of the host public key of the server

## display ssh user-information

**Syntax** `display ssh user-information [ username ]`

**View** Any view

**Parameters** *username*: SSH username, a string of 1 to 80 characters.

**Description** Use the **display ssh user-information** command to display information about a specified or all SSH users.

With the *username* argument not specified, the command displays information about all SSH users.

**Related commands:** **ssh user.**

**Examples** # Display information about all SSH users.

```
<Sysname> display ssh user-information
Total ssh users : 2
Username Authentication-type User-public-key-name Service-type
yemx password null stelnet|sftp
test publickey pubkey sftp
```

**Table 204** Description on fields of the display ssh user-information command

Field	Description
Username	Name of the user
Authentication-type	Authentication type
User-public-key-name	Public key of the user
Service-type	Service type

---

## peer-public-key end

**Syntax** **peer-public-key end**

**View** Public key view

**Parameters** None

**Description** Use the **peer-public-key end** command to return from public key view to system view.

**Related commands:** **public-key peer.**

**Examples** # Exit public key view.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] peer-public-key end
[Sysname]
```

---

## public-key-code begin

**Syntax** **public-key-code begin**

**View** Public key view

**Parameters** None

**Description** Use the **public-key-code begin** command to enter RSA key code view.

After entering public key code view, you can input the key data. It must be a hexadecimal string that is generated randomly by the SSH-supported client software and coded compliant to PKCS.

**Related commands:** **public-key peer, public-key-code end.**

**Examples** # Enter public key code view to input the key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC8014F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D1643135877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6B80EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE675AC30CB020301
[Sysname-pkey-key-code]0001
```

---

## public-key-code end

**Syntax** **public-key-code end**

**View** RSA key code view

**Parameters** None

**Description** Use the **public-key-code end** command to return from public key code view to public key view and to save the configured public key.

The system verifies the key before saving it. If the key contains illegal characters, the system displays an error message and discards the key. If the key is legal, the system saves it.

**Related commands:** **public-key peer, public-key-code begin.**

**Examples** # Exit RSA key code view save the configured public key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC8014F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D1643135877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6B80EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE675AC30CB020301
[Sysname-pkey-key-code]0001
[Sysname-pkey-key-code] public-key-code end
[Sysname-pkey-public-key]
```

---

**public-key local create****Syntax** **public-key local create rsa****View** System view**Parameters** **rsa**: RSA key pair.**Description** Use the **public-key local create** command to create the local key pair(s).

Note that:

- After entering this command, you will be prompted to provide the length of the key pair. The length of a server/host key must be in the range 512 to 2048 bits and defaults to 1024. If the key pair already exists, the system will ask you whether you want to overwrite it.
- The configuration of this command can survive a reboot. You only need to configure it once.

**Related commands:** **public-key local destroy, display public-key local.****Examples** # Create RSA local key pair.

```

<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
 It may take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating keys...
.....+++++
.....+++++
.....+++++
.....+++++
.....+++++
.

```

---

**public-key local destroy****Syntax** **public-key local destroy rsa****View** System view**Parameters** **rsa**: RSA key pair.**Description** Use the **public-key local destroy** command to destroy the local key pair(s).**Related commands:** **public-key local create.**

```

Examples # Destroy RSA local key pair.
<Sysname> system-view
[Sysname] public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]:y

```

---

## public-key local export rsa

**Syntax** `public-key local export rsa { openssh | ssh1 | ssh2 } [ filename ]`

**View** System view

**Parameters** **openssh**: Uses the format of OpenSSH.

**ssh1**: Uses the format of SSH1.

**ssh2**: Uses the format of SSH2.

*filename*: Name of the file for storing public key.

**Description** Use the **public-key local export rsa** command to display the RSA local public key on the screen or export it to a specified file.

If you do not specify the *filename* argument, the command displays the RSA local public key on the screen; otherwise, the command exports the RSA local public key to the specified file and saves the file.

SSH1, SSH2 and OpenSSH are three different public key file formats for different requirements.

**Related commands:** **public-key local create**, **public-key local destroy**.

```

Examples # Export the RSA local public key in OpenSSH format.
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub

```

```

Display the RSA local public key in SSH2 format.

```

```

<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20061105"
AAAAB3NzaC1yc2EAAAADAQABAAQgKRKxfoZ+T72Srs9c60+j2yrkd0AHBsXBh0Uq+iNvE12PaYR1On4
x+aNlwe9fjW1PYgzH+DRkTpiMrn3j2pIs7gaJXvefTW94rbVWJ94uiSDk1NLX1JcoTtWnQcVhft3mUZ+
J0jBEhAcw4bROe7/qr617VTC09FBZ0XgKuHroovX
---- END SSH2 PUBLIC KEY ----

```

```

Display the RSA local public key in OpenSSH format.

```

```

<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgLxMOSqXc0pjO6Dx2wH4TrUSKOyGreHbpZfg2QZv3E8Ed2zqNhD
SV4NB9dBJFDZw8ShlAsBtOdOfKPD1y6Yw2ozRwW7OinplKC8kB+h1fnk33M2122IM0fRxQbtxFxOXAjSERKLYkA
SXqHuNXxPWHE3vo9FKfcB2JHkFwdIm9i3z rsa-key

```

---

## public-key peer

**Syntax** `public-key peer keyname`  
`undo public-key peer keyname`

**View** System view

**Parameters** *keyname*: Public key name, a string of 1 to 64 characters.

**Description** Use the **public-key peer** command to enter public key view.

Use the **undo public-key peer** command to delete the configuration of peer public key.

After entering public key view, you can configure the peer public key with the **public-key-code begin** and **public-key-code end** commands. This requires that you obtain the hexadecimal public key from the peer beforehand.

**Related commands:** **public-key-code begin**, **public-key-code end**.

**Examples** # Enter public key view, specifying a public key name of key1.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key]
```

---

## public-key peer import sshkey

**Syntax** `public-key peer keyname import sshkey filename`  
`undo public-key peer keyname`

**View** System view

**Parameters** *keyname*: Public key name, a string of 1 to 64 characters.

*filename*: Public key file name.

**Description** Use the **public-key peer import sshkey** command to import a peer public key from the public key file.

Use the **undo public-key peer import sshkey** command to remove the setting.

After execution of this command, the system automatically transforms the public key file in SSH1, SSH2 or OpenSSH format to PKCS format, and imports the peer public key. This requires that you get a copy of the public key file from the peer through FTP/TFTP.



**Examples** # Import a peer public key named **key2** from public key file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```

---

## sftp

**Syntax** **sftp** *server* [*port-number*] [**prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } ] \*

**View** User view

**Parameters** *server*: IPv4 address or name of the server, a string of 1 to 20 characters.

*port-number*: Port number of the server, in the range 0 to 65535. The default is 22.

**prefer-ctos-cipher**: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

**prefer-ctos-hmac**: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

**prefer-kex**: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

**prefer-stoc-cipher**: Preferred algorithm from server to client, defaulted to **aes128**.

**prefer-stoc-hmac**: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

**Description** Use the **sftp** command to establish a connection to a remote IPv4 SFTP server and enter SFTP client view.

**Examples** # Connect to SFTP server 10.1.1.2.

```
<Sysname> sftp 10.1.1.2
Input Username:
```

## sftp client ipv6 source

**Syntax** **sftp client ipv6 source** { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

**undo sftp client ipv6 source**

**View** System view

**Parameters** **ipv6** *ipv6-address*: Specifies a source IPv6 address.

**interface** *interface-type interface-number*: Specifies a source interface by its type and number.

**Description** Use the **sftp client ipv6 source** command to specify the source IPv6 address or source interface for an SFTP client.

Use the **undo sftp client ipv6 source** command to remove the configuration.

By default, the client uses the interface address specified by the route of the device to access the SFTP server.

**Examples** # Specify the source IPv6 address of the SFTP client as 2:2::2:2.

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

## sftp client source

**Syntax** **sftp client source** { **ip** *ip-address* | **interface** *interface-type interface-number* }

**undo sftp client source**

**View** System view

**Parameters** **ip** *ip-address*: Specifies a source IPv4 address.

**interface** *interface-type interface-number*: Specifies a source interface by its type and number.

**Description** Use the **sftp client source** command to specify the source IPv4 address or interface of an SFTP client.

Use the **undo sftp source-interface** command to remove the configuration.

By default, a client uses the IP address or interface specified by the route to access the SFTP server.

**Related commands:** **display sftp client source.**

**Examples** # Specify the source IP address of the SFTP client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

---

## sftp ipv6

**Syntax** **sftp ipv6** *server* [*port-number*] [**prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } ] \*

**View** User view

**Parameters** *server*: IPv6 address or name of the server, a string of 1 to 46 characters.

*port-number*: Port number of the server, in the range 0 to 65535. The default is 22.

**prefer-ctos-cipher**: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

**prefer-ctos-hmac**: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

**prefer-kex**: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

**prefer-stoc-cipher**: Preferred encryption algorithm from server to client, defaulted to **aes128**.

**prefer-stoc-hmac:** Preferred HMAC algorithm from server to client, defaulted to **sha1**.

**Description** Use the **sftp ipv6** command to establish a connection to a remote IPv6 SFTP server and enter SFTP client view.

**Examples** # Connect to server 2:5::8:9.  
 <Sysname> sftp ipv6 2:5::8:9  
 Input Username:

## sftp server enable

**Syntax** **sftp server enable**

**undo sftp server enable**

**View** System view

**Parameters** None

**Description** Use the **sftp server enable** command to enable SFTP server.  
 Use the **undo sftp server enable** command to disable SFTP server.  
 By default, SFTP server is disabled.

**Related commands:** **display ssh server.**

**Examples** # Enable SFTP server.  
 <Sysname> system-view  
 [Sysname] sftp server enable

## sftp server idle-timeout

**Syntax** **sftp server idle-timeout** *time-out-value*

**undo sftp server idle-timeout**

**View** System view

**Parameters** *time-out-value*: Timeout period in minutes. It ranges from 1 to 35,791.

**Description** Use the **sftp server idle-timeout** command to set the idle timeout period for SFTP user connections.  
 Use the **undo sftp server idle-timeout** command to restore the default.

By default, the idle timeout period is 10 minutes.

**Related commands:** **display ssh server.**

**Examples** # Set the idle timeout period for SFTP user connections to 500 minutes.

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

## ssh client authentication server

**Syntax** **ssh client authentication server** *server* **assign publickey** *keyname*

**undo ssh client authentication server** *server* **assign publickey**

**View** System view

**Parameters** *server*: IP address or name of the server, a string of 1 to 80 characters.

*keyname*: Name of the host public key of the server, a string of 1 to 64 characters.

**Description** Use the **ssh client authentication server** command to configure the host public key of the server so that the client can determine whether the server is trustworthy.

Use the **undo ssh authentication server** command to remove the configuration.

By default, the host public key of the server is not configured, and when logging into the server, the client uses the IP address or host name used for login as the public key name.

**Examples** # Configure the public key of the server with the IP address of 192.168.0.1 to be key1.

```
<Sysname> system-view
[Sysname] ssh client authentication server 192.168.0.1 assign rsa-key key1
```

## ssh client first-time enable

**Syntax** **ssh client first-time enable**

**undo ssh client first-time**

**View** System view

**Parameters** None

- Description** Use the **ssh client first-time enable** command to enable the first authentication function.
- Use the **undo ssh client first-time** command to disable the function.
- By default, the function is enabled.
- When an SSH client tries to access a server whose public host key it does not know for the first time, the first authentication function enables it to access the server and obtain and save the public host key of the server. When the client accesses the server later, it can use the locally saved public host key of the server to authenticate the server.
- With the first authentication function disabled, an SSH client cannot access any server whose public host key it does not know. In this case, you must configure the public host key of the server to be accessed and specify the public key name on the client at first.

**Examples** # Enable the first authentication function.

```
<Sysname> system-view
[Sysname] ssh client first-time enable
```

---

## ssh client ipv6 source

- Syntax** **ssh client ipv6 source** { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }
- undo ssh client ipv6 source**
- View** System view
- Parameters** **ipv6** *ipv6-address*: Specifies a source IPv6 address.
- interface** *interface-type interface-number*: Specifies a source interface by its type and number.
- Description** Use the **ssh client ipv6 source** command to specify the source IPv6 address or source interface for the SSH client.
- Use the **undo ssh client ipv6 source** command to remove the configuration.
- By default, the client uses the source address specified by the route of the device to access the SSH server.
- Examples** # Specify the source IPv6 address as 2:2::2:2 for the SSH client.
- ```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

ssh client source

Syntax **ssh client source** { **ip** *ip-address* | **interface** *interface-type interface-number* }
undo ssh client source

View System view

Parameters **ip** *ip-address*: Specifies a source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description Use the **ssh client source** command to specify the source IPv4 address or source interface of the SSH client.

Use the **undo ssh client source** command to remove the configuration.

By default, an SSH client uses the IP address or interface specified by the route to access the SSH server.

Related commands: **display ssh client source.**

Examples # Specify the source IPv4 address of the SSH client as 192.168.0.1.

```
<Sysname> system-view  
[Sysname] ssh client source ip 192.168.0.1
```

ssh server authentication-retries

Syntax **ssh server authentication-retries** *times*
undo ssh server authentication-retries

View System view

Parameters *times*: Maximum number of authentication attempts, in the range 1 to 5.

Description Use the **ssh server authentication-retries** command to set the maximum number of SSH connection authentication attempts, which takes effect at next login.

Use the **undo ssh server authentication-retries** command to restore the default.

By default, the maximum number of SSH connection authentication attempts is 3.

Note that the threshold specified by using the **ssh server authentication-retries** command takes into account both publickey authentication attempts and password authentication attempts.

Related commands: **display ssh server.**

Examples # Set the maximum number of SSH connection authentication attempts to four.

```
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

ssh server authentication-timeout

Syntax **ssh server authentication-timeout** *time-out-value*

undo ssh server authentication-timeout

View System view

Parameters *time-out-value*: Authentication timeout period in seconds, in the range 1 to 120.

Description Use the **ssh server authentication-timeout** command to set the SSH user authentication timeout period on the SSH server.

Use the **undo ssh server authentication-timeout** command to restore the default.

By default, the authentication timeout period is 60 seconds.

Related commands: **display ssh server.**

Examples # Set the SSH user authentication timeout period to 10 seconds.

```
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

ssh server compatible-ssh1x enable

Syntax **ssh server compatible-ssh1x enable**

undo ssh server compatible-ssh1x

View System view

Parameters None

Description Use the **ssh server compatible-ssh1x** command to enable the SSH server to work with SSH1.x clients.

Use the **undo ssh server compatible-ssh1x** command to disable the SSH server from working with SSH1.x clients.

By default, the SSH server can work with SSH1.x clients.

This configuration takes effect at next login.

Related commands: **display ssh server.**

Examples # Enable the SSH server to work with SSH1.x clients.

```
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

ssh server enable

Syntax **ssh server enable**
undo ssh server enable

View System view

Parameters None

Description Use the **ssh server enable** command to enable SSH server.
Use the **undo ssh server enable** command to disable SSH server.
By default, SSH server is disabled.

Examples # Enable SSH server.

```
<Sysname> system-view
[Sysname] ssh server enable
```

ssh server rekey-interval

Syntax **ssh server rekey-interval** *hours*
undo ssh server rekey-interval

View System view

Parameters *hours*: Server key pair update interval in hours, in the range 1 to 24.

Description Use the **ssh server rekey-interval** command to set the interval for updating the RSA server key.

Use the **undo ssh server rekey-interval** command to remove the configuration.

By default, the update interval of the RSA server key is 0, that is, the RSA server key is not updated.

Related commands: **display ssh server.**



CAUTION: This command is only available to SSH users using SSH1 client software.

Examples # Set the RSA server key pair update interval to three hours.

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

ssh user

Syntax **ssh user** *username* **service-type** **stelnet** **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* } **work-directory** *directory-name* }

undo ssh user *username*

View System view

Parameters *username*: SSH username, a string of 1 to 80 characters.

service-type: Specifies the service type of an SSH user, which can be one of the following:

- **all**: Specifies both secure Telnet and secure FTP.
- **sftp**: Specifies the service type as secure FTP.
- **stelnet**: Specifies the service type of secure Telnet.

authentication-type: Specifies the authentication method of an SSH user, which can be one the following:

- **password**: Performs password authentication.
- **any**: Performs either password authentication or publickey authentication. The server performs publickey authentication first.
- **password-publickey**: Performs both password authentication and publickey authentication. A client running SSH1 client only needs to pass either type of authentication while a client running SSH2 client must pass both types of authentication to log in.
- **publickey**: Performs publickey authentication.

assign publickey *keyname*: Assigns an existing public key for an SSH user. *keyname* indicates the name of the client public key and is a string of 1 to 64 characters.

work-directory *directory-name*: Specifies the working folder for an SFTP user. *directory-name* indicates the name of the working folder and is a string of 1 to 135 characters.

Description Use the **ssh user** command to create an SSH user and specify the service type and authentication method.

Use the **undo ssh user** *username* command to delete an SSH user.

Note that:

- For a publickey authentication user, you must configure the username and the public key on the device. For a password authentication user, you can configure the account information on either the device or the remote authentication server such as a RADIUS server.
- If you use the **ssh user** command to configure a public key for a user who has already had a public key, the new one overwrites the old one.
- Authentication method and public key configuration for a user that has logged in takes effect when the user logs in next time.
- If an SFTP user has been assigned a public key, it is necessary to set a working folder for the user.
- The working folder of an SFTP user is subject to the user authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both the publickey and password authentication methods, the working folder is the one set by using the **ssh user** command.

Related commands: **display ssh user-information.**

Examples # Create an SSH user named **user1**, setting the service type as **sftp**, the authentication method as **publickey**, the work folder of the SFTP server as **flash**, and assigning a public key named **key1** to the user.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type publickey assign publickey key1 work-directory flash:
```

ssh2

Syntax **ssh2** *server* [*port-number*] [**prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View User view

Parameters *server*: IPv4 address or name of the server, a string of 1 to 20 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **ssh2** command to establish a connection to an SSH server, and specify the preferred key exchange algorithm, encryption algorithms, and HMAC algorithms of the client and the server.

Examples # Log in to remote SSH2 server 10.214.50.51, setting the algorithms as follows:

- Preferred key exchange algorithm: DH-group1
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> ssh2 10.214.50.51 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```

ssh2 ipv6

Syntax **ssh2 ipv6** *server* [*port-number*] [**prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex**

{ **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View User view

Parameters *server*: IPv6 address or name of the server, a string of 1 to 46 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, default to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **ssh2 ipv6** command to establish a connection to an IPv6 SSH server and specify the preferred key exchange algorithm, encryption algorithms, and HMAC algorithms of the client and the server.

Examples # Login to remote SSH2 server 2000::1, setting the algorithms as follows:

- Preferred key exchange algorithm: DH-group1
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```


52

ARP CONFIGURATION COMMANDS

arp max-learning-num

Syntax `arp max-learning-num number`

`undo arp max-learning-num`

View VLAN interface view

Parameters *number*: Maximum number of dynamic ARP entries that a VLAN interface can learn, in the range 1 to 8192.

Description Use the **arp max-learning-num** command to set the maximum number of dynamic ARP entries that a VLAN interface can learn.

Use the **undo arp max-learning-num** command to restore the default.

By default, a VLAN interface can learn up to 8,192 dynamic ARP entries.

Examples # Specify VLAN-interface 40 to learn up to 500 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 500
```

arp static

Syntax `arp static ip-address mac-address [vlan-id interface-type interface-number]`

`undo arp ip-address`

View System view

Parameters *ip-address*: IP address in an ARP entry.

mac-address: MAC address in an ARP entry, in the format H-H-H.

vlan-id: ID of a VLAN to which a static ARP entry belongs to, in the range 1 to 4094.

interface-type interface-number: Port type and port number.

Description Use the **arp static** command to configure a static ARP entry in the ARP mapping table.

Use the **undo arp** command to remove an ARP entry.

Note that:

- A static ARP entry is effective when the device works normally. However, when the VLAN or VLAN interface to which an ARP entry corresponds is deleted, the entry, if permanent, will be deleted, and if non-permanent and resolved, will become unresolved. A VLAN interface must be created for the VLAN.
- The *vlan-id* argument is used to specify the corresponding VLAN of an ARP entry and must be the ID of an existing VLAN. In addition, the Ethernet port following the argument must belong to that VLAN.

Related commands: **reset arp, display arp.**

Examples # Configure a static ARP entry, with the IP address being 202.38.10.2, the MAC address being 000f-e201-0000, and the outbound port being GigabitEthernet 2/0/10 of VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 000f-e201-0000 10 gigabitethernet 2/0/10
```

arp timer aging

Syntax **arp timer aging** *aging-time*

undo arp timer aging

View System view

Parameters *aging-time*: Aging time for dynamic ARP entries in minutes. It ranges from 1 to 1,440 and defaults to 20.

Description Use the **arp timer aging** command to set aging time for dynamic ARP entries.
Use the **undo arp timer aging** command to restore the default.

Related commands: **display arp timer aging.**

Examples # Set aging time for dynamic ARP entries to 10 minutes.

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

display arp

Syntax **display arp** { { **all** | **dynamic** | **static** } [**slot** *slot-id*] | **vlan** *vlan-id* | **interface** *interface-type interface-number* } [[**verbose**] [[{ **begin** | **exclude** | **include** } *string*]] | **count**]

View Any view

Parameters **all**: Displays all ARP entries.

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

slot *slot-id*: Displays the ARP entries of the specified slot.

vlan *vlan-id*: Displays the ARP entries of the specified VLAN. The VLAN ID ranges from 1 to 4,094.

interface *interface-type interface-number*: Displays the ARP entries of the port specified by the argument *interface-type interface-number*.

verbose: Displays detailed information about ARP entries.

]: Uses a regular expression to specify the ARP entries to be displayed. For detailed information about regular expression, refer to "Parameters" on page 1165.

begin: Displays ARP entries from the first one containing the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

include: Displays the ARP entries containing the specified string.

string: A case-sensitive string for matching, consisting of 1 to 256 characters.

count: Displays the number of ARP entries.

Description Use the **display arp** command to display ARP entries in the ARP mapping table.

Related commands: **arp static**, **reset arp**.

Examples # Display the information of all ARP entries.

```
<Sysname> display arp all
                                     Type: S-Static   D-Dynamic
IP Address      MAC Address      VLAN ID  Interface      Aging Type
20.1.1.1        000f-e200-0001  N/A     N/A            N/A     S
193.1.1.70     00e0-fe50-6503  100     GE2/0/1        DIS     D
192.168.0.115  000d-88f7-9f7d  1       GE2/0/2        DIS     D
192.168.0.39   0012-a990-2241  1       GE2/0/3        DIS     D
```

Table 205 Field descriptions of the display arp command

| Field | Description |
|-------------|---|
| IP Address | IP address in an ARP entry |
| MAC Address | MAC address in an ARP entry |
| VLAN ID | VLAN ID contained a static ARP entry |
| Interface | Outbound port in an ARP entry |
| Aging | Aging time for a dynamic ARP entry in minutes. "DIS" means the ARP entry is learned from an interface module. |
| Type | ARP entry type: D stands for dynamic and S for static. |

```
# Display the number of all ARP entries
```

```
<Sysname> display arp all count
Total Entry(ies): 4
```

display arp ip-address

Syntax **display arp** *ip-address* [**slot** *slot-id*] [**verbose**] [[{ **begin** | **exclude** | **include** } *string*]

View Any view

Parameters *ip-address*: Displays the ARP entry for the specified IP address.

slot *slot-id*: Displays the ARP entry for the specified slot.

verbose: Displays the detailed information about ARP entries.

]: Uses a regular expression to specify the ARP entries to be displayed. For detailed information about regular expression, refer to "Parameters" on page 1165

begin: Displays the ARP entries from the first one containing the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

include: Displays the ARP entries that contain the specified string.

string: A case-sensitive string for matching, consisting of 1 to 256 characters.

Description Use the **display arp** *ip-address* command to display the ARP entry for a specified IP address.

Related commands: **arp static**, **reset arp**.

Examples # Display the corresponding ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
Type: S-Static      D-Dynamic
IP Address          MAC Address        VLAN ID  Interface        Aging Type
20.1.1.1            000f-e200-0001    N/A      N/A              N/A      S
```

display arp timer aging

Syntax **display arp timer aging**

View Any view

Parameters None

Description Use the **display arp timer aging** command to display the aging time for dynamic ARP entries.

Related commands: **arp timer aging.**

Examples # Display the aging time for dynamic ARP entries.

```
[Sysname] display arp timer aging
Current ARP aging time is 10 minute(s)
```

naturemask-arp enable

Syntax **naturemask-arp enable**
undo naturemask-arp enable

View System view

Parameters None

Description Use the **naturemask-arp enable** command to cancel the restriction that ARP requests must be from the same subnet. In this case, ARP requests from a natural network are supported.

Use the **undo naturemask-arp enable** command to restore the default.

By default, the support for ARP requests from a natural network is disabled.

Examples # Enable the support for ARP requests from a natural network.

```
<Sysname> system-view
[Sysname] naturemask-arp enable
```

reset arp

Syntax **reset arp** { **all** | **dynamic** | **slot** *slot-id* | **static** | **interface** *interface-type interface-number* }

View User view

- Parameters**
- all:** Clears all ARP entries.
 - dynamic:** Clears all dynamic ARP entries.
 - static:** Clears all static ARP entries.
 - slot** *slot-id*: Clears the ARP entries for the specified slot.
 - interface** *interface-type interface-number*: Clears the ARP entries for the port specified by the argument *interface-type interface-number*.

Description Use the **reset arp** command to clear ARP entries from the ARP mapping table.

With **interface** *interface-type interface-number* or **slot** *slot-id* specified, the command clears only dynamic ARP entries of the port or the slot.

Related commands: **arp static**, **display arp**.

Examples

```
# Clear all static ARP entries.  
<Sysname> reset arp static
```

53

GRATUITOUS ARP CONFIGURATION COMMANDS

gratuitous-arp-sending enable

Syntax **gratuitous-arp-sending enable**
undo gratuitous-arp-sending enable

View System view

Parameters None

Description Use the **gratuitous-arp-sending enable** command to enable a device to send gratuitous ARP packets when receiving ARP requests from another network segment.

Use the **undo gratuitous-arp-sending enable** command to restore the default.

By default, a device cannot send gratuitous ARP packets when receiving ARP requests from another network segment.

Examples # Disable a device from sending gratuitous ARP packets.

```
<Sysname> system-view  
[Sysname] undo gratuitous-arp-sending enable
```

gratuitous-arp-learning enable

Syntax **gratuitous-arp-learning enable**
undo gratuitous-arp-learning enable

View System view

Parameters None

Description Use the **gratuitous-arp-learning enable** command to enable the gratuitous ARP packet learning function.

Use the **undo gratuitous-arp-learning enable** command to disable the function.

By default, the function is enabled.

Examples # Disable the gratuitous ARP packet learning function.

```
<Sysname> system-view  
[Sysname] undo gratuitous-arp-learning enable
```

54

ARP SOURCE SUPPRESSION CONFIGURATION COMMANDS

arp source-suppression enable

Syntax **arp source-suppression enable**
undo arp source-suppression enable

View System view

Parameters None

Description Use the **arp source-suppression enable** command to enable the ARP source suppression function.

Use the **undo arp source-suppression enable** command to disable the function.

By default, the ARP source suppression function is disabled.

Related commands: **display arp source-suppression.**

Examples # Enable the ARP source suppression function.

 <Sysname> system-view
 System View: return to User View with Ctrl+Z.
 [Sysname] arp source-suppression enable

arp source-suppression limit

Syntax **arp source-suppression limit** *limit-value*
undo arp source-suppression limit

View System view

Parameters *limit-value*: Specifies the maximum number of packets with the same source IP address but unresolvable destination IP addresses that a port can receive in five seconds. It ranges from 2 to 1,024.

Description Use the **arp source-suppression limit** command to set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that a port can receive in five seconds.

Use the **undo arp source-suppression limit** command to restore the default value, which is 10.

Related commands: **display arp source-suppression.**

Examples # Set to 100 the maximum number of packets with the same source address but unresolvable destination IP addresses that a port can receive in five seconds.

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

display arp source-suppression

Syntax **display arp source-suppression**

View Any view

Parameters None

Description Use the **display arp source-suppression** command to display information about the current ARP source suppression configuration.

Examples # Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
ARP source suppression is enabled
Current suppression limit: 100
Current cache length: 16
```

Table 206 Description on fields of display arp source-suppression

| Field | Description |
|-----------------------------------|---|
| ARP source suppression is enabled | The ARP source suppression function is enabled |
| Current suppression limit | Maximum number of packets with the same source IP address but unresolvable IP addresses that the device can receive in five seconds |
| Current cache length | Size of cache used to record source suppression information |

55

ARP SPOOFING PROTECTION CONFIGURATION COMMANDS

arp resolving-route enable

Syntax **arp resolving-route enable**
undo arp resolving-route enable

View System view

Parameters None

Description Use the **arp resolving-route enable** command to enable ARP defense against IP packet attacks.

Use the **undo arp resolving-route enable** command to disable the function.

By default, the support for ARP defense against IP packet attacks is enabled.

Examples # Enable ARP defense against IP packet attacks.

```
<Sysname> system-view  
[Sysname] arp resolving-route enable
```


56

PROXY ARP CONFIGURATION COMMANDS

proxy-arp enable

Syntax **proxy-arp enable**
undo proxy-arp enable

View VLAN interface view

Parameters None

Description Use the **proxy-arp enable** command to enable proxy ARP.
Use the **undo proxy-arp enable** command to disable proxy ARP.
By default, proxy ARP is disabled.

Related commands: **display proxy-arp.**

Examples # Enable proxy ARP on VLAN-interface 2.

```
<Sysname> system-view  
[Sysname] interface vlan-interface 2  
[Sysname-Vlan-interface2] proxy-arp enable
```

local-proxy-arp enable

Syntax **local-proxy-arp enable**
undo local-proxy-arp enable

View VLAN interface view

Parameters None

Description Use the **local-proxy-arp enable** command to enable local proxy ARP.
Use the **undo local-proxy-arp enable** command to disable local proxy ARP.
By default, local proxy ARP is disabled.

Related commands: **display local-proxy-arp.**

Examples # Enable local proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable
```

display proxy-arp

Syntax **display proxy-arp** [**interface Vlan-interface** *vlan-id*]

View Any view

Parameters **interface Vlan-interface** *vlan-id*: Displays the proxy ARP status of the VLAN interface specified by the argument *vlan-id*.

Description Use the **display proxy-arp** command to display the proxy ARP status.

Related commands: **proxy-arp enable.**

Examples # Display the proxy ARP status on VLAN-interface 1.

```
<Sysname> display proxy-arp interface vlan-interface 1
Interface Vlan-interfacel
Proxy ARP status: disabled
```

display local-proxy-arp

Syntax **display local-proxy-arp** [**interface Vlan-interface** *vlan-id*]

View Any view

Parameters **interface vlan-interface** *vlan-id*: Displays the local proxy ARP status of the VLAN interface specified by the argument *vlan-id*.

Description Use the **display local-proxy-arp** command to display the status of the local proxy ARP.

Related commands: **local-proxy-arp enable.**

Examples # Display the status of the local proxy ARP on VLAN-interface 2.

```
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
Local Proxy ARP status: enabled
```

57

DHCP SERVER CONFIGURATION COMMANDS



- *The DHCP server configuration is supported only on VLAN interfaces and loopback interfaces. The subaddress pool configuration is not supported on loopback interfaces.*
- *DHCP Snooping must be disabled on the DHCP server.*

bims-server

Syntax **bims-server ip** *ip-address* [**port** *port-number*] **sharekey** *key*
undo bims-server

View DHCP address pool view

Parameters **ip** *ip-address*: Specifies an IP address for the BIMS server.

port *port-number*: Specifies a port number for the BIMS server in the range 1 to 65534.

sharekey *key*: Specifies a shared key for the BIMS server, which is a string of 1 to 16 characters.

Description Use the **bims-server** command to specify the IP address, port number, and shared key of the BIMS server in the DHCP address pool for the client.

Use the **undo bims-server** command to remove BIMS server information assigned from the DHCP address pool to the DHCP client.

By default, no BIMS server information is specified.

If you execute the **bims-server** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

Examples # Specify the IP address 1.1.1.1, port number 80, shared key **aabbcc** of the BIMS server in DHCP address pool 0 for the client.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey aabbcc
```

bootfile-name**Syntax** **bootfile-name** *bootfile-name***undo bootfile-name****View** DHCP address pool view**Parameters** *bootfile-name*: Boot file name, a string of 1 to 63 characters.**Description** Use the **bootfile-name** command to specify a bootfile name in the DHCP address pool for the client.Use the **undo bootfile-name** command to remove the specified bootfile name assigned from the DHCP address pool to the DHCP client.

By default, no bootfile name is specified.

If you execute the **bootfile-name** command repeatedly, the latest configuration will overwrite the previous one.**Examples** # Specify the bootfile name **aaa** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name aaa
```

dhcp enable**Syntax** **dhcp enable****undo dhcp enable****View** System view**Parameters** None**Description** Use the **dhcp enable** command to enable DHCP.Use the **undo dhcp enable** command to disable DHCP.

By default, DHCP is disabled.

*You need to enable DHCP before performing DHCP server and relay agent configurations.***Examples** # Enable DHCP.

```
<Sysname> system-view
[Sysname] dhcp enable
```

dhcp select server global-pool

Syntax **dhcp select server global-pool** [**subaddress**]
undo dhcp select server global-pool subaddress

View Interface view

Parameters **subaddress**: Supports subaddress allocation. That is, the DHCP server and clients are on the same network segment, and the server allocates IP addresses from the address pool containing the network segment of the first subaddress if several subaddresses exist.

Description Use the **dhcp select server global-pool** command to enable the DHCP server on specified interface(s). After the interface receives a DHCP request, the DHCP server will allocate an IP address from the address pool.

Use the **undo dhcp select server global-pool subaddress** command to cancel the support for subaddress allocation.

By default, the DHCP server is enabled on an interface.

Examples # Enable the DHCP server on VLAN-interface 1.

```
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] dhcp select server global-pool
```

dhcp server detect

Syntax **dhcp server detect**
undo dhcp server detect

View System view

Parameters None

Description Use the **dhcp server detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp server detect** command to disable the function.

By default, the function is disabled.

Examples # Enable unauthorized DHCP server detection.

```
<Sysname> system-view  
[Sysname] dhcp server detect
```

dhcp server forbidden-ip

Syntax `dhcp server forbidden-ip low-ip-address [high-ip-address]`

`undo dhcp server forbidden-ip low-ip-address [high-ip-address]`

View System view

Parameters *low-ip-address*: Start IP address of the IP address range to be excluded from dynamic allocation.

high-ip-address: End IP address of the IP address range to be excluded from dynamic allocation. The end IP address must have a higher sequence than the start one.

Description Use the **dhcp server forbidden-ip** command to exclude IP addresses from dynamic allocation.

Use the **undo dhcp server forbidden-ip** command to remove the configuration.

By default, all IP addresses in a DHCP address pool are assignable except IP addresses of the DHCP server interfaces.

Note that:

- When you use the **dhcp server forbidden-ip** command to exclude an IP address that is bound to a user from dynamic assignment, the address can be still assigned to the user.
- When you use the **undo dhcp server forbidden-ip** command to remove the configuration, the specified address/address range must be consistent with the one specified with the **dhcp server forbidden-ip** command. If you have configured to exclude an address range from dynamic assignment, you need to specify an address range in the **undo dhcp server forbidden-ip** command instead of specifying one IP address.

Related commands: `dhcp server ip-pool`, `network`, `static-bind ip-address`.

Examples # Exclude the IP address range 10.110.1.1 to 10.110.1.63 from dynamic allocation.

```
<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

dhcp server ip-pool

Syntax `dhcp server ip-pool pool-name`

`undo dhcp server ip-pool pool-name`

View System view

Parameters *pool-name*: Global address pool name, which is a unique pool identifier, a string of 1 to 35 characters.

Description Use the **dhcp server ip-pool** command to create a DHCP address pool and enter its view. If the pool was created, you will directly enter its view.

Use the **undo dhcp server ip-pool** command to remove specified DHCP address pool.

By default, no DHCP address pool is created.

Related commands: **dhcp enable**.

Examples # Create the DHCP address pool identified by 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0]
```

dhcp server ping packets

Syntax **dhcp server ping packets** *number*

undo dhcp server ping packets

View System view

Parameters *number*: Number of ping packets, in the range of 0 to 10. 0 means no ping operation.

Description Use the **dhcp server ping packets** command to specify the maximum number of ping packets on the DHCP server.

Use the **undo dhcp server ping packets** command to restore the default.

The number defaults to 1.

Examples # Specify the maximum number of ping packets as 1.

```
<Sysname> system-view
[Sysname] dhcp server ping packets 10
```

dhcp server ping timeout

Syntax **dhcp server ping timeout** *milliseconds*

undo dhcp server ping timeout

| | |
|--------------------|--|
| View | System view |
| Parameters | <i>milliseconds</i> : Response timeout value for ping packets in milliseconds, in the range of 0 to 10,000. 0 means no ping operation. |
| Description | Use the dhcp server ping timeout command to configure response timeout time of the ping packet on the DHCP server.

Use the undo dhcp server ping timeout command to restore the default.

The time defaults to 500. |
| Examples | # Specify the response timeout time as 1000ms.

<pre><Sysname> system-view [Sysname] dhcp server ping timeout 1000</pre> |

dhcp server relay information enable

| | |
|--------------------|--|
| Syntax | dhcp server relay information enable

undo dhcp server relay information enable |
| View | System view |
| Parameters | None |
| Description | Use the dhcp server relay information enable command to enable the DHCP server to handle Option 82.

Use the undo dhcp server relay information enable command to configure the DHCP server to ignore Option 82.

By default, the DHCP server handles Option 82. |
| Examples | # Configure the DHCP server to ignore Option 82.

<pre><Sysname> system-view [Sysname] undo dhcp server relay information enable</pre> |

display dhcp server conflict

| | |
|-------------------|--|
| Syntax | display dhcp server conflict { all ip ip-address } |
| View | Any view |
| Parameters | all : Displays information about all IP address conflicts.

<i>ip-address</i> : Displays conflict information for the IP address. |

Description Use the **display dhcp server conflict** command to display information about IP address conflicts.

Related commands: **reset dhcp server conflict.**

Examples # Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict all
      Address           Discover time
      4.4.4.1           Apr 25 2007 16:57:20
--- total 1 entry ---
```

Table 207 Description on fields of the display dhcp server conflict command

| Field | Description |
|---------------|---------------------------------------|
| Address | Conflicted IP address |
| Discover Time | Time when the conflict was discovered |

display dhcp server expired

Syntax **display dhcp server expired** { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View Any view

Parameters **all**: Displays the lease expiration information of all DHCP address pools.

ip *ip-address*: Displays the lease expiration information of a specified IP address.

pool [*pool-name*]: Displays the lease expiration information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If the *pool name* is not specified, the lease expiration information of all address pools is displayed.

Description Use the **display dhcp server expired** command to display the lease expiration information of specified DHCP address pool(s) or an IP address.

DHCP will assign these expired IP addresses to DHCP clients after all addresses have been assigned.

Examples # Display information about lease expirations in all DHCP address pools.

```
<Sysname> display dhcp server expired all
Global pool:
 IP address           Client-identifier/      Lease expiration        Type
                    Hardware address
 4.4.4.6              3030-3066-2e65-3230-   Apr 25 2007 17:10:47   Release
                    302e-3130-3234-2d45-
                    7468-6572-6e65-7430-
                    2f31
--- total 1 entry ---
```

Table 208 Description on fields of the display dhcp server expired command

| Field | Description |
|-------------|---|
| Global pool | Information about lease expiration of a DHCP address pool |

Table 208 Description on fields of the display dhcp server expired command

| Field | Description |
|------------------------------------|--|
| IP address | Expired IP addresses |
| Client-identifier/Hardware address | IDs or MACs of clients whose IP addresses were expired |
| Lease expiration | The lease expiration time |
| Type | Types of lease expirations. Currently, this field is set to Release. |

display dhcp server free-ip

Syntax `display dhcp server free-ip`

View Any view

Parameters None

Description Use the **display dhcp server free-ip** command to display information about assignable IP addresses, which have never been assigned.

Examples # Display information about assignable IP addresses.

```
<Sysname> display dhcp server free-ip
IP Range from 10.0.0.0          to 10.0.0.255
```

display dhcp server forbidden-ip

Syntax `display dhcp server forbidden-ip`

View Any view

Parameters None

Description Use the **display dhcp server forbidden-ip** command to display IP addresses excluded from dynamic allocation in DHCP address pool.

Examples # Display IP addresses excluded from dynamic allocation in the DHCP address pool.

```
<Sysname> display dhcp server forbidden-ip
IP Range from 1.1.1.1          to 1.1.1.1
IP Range from 2.2.2.2          to 2.2.2.5
```

display dhcp server ip-in-use

Syntax `display dhcp server ip-in-use { all | ip ip-address | pool [pool-name] }`

View Any view

- Parameters** **all**: Displays the binding information of all DHCP address pools.
- ip** *ip-address*: Displays the binding information of a specified IP address.
- pool** [*pool-name*]: Displays the binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the binding information of all address pools is displayed.

Description Use the **display dhcp server ip-in-use** command to display the binding information of DHCP address pool(s) or an IP address.

Related commands: **reset dhcp server ip-in-use.**

Examples # Display the binding information of all DHCP address pools.

```
<Sysname> display dhcp server ip-in-use all
Global pool:
 IP address      Client-identifier/      Lease expiration      Type
                Hardware address
 10.1.1.1        4444-4444-4444         NOT Used              Manual
--- total 1 entry ---
```

Table 209 Description on fields of the display dhcp server ip-in-use command

| Field | Description |
|------------------------------------|--|
| Global pool | Binding information of a DHCP address pool |
| IP address | Bound IP address |
| Client-identifier/Hardware address | Client's ID or MAC of the binding |
| Lease expiration | Lease expiration time |
| Type | Binding types, including Manual, Auto:OFFERED and Auto:COMMITTED. <ul style="list-style-type: none"> ■ Manual: Static binding ■ Auto:OFFERED: The binding sent in the DHCP-OFFER message from the server to the client. ■ Auto:COMMITTED: The binding sent in the DHCP-ACK message from the server to the client. |

display dhcp server statistics

Syntax **display dhcp server statistics**

View Any view

Parameters None

Description Use the **display dhcp server statistics** command to display the statistics of the DHCP server.

Related commands: **reset dhcp server statistics.**

Examples # Display the statistics on the DHCP server.

```
<Sysname> display dhcp server statistics
Global Pool:
  Pool Number:          1
  Binding:
    Auto:               1
    Manual:             0
    Expire:             0
  BOOTP Request:       10
    DHCPDISCOVER:      5
    DHCPREQUEST:       3
    DHCPDECLINE:       0
    DHCPRELEASE:       2
    DHCPINFORM:        0
    BOOTPREREQUEST:    0
  BOOTP Reply:         6
    DHCPOFFER:         3
    DHCPACK:           3
    DHCPNAK:           0
    BOOTPREPLY:        0
  Bad Messages:        0
```

Table 210 Description on fields of the display dhcp server statistics command

| Field | Description |
|---------------|---|
| Global Pool | Statistics of a DHCP address pool |
| Pool Number | The number of address pools |
| Auto | The number of dynamic bindings |
| Manual | The number of static bindings |
| Expire | The number of expired bindings |
| BOOTP Request | The number of DHCP requests sent from DHCP clients to the DHCP server, including: <ul style="list-style-type: none"> ■ DHCPDISCOVER ■ DHCPREQUEST ■ DHCPDECLINE ■ DHCPRELEASE ■ DHCPINFORM ■ BOOTPREREQUEST |
| BOOTP Reply | The number of DHCP replies sent from the DHCP server to DHCP clients, including: <ul style="list-style-type: none"> ■ DHCPOFFER ■ DHCPACK ■ DHCPNAK ■ BOOTPREPLY |
| Bad Messages | The number of erroneous messages |

display dhcp server tree

Syntax `display dhcp server tree { all | pool [pool-name] }`

View Any view

Parameters **all**: Displays the tree organization information of all DHCP address pools.

pool [*pool-name*]: Displays the tree organization information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the tree organization information of all address pools will be displayed.

Description Use the **display dhcp server tree** command to display the tree organization information of DHCP address pool(s).

Examples # Display the tree organization information of all DHCP address pools.

```
<Sysname> display dhcp server tree all
Global pool:
```

```
Pool name: 0
network 20.1.1.0 mask 255.255.255.0
Sibling node:1
option 2 ip-address 1.1.1.1
expired 1 0 0
```

```
Pool name: 1
static-bind ip-address 10.10.1.2 mask 255.0.0.0
static-bind mac-address 00e0-00fc-0001
PrevSibling node:0
expired unlimited
```

Table 211 Description on fields of the display dhcp server tree command

| Field | Description |
|---|---|
| Global pool | Information of a address pool |
| Pool name | Address pool name |
| network | Network segment for address allocation |
| static-bind ip-address 10.10.1.2 mask 255.0.0.0 | The IP address and MAC address of the static binding |
| static-bind mac-address 00e0-00fc-0001 | |
| Sibling node | The sibling node of the current node, nodes of this kind in the output are: <ul style="list-style-type: none"> ■ Child node: The child node (subnet segment) address pool of the current node ■ Parent node: The parent node (nature network segment) address pool of the current node ■ Sibling node: The latter sibling node of the current node (another subnet of the same nature network). The earlier the sibling node is configured, the higher selection priority the sibling node has. ■ PrevSibling node: The previous sibling node of the current node |
| option | Self-defined DHCP options |
| expired | The lease duration, in the format of day, hour, and minute |

dns-list

Syntax **dns-list** *ip-address*&<1-8>

undo dns-list { *ip-address* | **all** }

View DHCP address pool view

Parameters *ip-address*&<1-8>: DNS server IP address. &<1-8> means you can specify up to eight DNS server addresses separated by spaces.

all: Specifies all DNS server addresses to remove.

Description Use the **dns-list** command to specify DNS server addresses in a DHCP address pool.

Use the **undo dns-list** command to remove DNS server addresses from a DHCP address pool.

By default, no DNS server address is specified.

If you repeatedly use the **dns-list** command, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

Examples # Specify the DNS server address 10.1.1.254 for the DHCP client in DHCP address pool 0.

```
<Sysname> system-view  
[Sysname] dhcp server ip-pool 0  
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

domain-name

Syntax **domain-name** *domain-name*

undo domain-name

View DHCP address pool view

Parameters *domain-name*: Domain name suffix for DHCP clients, a string of 1 to 50 characters.

Description Use the **domain-name** command to specify a domain name suffix for the DHCP clients in the DHCP address pool.

Use the **undo domain-name** command to remove the domain name suffix assigned from the DHCP address pool to the DHCP client.

No domain name suffix is specified by default.

Related commands: **dhcp server ip-pool.**

Examples # Specify a domain name suffix of mydomain.com for the DHCP clients in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name mydomain.com
```

expired

Syntax **expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo expired

View DHCP address pool view

Parameters **day** *day*: Specifies the number of days, in the range of 0 to 365.
hour *hour*: Specified the number of hours, in the range of 0 to 23.
minute *minute*: Specifies the number of minutes, in the range of 0 to 59.
unlimited: Specifies the infinite duration, which is actually 136 years.

Description Use the **expired** command to specify the lease duration in a DHCP address pool.
 Use the **undo expired** command to restore the default lease duration in a DHCP address pool.
 The lease duration defaults to one day.
 Note that if the lease duration you specified is beyond the year 2106, the system regards the lease as expired.

Related commands: **dhcp server ip-pool.**

Examples # Specify the lease duration as one day, two hours and three minutes in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3
```

gateway-list

Syntax **gateway-list** *ip-address*&<1-8>

undo gateway-list { *ip-address* | **all** }

View DHCP address pool view

Parameters *ip-address*&<1-8>: Gateway IP address. &<1-8> means you can specify up to eight gateway addresses separated by spaces.

all: Specifies all gateway IP addresses to be removed.

Description Use the **gateway-list** command to specify gateway address(es) in a DHCP address pool.

Use the **undo gateway-list** command to remove specified gateway address(es) specified for the DHCP client from a DHCP address pool.

By default, no gateway address is specified.

If you use the **gateway-list** command repeatedly, the latest configuration will overwrite the previous one.

Examples # Specify the gateway address 10.110.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.110.1.99
```

nbns-list

Syntax **nbns-list** *ip-address*&<1-8>

undo nbns-list { *ip-address* | **all** }

View DHCP address pool view

Parameters *ip-address*&<1-8>: WINS server IP address. &<1-8> means you can specify up to eight WINS server addresses separated by spaces.

all: Specifies all WINS server addresses to be removed.

Description Use the **nbns-list** command to specify WINS server address(es) in a DHCP address pool.

Use the **undo nbns-list** command to remove WINS server address(es) assigned from a DHCP address pool to the DHCP client.

By default, no WINS server address is specified.

If you use the **nbns-list** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **netbios-type**.

Examples # Specify WINS server address 10.12.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.12.1.99
```

netbios-type

Syntax **netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

View DHCP address pool view

Parameters **b-node**: Broadcast node. A b-node client sends the destination name in a broadcast message. The destination returns the name-to-IP mapping to the client after receiving the message.

p-node: Peer-to-peer node. A p-node client sends the destination name in a unicast message to the WINS server, and the WINS server returns the mapping to the client.

m-node: Mixed node, a combination of a b-node first and p-node second. An m-node client broadcasts the destination name, if there is no response, and then unicasts the destination name to the WINS server to get the mapping.

h-node: Hybrid node, a combination of a p-node first and b-node second. An h-node is a p-node with the peer-to-peer communication mechanism. An h-node client unicasts the destination name to the WINS server, if there is no response, and then broadcasts it to get the mapping from the destination.

Description Use the **netbios-type** command to specify the client NetBIOS node type in a DHCP address pool.

Use the **undo netbios-type** command to remove the client NetBIOS node type assigned from a DHCP address pool to the DHCP client.

By default, no NetBIOS node type is specified.

Related commands: **dhcp server ip-pool**, **nbns-list**.

Examples # Specify the NetBIOS node type as b-node in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type b-node
```

network

Syntax **network** *ip-address* [*mask-length* | **mask** *mask*]

undo network**View** DHCP address pool view**Parameters** *ip-address*: IP address range for dynamic allocation. If no mask length and mask is specified, the natural mask will be used.*mask-length*: Mask length, in the range of 1 to 30.**mask** *mask*: Specifies the IP address network mask, in dotted decimal format.**Description** Use the **network** command to specify the IP address range for dynamic allocation in a DHCP address pool.Use the **undo network** command to remove the specified address range.

No IP address range is specified by default.

Note that you can specify only one network segment for each DHCP global address pool. If you use the **network** command repeatedly, the latest configuration will overwrite the previous one.**Related commands:** **dhcp server ip-pool**, **dhcp server forbidden-ip**.**Examples** # Specify 192.168.8.0/24 as the address range for dynamic allocation in DHCP address pool 0.

```

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0

```

option**Syntax** **option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-16> | **ip-address** *ip-address*&<1-8> }**undo option** *code***View** DHCP address pool view**Parameters** *code*: Self-defined option number, in the range of 2 to 254.**ascii** *ascii-string*: Specifies an ASCII string with 1 to 63 characters.**hex** *hex-string*&<1-16>: Specifies hex digit strings. &<1-16> indicates you can specify up to 16 hex digit strings, separated by spaces. Each string contains 2, 4, 6 or 8 hex digits.**ip-address** *ip-address*&<1-8>: Specifies IP addresses. &<1-8> indicates you can specify up to eight IP addresses, separated by spaces.

- Description** Use the **option** command to configure a self-defined DHCP option in a DHCP address pool.
- Use the **undo option** command to remove a self-defined DHCP option from a DHCP address pool.
- The **option** command is not configured by default.
- If you use the **option** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool.**

- Examples** # Configure the hex digits 0x11 and 0x22 for the self-defined DHCP Option 100 in DHCP address pool 0.
- ```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 100 hex 11 22
```

## reset dhcp server conflict

**Syntax** **reset dhcp server conflict** { **all** | **ip** *ip-address* }

**View** User view

- Parameters** **all**: Clears the statistics of all IP address conflicts.
- ip** *ip-address*: Clears the conflict statistics of a specified IP address.

**Description** Use the **reset dhcp server conflict** command to clear statistics of IP address conflict(s).

**Related commands:** **display dhcp server conflict.**

- Examples** # Clears the statistics of all IP address conflicts.
- ```
<Sysname> reset dhcp server conflict all
```

reset dhcp server ip-in-use

Syntax **reset dhcp server ip-in-use** { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View User view

- Parameters** **all**: Clears the IP address dynamic binding information of all DHCP address pools.
- ip** *ip-address*: Clears the dynamic binding information of a specified IP address.

pool [*pool-name*]: Clears the dynamic binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the dynamic binding information of all address pools is cleared.

Description Use the **reset dhcp server ip-in-use** command to clear dynamic IP address binding information.

Related commands: **display dhcp server ip-in-use**

Examples # Clear the binding information of IP address 10.110.1.1.
 <Sysname> reset dhcp server ip-in-use ip 10.110.1.1

reset dhcp server statistics

Syntax **reset dhcp server statistics**

View User view

Parameters None

Description Use the **reset dhcp server statistics** command to clear the statistics of the DHCP server.

Related commands: **display dhcp server statistics.**

Examples # Clear the statistics of the DHCP server.
 <Sysname> reset dhcp server statistics

static-bind client-identifier

Syntax **static-bind client-identifier** *client-identifier*

undo static-bind client-identifier

View DHCP address pool view

Parameters *client-identifier*: The client ID of a static binding, a string with 4 to 160 characters in the format H-H-H..., each H indicates 4 hex digits except the last H indicates 2 or 4 hex digits. For example, aabb-cccc-dd is a valid ID, while aabb-c-dddd and aabb-cc-dddd are both invalid.

Description Use the **static-bind client-identifier** command to specify the client ID of a static binding in a DHCP address pool.

Use the **undo static-bind client-identifier** command to remove the client ID of a static binding from a DHCP address pool.

By default, no client ID is specified.

Note that:

- Use the **static-bind client-identifier** command together with the **static-bind ip-address** command to accomplish a static binding configuration.
- The ID of the static binding of a client must be identical to the ID displayed by using the **display dhcp client verbose** command on the client. Otherwise, the client cannot obtain an IP address.
- If you use the **static-bind client-identifier** or **static-bind mac-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool, static-bind ip-address, static-bind mac-address, display dhcp client.**

Examples # Bind the client ID aaaa-bbbb to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind client-identifier aaaa-bbbb
```

static-bind ip-address

Syntax **static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*]

undo static-bind ip-address

View DHCP address pool view

Parameters *ip-address*: IP address of a static binding, if no mask and mask length is specified, the natural mask is used.

mask-length: Mask length of the IP address, that is, the number of ones in the mask.

mask *mask*: Specifies the IP address mask, in dotted decimal format.

Description Use the **static-bind ip-address** command to specify an IP address in a DHCP address pool for a static binding.

Use the **undo static-bind ip-address** command to remove the statically bound IP address.

By default, no IP address is statically bound in a DHCP address pool.

Note that:

- Use the **static-bind ip-address** command together with the **static-bind mac-address** or **static-bind client-identifier** command to accomplish a static binding configuration.
- If the statically bound IP address is an interface address of the DHCP server, the static binding does not take effect.
- If you use the **static-bind ip-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **static-bind client-identifier**, **static-bind mac-address**.

Examples # Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

static-bind mac-address

Syntax **static-bind mac-address** *mac-address*

undo static-bind mac-address

View DHCP address pool view

Parameters *mac-address*: The MAC address of a static binding, in the format H-H-H.

Description Use the **static-bind mac-address** command to statically bind a MAC address to an IP address in a DHCP address pool.

Use the **undo static-bind mac-address** command to remove the statically bound MAC address.

By default, no MAC address is statically bound.

Note that:

- Use the **static-bind mac-address** command together with the **static-bind ip-address** command to complete a static binding configuration.
- If you use the **static-bind mac-address** or **static-bind client-identifier** command repeatedly, the latest configuration will overwrite the previous one.

Relate command: **dhcp server ip-pool**, **static-bind client-identifier** and **static-bind ip-address**.

Examples # Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
```



```
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

tftp-server domain-name

Syntax **tftp-server domain-name** *domain-name*

undo tftp-server domain-name

View DHCP address pool view

Parameters *domain-name*: TFTP server name, a string of 1 to 63 characters.

Description Use the **tftp-server domain-name** command to specify a TFTP server name in a DHCP address pool.

Use the **undo tftp-server domain-name** command to remove the TFTP server name from a DHCP address pool.

By default, no TFTP server name is specified.

Using the **tftp-server domain-name** command repeatedly will overwrite the previous configuration.

Examples # Specify the TFTP server name as **aaa** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

tftp-server ip-address

Syntax **tftp-server ip-address** *ip-address*

undo tftp-server ip-address

View DHCP address pool view

Parameters *ip-address*: TFTP server IP address.

Description Use the **tftp-server ip-address** command to specify the TFTP server IP address in a DHCP address pool.

Use the **undo tftp-server ip-address** command to remove the TFTP server IP address from a DHCP address pool.

By default, no TFTP server address is specified.

Using the **tftp-server ip-address** command repeatedly will overwrite the previous configuration.

Examples # Specify the TFTP server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

voice-config

Syntax **voice-config** { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

View DHCP address pool view

Parameters **as-ip** *ip-address*: Specifies IP address for the backup network calling processor.

fail-over *ip-address dialer-string*: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters, which can be 0 to 9, and "*".

ncp-ip *ip-address*: Specifies IP address for the primary network calling processor.

voice-vlan *vlan-id*: Specifies the voice VLAN ID, in the range of 2 to 4094.

- **disable**: Disables the specified voice VLAN ID, meaning DHCP clients will not take this ID as their voice VLAN.
- **enable**: Enables the specified voice VLAN ID, meaning DHCP clients will take this ID as their voice VLAN.

Description Use the **voice-config** command to configure specified Option 184 contents in a DHCP address pool.

Use the **undo voice-config** command to remove specified Option 184 contents from a DHCP address pool.

By default, no Option 184 content is configured.

Note that specifying the IP address of a network calling processor first is necessary to make other configured parameters take effect.

Examples # Configure Option 184 in DHCP address pool 0: the primary network calling processor 10.1.1.1, backup network calling processor 10.2.2.2, voice VLAN ID 3 that is enabled, the failover IP address 10.3.3.3 and dialer string 99*.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
```

```
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable  
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```


58

DHCP RELAY AGENT CONFIGURATION COMMANDS



- The DHCP relay agent configuration is supported only on VLAN interfaces.
- DHCP Snooping cannot be configured on the DHCP relay agent.

dhcp enable

Syntax **dhcp enable**
undo dhcp enable

View System view

Parameters None

Description Use the **dhcp enable** command to enable DHCP.
Use the **undo dhcp enable** command to disable DHCP.
By default, DHCP is disabled.



For both DHCP server and relay agent configuration, enabling DHCP first is necessary to make other configurations take effect.

Examples # Enable DHCP.

 <Sysname> system-view
 [Sysname] dhcp enable

dhcp relay address-check

Syntax **dhcp relay address-check { disable | enable }**

View Interface view

Parameters **disable**: Disables IP address match checking on the relay agent.
enable: Enables IP address match checking on the relay agent.

Description Use the **dhcp relay address-check enable** command to enable IP address match check on the relay agent.

Use the **dhcp relay address-check disable** command to disable IP address match check on the relay agent.

By default, the function is disabled.

Examples # Enable IP address match checking on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay address-check enable
```

dhcp relay information enable

Syntax **dhcp relay information enable**

undo dhcp relay information enable

View Interface view

Parameters None

Description Use the **dhcp relay information enable** command to enable the relay agent to support Option 82.

Use the **undo dhcp relay information enable** command to disable Option 82 support.

By default, Option 82 support is disabled on DHCP relay agent.

Examples # Enable Option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
```

dhcp relay information format

Syntax **dhcp relay information format** { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] }

undo dhcp relay information format [**verbose** **node-identifier**]

View Interface view

Parameters **normal**: Specifies the normal padding format.

verbose: Specifies the verbose padding format.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string with 1 to 50 characters.

Description Use the **dhcp relay information format** command to specify a padding format for Option 82.

Use the **undo dhcp relay information format** command to restore the default padding format.

The Option 82 padding format defaults to **normal**.



- Using the **undo dhcp relay information format** command without the keyword **verbose node-identifier** restores the default **normal** padding format, or with the keyword **verbose node-identifier** restores the **mac** mode of the **verbose** padding format.
- If configuring the handling strategy of the DHCP relay agent as **replace**, you need to configure a padding format of Option 82. If the handling strategy is **keep** or **drop**, you need not configure any padding format.
- If sub-option 1 (node identifier) of Option 82 is padded with the device name (*sysname*) of a node, the device name must contain no spaces. Otherwise, the DHCP relay agent will drop the message.

Examples # Specify the verbose padding format for Option 82.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy replace
[Sysname-Vlan-interface1] dhcp relay information format verbose
```

dhcp relay information strategy

Syntax **dhcp relay information strategy** { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

View Interface view

Parameters **drop**: Specifies to drop messages containing Option 82.

keep: Specifies to forward messages containing Option 82 without any change.

replace: Specifies to forward messages containing Option 82 after replacing the original Option 82 with the Option 82 padded in the specified padding format.

Description Use the **dhcp relay information strategy** command to configure DHCP relay agent handling strategy for messages containing Option 82.

Use the **undo dhcp relay information strategy** command to restore the default handling strategy.

The handling strategy for messages containing Option 82 defaults to **replace**.

Examples # Configure the DHCP relay agent handling strategy for messages containing Option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy keep
```

dhcp relay release

Syntax **dhcp relay release ip** *client-ip*

View System view

Parameters *client-ip*: DHCP client IP address.

Description Use the **dhcp relay release ip** command to request the DHCP server to release a specified client IP address.

Examples # Request the DHCP server to release the IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay security static

Syntax **dhcp relay security static** *ip-address mac-address* [**interface** *interface-type interface-number*]

undo dhcp relay security { *ip-address* | **all** | **dynamic** | **static** }

View System view

Parameters *ip-address*: Client IP address for creating a static binding.

mac-address: Client MAC address for creating a static binding, in the format H-H-H.

interface *interface-type interface-number*: Specifies an interface connecting to the DHCP client. *interface-type interface-number* specifies the interface type and interface number.

all: Specifies all client entries to be removed.

dynamic: Specifies dynamic client entries to be removed.

static: Specifies manual client entries to be removed.

Description Use the **dhcp relay security static** command to configure a static client entry, that is, the binding between IP address, MAC address, and VLAN interface on the relay agent.

Use the **undo dhcp relay security** command to remove specified client entries from the relay agent.

No manual client entry is configured on the DHCP relay agent by default.

Note that:

When using the **dhcp relay security static** command to bind an interface to a static client entry, make sure that the interface is configured as a DHCP relay agent; otherwise, entry conflicts may occur.

Related commands: **display dhcp relay security.**

Examples # Bind DHCP relay interface VLAN-interface 2 to IP address 10.10.1.1 and MAC address 0005-5d02-f2b3 of the client.

```
<Sysname> system-view
[Sysname] dhcp relay security static 1.1.1.1 0005-5d02-f2b3 interface vlan-interface 2
```

dhcp relay security tracker

Syntax **dhcp relay security tracker** { *interval* | **auto** }

undo dhcp relay security tracker [*interval*]

View System view

Parameters *interval*: Refreshing interval in seconds, in the range of 1 to 120.

auto: Specifies the **auto** refreshing interval, which is the value of 60 seconds divided by the number of binding entries. Thus, the more entries are, the shorter interval is, but the shortest interval is no less than 500 ms.

Description Use the **dhcp relay security tracker** command to set a refreshing interval at which the relay agent contacts the DHCP server for refreshing dynamic bindings.

Use the **undo dhcp relay security tracker** command to restore the default interval.

The default handshake interval is **auto**, the value of 60 seconds divided by the number of binding entries.

Examples # Set the handshake interval as 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay security tracker 100
```

dhcp relay server-detect

Syntax **dhcp relay server-detect**

undo dhcp relay server-detect

View System view

Parameters None

Description Use the **dhcp relay server-detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp relay server-detect** command to disable unauthorized DHCP server detection.

By default, unauthorized DHCP server detection is disabled.

Examples # Enable unauthorized DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp relay server-detect
```

dhcp relay server-group

Syntax **dhcp relay server-group** *group- id ip ip-address*

undo dhcp relay server-group *group-id [ip ip-address]*

View System view

Parameters *group-id*: DHCP server group number, in the range of 0 to 19.

ip ip-address: DHCP server IP address.

Description Use the **dhcp relay server-group** command to specify a DHCP server for a DHCP server group.

Use the **undo dhcp relay server-group** command to remove a DHCP server from a DHCP server group, if no **ip ip-address** is specified, all servers in the DHCP server group and the server group itself will be removed.

By default, no DHCP server is specified for a DHCP server group.

Note that:

- The IP address of any DHCP server and any interface's IP address of the DHCP relay agent cannot be in the same network segment. Otherwise, the client may fail to obtain an IP address.
- If a server group has been correlated to multiple interfaces, you need to cancel these correlations before removing the server group.

Related commands: **display dhcp relay server-group.**

Examples # Specify DHCP server 1.1.1.1 for DHCP server group 1 on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay server-group 1 ip 1.1.1.1
```

dhcp relay server-select

Syntax **dhcp relay server-select** *group-id*

undo dhcp relay server-select

View Interface view

Parameters *group-id*: DHCP server group number to be correlated, in the range of 0 to 19. The specified server group must be an existing group containing at least a DHCP server.

Description Use the **dhcp relay server-select** command to correlate specified interface(s) to a specified DHCP server group.

Use the **undo dhcp relay server-select** command to remove a configured correlation.

By default, no DHCP server group is correlated with an interface on the relay agent.

Note that an interface on the relay agent can only be correlated to one DHCP server group, and a newly configured correlation overwrites the previous one. If the server group in the new correlation does not exist, the new configuration will not work. The interface still maintains the previous correlation.

Examples # Correlate VLAN-interface 1 to DHCP server group 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay server-select 1
```

dhcp select relay

Syntax **dhcp select relay**

undo dhcp select relay

- View** Interface view
- Parameters** None
- Description** Use the **dhcp select relay** command to enable the relay agent on the current interface, specified or all interfaces. Upon receiving requests from an enabled interface, the relay agent will forward these requests to outside DHCP servers for IP address allocation.
- Use the **undo dhcp select relay** command to restore the default on interface(s).
- After DHCP is enabled, the DHCP server is enabled on an interface by default. That is, upon receiving a client's request from the interface, the DHCP server allocates an IP address from the DHCP address pool to the client.
- Examples** # Enable the DHCP relay agent on VLAN-interface 1.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select relay
```

---

## display dhcp relay

- Syntax** **display dhcp relay** { **all** | **interface** *interface-type interface-number* }
- View** Any view
- Parameters** **all**: Displays information of DHCP server groups that all interfaces correspond to.
- interface** *interface-type interface-number*: Displays information of the DHCP server group that a specified interface corresponds to.
- Description** Use the **display dhcp relay** command to display information about DHCP server groups correlated to an interface or all interfaces.
- Examples** # Display information about DHCP server groups correlated to all interfaces.

```
<Sysname> display dhcp relay all
 Interface name Server-group
 Vlan-interface3 2
```

**Table 212** Description on fields of the display dhcp relay all command

Field	Description
Interface name	Interface name
Server-group	DHCP server group number correlated to the interface.

---

## display dhcp relay security

- Syntax** **display dhcp relay security** [ *ip-address* | **dynamic** | **static** ]

- View** Any view
- Parameters** *ip-address*: Displays the binding information of an IP address.
- dynamic**: Displays information about dynamic bindings.
- static**: Displays information about static bindings.
- Description** Use the **display dhcp relay security** command to display information about bindings of DHCP relay agents. If no parameter is specified, information about all bindings will be displayed.

**Examples** # Display information about all bindings.

```
<Sysname> display dhcp relay security
 IP Address MAC Address Type Interface
 10.1.1.5 00e0-0000-0000 Static Vlan2
 10.10.1.2 0002-0002-0002 Static N/A
--- 2 dhcp-security item(s) found ---
```

**Table 213** Description on fields of the display dhcp relay security command

Field	Description
IP Address	Client IP address
MAC Address	Client MAC address
Type	Type of binding, including dynamic and static
Interface	VLAN interface connecting to the DHCP client. If no VLAN interface is recorded in the binding entry, "N/A" is displayed.

---

## display dhcp relay security statistics

- Syntax** **display dhcp relay security statistics**
- View** Any view
- Parameters** None
- Description** Use the **display dhcp relay security statistics** command to display statistics information about bindings of DHCP relay agents.
- Examples** # Display statistics about client address binding entries.

```
<Sysname> display dhcp relay security statistics
Static Items :1
Dynamic Items :0
Temporary Items :0
All Items :1
```

**Table 214** Description on fields of the display dhcp relay security statistics command

Field	Description
Static Items	Static client address binding items

**Table 214** Description on fields of the display dhcp relay security statistics command

Field	Description
Dynamic Items	Dynamic client address binding items
Temporary Items	Temporary client address binding items
All Items	All client address binding items

---

## display dhcp relay security tracker

**Syntax** **display dhcp relay security tracker**

**View** Any view

**Parameters** None

**Description** Use the **display dhcp relay security tracker** command to display the interval for refreshing dynamic bindings on the relay agent.

**Examples** # Display the interval for refreshing dynamic bindings on the relay agent.

```
<Sysname> display dhcp relay security tracker
Current tracker interval: 10s (Specified by user)
```

The interval is 10 seconds.

---

## display dhcp relay server-group

**Syntax** **display dhcp relay server-group** { *group-id* | **all** }

**View** Any view

**Parameters** *group-id*: Displays the information of the specified DHCP server group numbered from 0 to 19.

**all**: Displays the information of all DHCP server groups.

**Description** Use the **display dhcp relay server-group** command to display the configuration information of a specified or all DHCP server groups.

**Examples** # Display IP addresses of DHCP servers in DHCP server group 1.

```
<Sysname> display dhcp relay server-group 1
No. Group IP
1 1.1.1.1
2 1.1.1.2
```

**Table 215** Description on fields of the display dhcp relay server-group command

Field	Description
No.	Sequence number

**Table 215** Description on fields of the display dhcp relay server-group command

Field	Description
Group IP	IP address in the server group

---

## display dhcp relay statistics

**Syntax** `display dhcp relay statistics [ server-group { group-id | all } ]`

**View** Any view

**Parameters** *group-id*: Specifies a server group number in the range of 0 to 19 about which to display DHCP packet statistics.

**all**: Specifies all server groups about which to display DHCP packet statistics. Information for each group will be displayed.

**Description** Use the **display dhcp relay statistics** command to display DHCP packet statistics related to a specified or all DHCP server groups.

Note that if no parameter (**server-group** and **all**) is specified, all DHCP packet statistics on the relay agent will be displayed.

**Examples** # Display all DHCP packet statistics on the relay agent.

```
<Sysname> display dhcp relay statistics
Bad packets received: 0
DHCP packets received from clients: 0
 DHCPDISCOVER packets received: 0
 DHCPREQUEST packets received: 0
 DHCPINFORM packets received: 0
 DHCPRELEASE packets received: 0
 DHCPDECLINE packets received: 0
 BOOTPREREQUEST packets received: 0
DHCP packets received from servers: 0
 DHCPOFFER packets received: 0
 DHCPACK packets received: 0
 DHCPNAK packets received: 0
 BOOTPREPLY packets received: 0
DHCP packets relayed to servers: 0
 DHCPDISCOVER packets relayed: 0
 DHCPREQUEST packets relayed: 0
 DHCPINFORM packets relayed: 0
 DHCPRELEASE packets relayed: 0
 DHCPDECLINE packets relayed: 0
 BOOTPREREQUEST packets relayed: 0
DHCP packets relayed to clients: 0
 DHCPOFFER packets relayed: 0
 DHCPACK packets relayed: 0
 DHCPNAK packets relayed: 0
 BOOTPREPLY packets relayed: 0
DHCP packets sent to servers: 0
 DHCPDISCOVER packets sent: 0
 DHCPREQUEST packets sent: 0
```

```

DHCPINFORM packets sent: 0
DHCPRELEASE packets sent: 0
DHCPDECLINE packets sent: 0
BOOTPREREQUEST packets sent: 0
DHCP packets sent to clients: 0
DHCPOFFER packets sent: 0
DHCPACK packets sent: 0
DHCPNAK packets sent: 0
BOOTPREPLY packets sent: 0

```

# Display DHCP packet statistics related to every server group on the relay agent.

```

<Sysname> display dhcp relay statistics server-group all
DHCP relay server-group #0
 Packet type Packet number
Client -> Server:
 DHCPDISCOVER 0
 DHCPREQUEST 0
 DHCPINFORM 0
 DHCPRELEASE 0
 DHCPDECLINE 0
 BOOTPREREQUEST 0
Server -> Client:
 DHCPOFFER 0
 DHCPACK 0
 DHCPNAK 0
 BOOTPREPLY 0

```

---

## reset dhcp relay statistics

**Syntax** `reset dhcp relay statistics [ server-group group-id ]`

**View** User view

**Parameters** `server-group group-id`: Specifies a server group ID in the range of 0 to 19 about which to remove statistics from the relay agent.

**Description** Use the **reset dhcp relay statistics** command to remove statistics from the relay agent.

If no **server-group** is specified, all statistics will be removed from the relay agent.

**Related commands:** `display dhcp relay statistics.`

**Examples** # Remove all statistics from the DHCP relay agent.

```
<Sysname> reset dhcp relay statistics
```



# 59

## DHCP CLIENT CONFIGURATION COMMANDS



- The DHCP client configuration is supported only on VLAN interfaces.
- When multiple VLAN interfaces having the same MAC address use DHCP for IP address acquisition via a relay agent, the DHCP server cannot be the Windows 2000 Server or Windows 2003 Server.
- You are not recommended to enable both the DHCP client and the DHCP Snooping on the same device. Otherwise, DHCP Snooping entries may fail to be generated, or the DHCP client may fail to obtain an IP address.

---

### display dhcp client

**Syntax** `display dhcp client [ verbose ] [ interface interface-type interface-number ]`

**View** Any view

**Parameters** **verbose**: Specifies verbose DHCP client information to be displayed.

**interface interface-type interface-number**: Specifies an interface of which to display DHCP client information.

**Description** Use the **display dhcp client** command to display DHCP client information. If no **interface interface-type interface-number** is specified, DHCP client information of all interfaces will be displayed.

**Examples** # Display DHCP client information of all interfaces.

```
<Sysname> display dhcp client
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

# Display verbose DHCP client information.

```
<Sysname> display dhcp client verbose
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from 2005.08.13 15:37:59 to 2005.08.16 15:37:59
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 DNS server: 44.1.1.11
```

```

DNS server: 44.1.1.12
Domain name: ddd.com
Boot server: 200.200.200.200 1.1.1.1
Client ID: 3030-3066-2e65-3234-
392e-3830-3438-2d56-
6c61-6e2d-696e-7465-
7266-6163-6531
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.

```

**Table 216** Description on fields of the display dhcp client command

Field	Description
Vlan-interface1 DHCP client information	Information of the interface acting as the DHCP client
Current machine state	DHCP client current machine state
Allocated IP	The IP address allocated by the DHCP server
Allocated lease	The allocated lease time
T1	The 1/2 lease time (in seconds) of the DHCP client IP address
T2	The 7/8 lease time (in seconds) of the DHCP client IP address
Lease from....to....	The start and end time of the lease.
DHCP Server	DHCP server IP address that assigned the IP address
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	The gateway address assigned to the client
DNS server	The DNS server address assigned to the client
Domain name	The domain name suffix assigned to the client
Boot server	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
Client ID	Client ID
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

---

## ip address dhcp-alloc

**Syntax** **ip address dhcp-alloc** [ **client-identifier mac** *interface-type interface-number* ]

**undo ip address dhcp-alloc**

**View** Interface view

**Parameters** **client-identifier mac** *interface-type interface-number*: Specifies the MAC address of an interface using which as the client ID to obtain an IP address.

**Description** Use the **ip address dhcp-alloc** command to configure an interface to use DHCP for IP address acquisition.

Use the **undo ip address dhcp-alloc** command to cancel an interface from using DHCP.

By default, an interface does not use DHCP for IP address acquisition.

Note that:

- If no parameter is specified, the client uses a character string comprised of the current interface name and MAC address as its ID for address acquisition.
- The DHCP client sends a DHCP-RELEASE message for releasing the IP address obtained via DHCP, if the interface of the client is down, the message cannot be sent.

**Examples** # Configure VLAN-interface 1 to use DHCP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address dhcp-alloc
```



# 60

## DHCP SNOOPING CONFIGURATION COMMANDS



- *DHCP Snooping supports no link aggregation. If an Ethernet port is added into an aggregation group, DHCP Snooping configuration on it will not take effect. When the port is removed from the group, DHCP Snooping can take effect.*
- *The DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server, and it can work when it is between the DHCP client and relay agent or between the DHCP client and server.*
- *The DHCP Snooping enabled device cannot be a DHCP server or DHCP relay agent.*
- *You are not recommended to enable the DHCP client and DHCP Snooping on the same device. Otherwise, DHCP Snooping entries may fail to be generated, or the DHCP client may fail to obtain an IP address.*

---

### dhcp-snooping

**Syntax** `dhcp-snooping`

`undo dhcp-snooping`

**View** System view

**Parameters** None

**Description** Use the **dhcp-snooping** command to enable DHCP snooping.

Use the **undo dhcp-snooping** command to disable DHCP snooping.

With DHCP snooping disabled, all ports can forward responses from any DHCP servers and does not record binding information about MAC addresses of DHCP clients and the obtained IP addresses.

By default, DHCP snooping is disabled.

**Related commands:** `display dhcp-snooping`.

**Examples** # Enable DHCP snooping.

```
[Sysname] dhcp-snooping
```

---

## dhcp-snooping information enable

<b>Syntax</b>	<b>dhcp-snooping information enable</b> <b>undo dhcp-snooping information enable</b>
<b>View</b>	Ethernet port view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>dhcp-snooping information enable</b> command to configure DHCP Snooping to support Option 82.  Use the <b>undo dhcp-snooping information enable</b> command to disable this function.  By default, DHCP Snooping does not support Option 82.
<b>Examples</b>	# Configure DHCP Snooping to support Option 82. <pre>&lt;Sysname&gt; system-view [Sysname] interface gigabitethernet2/0/1 [Sysname-GigabitEthernet2/0/1] dhcp-snooping information enable</pre>

---

## dhcp-snooping information format

<b>Syntax</b>	<b>dhcp-snooping information format</b> { <b>normal</b>   <b>verbose</b> [ <b>node-identifier</b> { <b>mac</b>   <b>sysname</b>   <b>user-defined</b> <i>node-identifier</i> } ] }  <b>undo dhcp-snooping information format</b> [ <b>verbose</b> <b>node-identifier</b> ]
<b>View</b>	Ethernet port view
<b>Parameters</b>	<b>normal</b> : Specifies the normal padding format.  <b>verbose</b> : Specifies the verbose padding format.  <b>node-identifier</b> { <b>mac</b>   <b>sysname</b>   <b>user-defined</b> <i>node-identifier</i> }: Specifies access node identifier. By default, the node MAC address is used as the node identifier.  <ul style="list-style-type: none"> <li>■ <b>mac</b> indicates using MAC address as the node identifier.</li> <li>■ <b>sysname</b> indicates using the device name of a node as the node identifier.</li> <li>■ <b>user-defined</b> <i>node-identifier</i> indicates using a specified character string as the node identifier, in which <i>node-identifier</i> is a string with 1 to 50 characters.</li> </ul>
<b>Description</b>	Use the <b>dhcp-snooping information format</b> command to specify the padding format for Option 82.

Use the **undo dhcp-snooping information format command** to restore the default padding format.

By default, the padding format for Option 82 is **normal**.

Note that when you use the **undo dhcp-snooping information format** command, if the **verbose node-identifier** argument is not specified, the padding format will be restored to **normal**; if the **verbose node-identifier** argument is specified, the padding format will be restored to **verbose** with MAC address as the node identifier.

**Examples** # Specify the padding format as **verbose** for Option 82.

```
<Sysname> system-view
[Sysname] interface gigabitethernet2/0/1
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information strategy replace
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information format verbose
```

---

## dhcp-snooping information strategy

**Syntax** **dhcp-snooping information strategy { drop | keep | replace }**  
**undo dhcp-snooping information strategy**

**View** Ethernet port view

**Parameters** **drop**: Drops the requesting message containing Option 82.

**keep**: Forwards the requesting message containing Option 82 without changing Option 82.

**replace**: Forwards the requesting message containing Option 82 after replacing the original Option 82 with the one padded in specified format.

**Description** Use the **dhcp-snooping information strategy** command to configure the handling strategy for Option 82 in requesting messages.

Use the **undo dhcp-snooping information strategy command** to restore the default setting.

By default, the handling strategy for Option 82 in requesting messages is **replace**.

**Examples** # Configure the handling strategy for Option 82 in requesting messages as **keep**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet2/0/1
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information strategy keep
```

---

## dhcp-snooping trust

**Syntax** **dhcp-snooping trust** [ **no-user-binding** ]

**undo dhcp-snooping trust**

**View** Ethernet port view

**Parameters** **no-user-binding**: Specifies the port not to record the clients' IP-to-MAC bindings in DHCP requests it receives. The command without this keyword allows the port to record the IP-to-MAC bindings of clients.

**Description** Use the **dhcp-snooping trust** command to set a port as trusted.  
Use the **undo dhcp-snooping trust** command to restore the default state of a port.

All ports are untrusted by default.

**Related commands:** **display dhcp-snooping trust**.

**Examples** # Specify GigabitEthernet 2/0/1 as a trusted port and allow it to record the IP-to-MAC bindings of clients.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] dhcp-snooping trust
```

---

## display dhcp-snooping

**Syntax** **display dhcp-snooping**

**View** Any view

**Parameters** None

**Description** Use the **display dhcp-snooping** command to display the binding information recorded through DHCP snooping.

**Related commands:** **dhcp-snooping**.



*Using the **display dhcp-snooping** command displays IP-to-MAC bindings that are present both in the DHCP-ACK and DHCP-REQUEST messages.*

**Examples** # Display DHCP snooping address binding information.

```
<Sysname> display dhcp-snooping
DHCP Snooping is enabled.
The client binding table for all untrusted ports.
Type : D--Dynamic , S--Static
```



```

Type IP Address MAC Address Lease VLAN Interface
==== ===== =====
D 10.1.1.1 000f-e200-0006 286 1 GigabitEthernet2/0/1
--- 1 dhcp-snooping item(s) found ---

```

**Table 217** Description on fields of the display dhcp snooping command

Field	Description
Type	Binding type
IP Address	IP address assigned to the DHCP client
MAC Address	MAC address of the DHCP client
Lease	Lease period of the IP address in seconds
VLAN	VLAN where the port connecting the DHCP client resides
Interface	Port to which the DHCP client is connected

## display dhcp-snooping trust

**Syntax** `display dhcp-snooping trust`

**View** Any view

**Parameters** None

**Description** Use the **display dhcp-snooping trust** command to display information about trusted ports.

**Related commands:** `dhcp-snooping trust`.

**Examples** # Display information about trusted ports.

```

<Sysname> display dhcp-snooping trust
DHCP Snooping is enabled.
DHCP Snooping trust becomes active.
Interface Trusted
===== =====
GigabitEthernet2/0/1 Trusted

```

The above output shows that DHCP snooping is enabled, DHCP snooping trust is active, and port GigabitEthernet 2/0/1 is trusted

## reset dhcp-snooping

**Syntax** `reset dhcp-snooping { all | ip ip-address }`

**View** User view

**Parameters** **all**: Clears all DHCP snooping binding information.

**ip ip-address**: Clears the DHCP snooping binding information of the specified IP address.

**Description** Use the **reset dhcp-snooping** command clear DHCP snooping binding information.

For a distributed device, DHCP snooping binding information on all slots will be cleared after you execute this command.

**Examples** # Clear all DHCP binding information.  
<Sysname> reset dhcp-snooping all

# 61

## COMMON ACL CONFIGURATION COMMANDS

---

### display acl resource

**Syntax** `display acl resource [ slot slot-id ]`

**View** Any view

**Parameters** *slot-id*: Number of the slot.

**Description** Use the **display acl resource** command to display the ACL uses on a switch.

Note that:

- Using the command with a specified a slot will display the ACL uses of that slot. Otherwise, the ACL uses of all slots of the device will be displayed.
- If the module specified by the slot number is not in place or not working normally, this command will display nothing.

**Examples** # Display the ACL uses of all slots on the switch.

```
<Sysname> display acl resource
```

```
Interface:
 Eth2/0/1 to Eth2/0/24
```

Type	Total	Reserved	Configured	Remaining
IFP ACL	1024	0	50	974
IFP Meter	512	0	44	468
IFP Counter	512	0	0	512

```
Interface:
 Eth2/0/25 to Eth2/0/48
```

Type	Total	Reserved	Configured	Remaining
IFP ACL	1024	0	46	978
IFP Meter	512	0	44	468
IFP Counter	512	0	0	512

```
Interface:
 GE3/0/1 to GE3/0/24
```

Type	Total	Reserved	Configured	Remaining
VFP ACL	1024	0	0	1024
IFP ACL	4096	0	46	4050

```

IFP Meter 2048 0 46 2002
IFP Counter 2048 0 0 2048
EFP ACL 512 0 0 512
EFP Meter 256 0 0 256
EFP Counter 512 0 0 512

```

```

Interface:
 GE3/0/25 to GE3/0/48

```

Type	Total	Reserved	Configured	Remaining
VFP ACL	1024	0	0	1024
IFP ACL	4096	0	46	4050
IFP Meter	2048	0	46	2002
IFP Counter	2048	0	0	2048
EFP ACL	512	0	0	512
EFP Meter	256	0	0	256
EFP Counter	512	0	0	512

**Table 218** Field descriptions of the display acl resource command

Field	Description
Interface	Interface indicated by its type and number
Type	Resource type: <ul style="list-style-type: none"> <li>■ ACL indicates ACL rule resources,</li> <li>■ Meter indicates traffic policing resources,</li> <li>■ Counter indicates traffic statistics resources,</li> <li>■ IFP indicates the count of resources in the inbound direction,</li> <li>■ EFP indicates the count of resources in the outbound direction</li> <li>■ VFP indicates the count of resources that are before Layer 2 forwarding and applied in QinQ.</li> </ul>
Total	Total number of ACLs supported
Reserved	Number of reserved ACLs
Configured	Number of configured ACLs
Remaining	Number of remaining ACLs

## display time-range

**Syntax** `display time-range { time-name | all }`

**View** Any view

**Parameters** *time-name*: Time range name comprising 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

**all**: All existing time ranges.

**Description** Use the **display time-range** command to display the configuration and state of a specified or all time ranges.

A time range is active if the system time falls into its range, and if otherwise, inactive.

**Examples** # Display the configuration and state of time range trname.

```
<Sysname> display time-range trname
Current time is 22:20:18 1/5/2006 Thursday
```

```
Time-range : trname (Inactive)
 from 15:00 1/28/2006 to 15:00 1/28/2008
```

**Table 219** Field descriptions of the display time-range command

Field	Description
Current time	Current system time
Time-range	The configuration and state of time range, such as time range name, its activated state, and start time and ending time.

---

## time-range

**Syntax** **time-range** *time-name* { *start-time* **to** *end-time* *days* [ **from** *time1* *date1* ] [ **to** *time2* *date2* ] | **from** *time1* *date1* [ **to** *time2* *date2* ] | **to** *time2* *date2* }

**undo time-range** *time-name* [ *start-time* **to** *end-time* *days* [ **from** *time1* *date1* ] [ **to** *time2* *date2* ] | **from** *time1* *date1* [ **to** *time2* *date2* ] | **to** *time2* *date2* ]

**View** System view

**Parameters** *time-name*: Time range name comprising 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

*start-time*: Start time of a periodic time range, in *hh:mm* format as 24-hour time, where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59.

*end-time*: End time of the periodic time range, in *hh:mm* format as 24-hour time, where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 24:00. The end time must be greater than the start time.

*days*: Indicates on which day or days of the week the periodic time range is valid. You may specify multiple values, in words or in digits, separated by spaces, for this argument, but make sure that they do not overlap. These values can take one of the following forms:

- A digit in the range 0 to 6, respectively for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- Week in words, that is, **Mon, Tue, Wed, Thu, Fri, Sat, or Sun**.
- **working-day** for Monday through Friday.
- **off-day** for Saturday and Sunday.
- **daily** for seven days of a week.

**from** *time1* *date1*: Indicates the start time and date of an absolute time range. The *time1* argument specifies the time of the day in *hh:mm* format as 24-hour time, where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59. The *date1* argument specifies a date in *MMDDIYYYY* or *YYYYIMMIDD* format, where *MM* is the month of the year in the range 1 to 12, *DD* is the day of the

month in the range 1 to 31, and YYYY is the year in the usual Gregorian calendar in the range 1970 to 2100. If not specified, the start time is the earliest time available from the system, namely, 01/01/1970 00:00:00 AM.

**to time2 date2:** Indicates the end time and date of the absolute time range. The format of the *time2* argument is the same as that of the *time1* argument, but its value ranges from 00:00 to 24:00. The end time must be greater than the start time. If not specified, the end time is the maximum time available from the system, namely, 12/31/2100 24:00:00 PM. The format and value range of the *date2* argument are the same as those of the *date1* argument.

**Description** Use the **time-range** command to create a time range.

Use the **undo time-range** command to remove a time range.

A time range can be one of the following:

- Periodic time range created using the **time-range time-name start-time to end-time days** command. A time range thus created recurs periodically on the day or days of the week.
- Absolute time range created using the **time-range time-name { from time1 date1 [ to time2 date2 ] | to time2 date2 }** command. Unlike a periodic time range, a time range thus created does not recur. For example, to create an absolute time range that is active between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test from 00:00 01/01/2004 to 23:59 12/31/2004** command.
- Compound time range created using the **time-range time-name start-time to end-time days { from time1 date1 [ to time2 date2 ] | to time2 date2 }** command. A time range thus created recurs on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test 12:00 to 14:00 wednesday from 00:00 01/01/2004 to 23:59 12/31/2004** command.

Note that:

- You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.
- Up to 256 time ranges can be defined.

**Examples** # Create an absolute time range named test, setting it to become active from 00:00 on January 1, 2008.

```
<Sysname> system-view
[Sysname] time-range test from 0:0 2008/1/1
```

# Create a periodic time range named test, setting it to be active between 14:00 and 18:00 on Saturday and Sunday.

```
<Sysname> system-view
[Sysname] time-range test 14:00 to 18:00 off-day
```

# 62

## IPv4 ACL CONFIGURATION COMMANDS

---

### acl

**Syntax** `acl number acl-number [ name acl-name ] [ match-order { auto | config } ]`  
`undo acl { all | name acl-name | number acl-number }`

**View** System view

**Parameters** **number**: Defines a numbered access control list (ACL).

*acl-number*: IPv4 ACL number, in the range of 2000 to 4999.

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

**name *acl-name***: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**match-order**: Sets the order in which ACL rules are matched.

- **auto**: Performs depth-first match.
- **config**: Performs matching against rules in the order in which they are configured.

**all**: All IPv4 ACLs.

**Description** Use the **acl** command to enter IPv4 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl** command to remove a specified or all IPv4 ACLs.

By default, the match order is **config**.

Note that:

- You can specify a name for an IPv4 ACL only when you create the ACL. After creating an ACL, you cannot specify a name for it, nor can you change or remove the name of the ACL.

- The name of an IPv4 ACL must be unique among IPv4 ACLs. However, an IPv4 ACL and an IPv6 ACL can share the same name.
- If you specify both an ACL number and an ACL name in one command to enter the view of an existing ACL, be sure that the ACL number and ACL name identify the same ACL.
- You can also use this command to modify the match order of an existing ACL but only when it is empty.

**Examples** # Create IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

# Create IPv4 ACL 2002, giving the ACL a name of flow.

```
<Sysname> system-view
[Sysname] acl number 2002 name flow
[Sysname-acl-basic-2002-flow]
```

# Enter the view of an IPv4 ACL that has no name by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

# Enter the view of an IPv4 ACL that has a name by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2002
[Sysname-acl-basic-2002-flow]
```

# Delete the IPv4 ACL with the number of 2000.

```
<Sysname> system-view
[Sysname] undo acl number 2000
```

# Delete the IPv4 ACL named flow.

```
<Sysname> system-view
[Sysname] undo acl name flow
```

---

## acl copy

**Syntax** **acl copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

**View** System view

**Parameters** *source-acl-number*: Number of an existing IPv4 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs



- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

*source-acl-name*: Name of an existing IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

*dest-acl-number*: Number of a non-existent IPv4 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

*dest-acl-name*: Name for the new IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion. The system will automatically assign the new ACL a sequence number which is the smallest one among the available ones in the ACL range for the ACL type.

**Description** Use the **acl copy** command to copy an existent IPv4 ACL (namely, the source IPv4 ACL) to generate a new one (namely, the destination IPv4 ACL). The new ACL is of the same type and has the same match order, match rules, rule numbering step and descriptions.

Note that:

- The source IPv4 ACL and the destination IPv4 ACL must be of the same type.
- The generated ACL does not take the name of the source IPv4 ACL.

**Examples** # Copy basic IPv4 ACL 2008 to generate basic IPv4 ACL 2009.

```
<Sysname> system-view
[Sysname] acl copy 2008 to 2009
```

---

## acl name

**Syntax** **acl name** *acl-name*

**View** System view

**Parameters** *acl-name*: Name of the IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**Description** Use the **acl name** command to enter the view of an existing IPv4 ACL by specifying its name.

**Examples** # Enter the view of the IPv4 ACL named flow.

```

<Sysname> system-view
[Sysname] acl name flow
[Sysname-acl-basic-2002-flow]

```

---

## description

**Syntax** `description text`

**undo description**

**View** Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

**Parameters** *text*: ACL description, a case-sensitive string of 1 to 127 characters.

**Description** Use the **description** command to create an IPv4 ACL description, to describe the purpose of the ACL for example.

Use the **undo description** command to remove the ACL description.

By default, no IPv4 ACL description is present.

**Examples** # Create a description for IPv4 ACL 2000.

```

<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This acl is used in eth 2/0/1

```

# Create a description for IPv4 ACL 3000.

```

<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] description This acl is used in eth 2/0/1

```

# Create a description for ACL 4000.

```

<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] description This acl is used in eth 2/0/1

```

---

## display acl

**Syntax** `display acl { acl-number | all | name acl-name }`

**View** Any view

**Parameters** *acl-number*: IPv4 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

**all:** All IPv4 ACLs.

**name** *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**Description** Use the **display acl** command to display information about the specified or all IPv4 ACLs.

This command displays IPv4 ACL rules in the order in which the system compares a packet against them.

**Examples** # Display information about IPv4 ACL 2001.

```
<Sysname> display acl 2001
Basic ACL 2001, named flow, 1 rule,
ACL's step is 5
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used in eth 2/0/1
```

**Table 220** Field descriptions of the display acl command

Field	Description
Basic ACL 2001	The displayed information is about the basic IPv4 ACL 2001.
named flow	The name of the ACL is flow.
1 rule	The ACL contains one rule.
ACL's step is 5	The rules in this ACL are numbered in steps of 5.
5 times matched	Five matches for the rule. Only ACL matches performed by software are counted. This field appears as long as one match is found.
rule 5 comment This rule is used in eth 2/0/1	The description of ACL rule 5 is "This rule is used in eth 2/0/1."

---

## reset acl counter

**Syntax** **reset acl counter** { *acl-number* | **all** | **name** *acl-name* }

**View** User view

**Parameters** *acl-number*: IPv4 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

**all:** All IPv4 ACLs except for user-defined ACLs.

**name** *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**Description** Use the **reset acl counter** command to clear statistics about a specified or all IPv4 ACLs that are referenced by upper layer software.

**Examples** # Clear statistics about IPv4 ACL 2001, which is referenced by upper layer software.

```
<Sysname> reset acl counter 2001
```

# Clear statistics about the IPv4 ACL named flow, which is referenced by upper layer software.

```
<Sysname> reset acl counter name flow
```

## rule

**Syntax** **rule** [ *rule-id* ] { **deny** | **permit** } [ **fragment** | **logging** | **source** { *sour-addr* | *sour-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* ] \*

**undo rule** *rule-id* [ **fragment** | **logging** | **source** | **time-range** | **vpn-instance** ] \*

**View** Basic IPv4 ACL view

**Parameters** *rule-id*: Basic IPv4 ACL rule number in the range 0 to 65534.

**deny**: Defines a deny statement to drop matched packets.

**permit**: Defines a permit statement to allow matched packets to pass.

**fragment**: Specifies that the rule applies to only IP fragments. Note that a rule defined with the **fragment** keyword matches non-last IP fragments on an SA Series I/O Modules (line processing units) (for example, LSQ13C16915SA) or EA Series I/O Modules (for example, 0231A92P) while matching non-first IP fragments on an SC Series I/O Modules (for example, 0231A931). For detailed information about types of I/O Modules, refer to the installation manual.

**logging**: Specifies to log matched packets.

**source** { *sour-addr* | *sour-wildcard* | **any** }: Specifies a source address. The *sour-addr* | *sour-wildcard* argument specifies a source IP address in dotted decimal notation. Setting the wildcard to a zero indicates a host address. The **any** keyword indicates any source IP address.

**time-range** *time-name*: Specifies the time range in which the rule takes effect. The *time-name* argument specifies a time range name with 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

**vpn-instance** *vpn-instance-name*: Specifies a VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Without this combination, the rule applies to only non-VPN packets.

**Description** Use the **rule** command to create a basic IPv4 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove a basic IPv4 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.
- You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.



*For a basic IPv4 ACL rule to be referenced by a QoS policy for traffic classification, the **logging** and **vpn-instance** keywords are not supported.*

**Examples** # Create a rule to deny packets with the source IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 1.1.1.1 0
```

---

## rule

**Syntax** **rule** [ *rule-id* ] { **deny** | **permit** } **protocol** [ **destination** { *dest-addr* *dest-wildcard* | **any** } | **destination-port** *operator* *port1* [ *port2* ] | **dscp** *dscp* | **established** | **fragment** | **icmp-type** { *icmp-type* *icmp-code* | *icmp-message* } | **logging** | **precedence** *precedence* | **reflective** | **source** { *sour-addr* *sour-wildcard* | **any** } | **source-port** *operator* *port1* [ *port2* ] | **time-range** *time-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name* ] \*

**undo rule** *rule-id* [ **destination** | **destination-port** | **dscp** | **established** | **fragment** | **icmp-type** | **logging** | **precedence** | **reflective** | **source** | **source-port** | **time-range** | **tos** | **vpn-instance** ] \*

**View** Advanced IPv4 ACL view

**Parameters** *rule-id*: Advanced IPv4 ACL rule number in the range 0 to 65534.

**deny**: Defines a deny statement to drop matched packets.

**permit:** Defines a permit statement to allow matched packets to pass.

*protocol:* Protocol carried by IP. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), **udp** (17).

**Table 221** Parameters for advanced IPv4 ACL rules

Parameters	Function	Description
<b>source</b> { <i>sour-addr</i> <i>sour-wildcard</i>   <b>any</b> }	Specifies a source address.	The <i>sour-addr</i> <i>sour-wildcard</i> argument specifies a source IP address in dotted decimal notation. Setting the wildcard to a zero indicates a host address. The <b>any</b> keyword indicates any source IP address.
<b>destination</b> { <i>dest-addr</i> <i>dest-wildcard</i>   <b>any</b> }	Specifies a destination address.	The <i>dest-addr</i> <i>dest-wildcard</i> argument specifies a destination IP address in dotted decimal notation. Setting the <i>dest-wildcard</i> to a zero indicates a host address. The <b>any</b> keyword indicates any destination IP address.
<b>precedence</b> <i>precedence</i>	Specifies an IP precedence value.	The <i>precedence</i> argument can be a number in the range 0 to 7, or in words, <b>routine</b> (0), <b>priority</b> (1), <b>immediate</b> (2), <b>flash</b> (3), <b>flash-override</b> (4), <b>critical</b> (5), <b>internet</b> (6), or <b>network</b> (7).
<b>tos</b> <i>tos</i>	Specifies a ToS preference.	The <i>tos</i> argument can be a number in the range 0 to 15, or in words, <b>max-reliability</b> (2), <b>max-throughput</b> (4), <b>min-delay</b> (8), <b>min-monetary-cost</b> (1), or <b>normal</b> (0).
<b>dscp</b> <i>dscp</i>	Specifies a DSCP priority.	The <i>dscp</i> argument can be a number in the range 0 to 63, or in words, <b>af11</b> (10), <b>af12</b> (12), <b>af13</b> (14), <b>af21</b> (18), <b>af22</b> (20), <b>af23</b> (22), <b>af31</b> (26), <b>af32</b> (28), <b>af33</b> (30), <b>af41</b> (34), <b>af42</b> (36), <b>af43</b> (38), <b>cs1</b> (8), <b>cs2</b> (16), <b>cs3</b> (24), <b>cs4</b> (32), <b>cs5</b> (40), <b>cs6</b> (48), <b>cs7</b> (56), <b>default</b> (0), or <b>ef</b> (46).
<b>logging</b>	Specifies to log matched packets.	--
<b>reflective</b>	Specifies the rule to be reflective.	A rule with the <b>reflective</b> keyword can be defined only for TCP, UDP, or ICMP packets and its statement can only be <b>permit</b> .
<b>fragment</b>	Specifies that the rule applies to only IP fragments.	A rule defined with the <b>fragment</b> keyword matches non-last IP fragments on an SA Series I/O Modules (for example, LSQ13C16915SA) or EA Series I/O Modules (for example, 0231A92P) while matching non-first IP fragments on an SC Series I/O Modules (for example, 0231A931).
<b>time-range</b> <i>time-name</i>	Specifies the time range in which the rule can take effect.	The <i>time-name</i> argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.
<b>vpn-instance</b> <i>vpn-instance-name</i>	Specifies a VPN instance.	The <i>vpn-instance-name</i> argument is a case-sensitive string of 1 to 31 characters. Without this combination, the rule applies to only non-VPN packets.

If the *protocol* argument is set to **tcp** or **udp**, you may define the parameters in the following table.

**Table 222** TCP/UDP-specific parameters for advanced IPv4 ACL rules

Parameters	Function	Description
<b>source-port</b> <i>operator port1</i> [ <i>port2</i> ]	Defines a UDP or TCP source port against which UDP or TCP packets are matched.	The <i>operator</i> argument can be <b>lt</b> (lower than), <b>gt</b> (greater than), <b>eq</b> (equal to), <b>neq</b> (not equal to), and <b>range</b> (inclusive range).  <i>port1, port2</i> : TCP or UDP port number, represented by a number in the range 0 to 65535. TCP port number can be represented in words as follows:  <b>chargen</b> (19), <b>bgp</b> (179), <b>cmd</b> (514), <b>daytime</b> (13), <b>discard</b> (9), <b>domain</b> (53), <b>echo</b> (7), <b>exec</b> (512), <b>finger</b> (79), <b>ftp</b> (21), <b>ftp-data</b> (20), <b>gopher</b> (70), <b>hostname</b> (101), <b>irc</b> (194), <b>klogin</b> (543), <b>kshell</b> (544), <b>login</b> (513), <b>lpd</b> (515), <b>nntp</b> (119), <b>pop2</b> (109), <b>pop3</b> (110), <b>smtp</b> (25), <b>sunrpc</b> (111), <b>tacacs</b> (49), <b>talk</b> (517), <b>telnet</b> (23), <b>time</b> (37), <b>uucp</b> (540), <b>whois</b> (43), or <b>www</b> (80).  UDP port number can be represented in words as follows: <b>biff</b> (512), <b>bootpc</b> (68), <b>bootps</b> (67), <b>discard</b> (9), <b>dns</b> (53), <b>dnsix</b> (90), <b>echo</b> (7), <b>mobilip-ag</b> (434), <b>mobilip-mn</b> (435), <b>nameserver</b> (42), <b>netbios-dgm</b> (138), <b>netbios-ns</b> (137), <b>netbios-ssn</b> (139), <b>ntp</b> (123), <b>rip</b> (520), <b>snmp</b> (161), <b>snmptrap</b> (162), <b>sunrpc</b> (111), <b>syslog</b> (514), <b>tacacs-ds</b> (65), <b>talk</b> (517), <b>tftp</b> (69), <b>time</b> (37), <b>who</b> (513), <b>xmcp</b> (177).  With the <b>range</b> operator, the value of <i>port2</i> does not need to be greater than that of <i>port1</i> because the switch can automatically judge the value range. If the two values are the same, the switch will convert the operator <b>range</b> to <b>eq</b> .  Note that if you specify a combination of <b>lt</b> 1 or <b>gt</b> 65534, the switch will convert it to <b>eq</b> 0 or <b>eq</b> 65535.
<b>destination-port</b> <i>operator port1</i> [ <i>port2</i> ]	Defines a UDP or TCP destination port against which UDP or TCP packets are matched.	
<b>established</b>	Defines the rule for TCP connection packets.	A rule defined with this keyword matches TCP connection packets with the ack flag set.

If the *protocol* argument is set to **icmp**, you may define the parameters in the following table.

**Table 223** Parameters for advanced IPv4 ACL rules

Parameters	Function	Description
<b>icmp-type</b> { <i>icmp-type</i> <i>icmp-code</i>   <i>icmp-message</i> }	Specifies the ICMP message type and code.	The <i>icmp-type</i> argument ranges from 0 to 255.  The <i>icmp-code</i> argument ranges from 0 to 255.  The <i>icmp-message</i> argument specifies a message name. For available ICMP messages, see Table 224.

The following table provides the ICMP messages that you can specify in advanced IPv4 ACL rules.

**Table 224** ICMP messages and their codes

ICMP message	Type	Code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

**Description** Use the **rule** command to define or modify an advanced IPv4 ACL rule. If the rule does not exist, it is created first.

Use the **undo rule** command to remove an advanced IPv4 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30.
- You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first order rather than by rule number.





For an advanced IPv4 ACL to be referenced by a QoS policy for traffic classification

- The **logging**, **vpn-instance** and **reflective** keywords are not supported.
- The operator cannot be **neq** if the ACL is for the inbound traffic.
- The operator cannot be **gt**, **lt**, **neq**, or **range** if the ACL is for the outbound traffic.

**Examples** # Define a rule to permit the TCP packets to pass with the destination port 80 sent from 129.9.0.0 to 202.38.160.0.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80
```

---

## rule

**Syntax** **rule** [ *rule-id* ] { **deny** | **permit** } [ **cos** *vlan-pri* | **dest-mac** *dest-addr dest-mask* | **lsap** *lsap-code lsap-wildcard* | **source-mac** *sour-addr source-mask* | **time-range** *time-name* | **type** *type-code type-wildcard* ] \*

**undo rule** *rule-id*

**View** Ethernet frame header ACL view

**Parameters** *rule-id*: Ethernet frame header ACL rule number in the range 0 to 65534.

**deny**: Defines a deny statement to drop matched packets.

**permit**: Defines a permit statement to allow matched packets to pass.

**cos** *vlan-pri*: Defines an 802.1p priority. The *vlan-pri* argument takes a value in the range 0 to 7; or its equivalent in words, **best-effort**, **background**, **spare**, **excellent-effort**, **controlled-load**, **video**, **voice**, or **network-management**.

**dest-mac** *dest-addr dest-mask*: Specifies a destination MAC address range. The *dest-addr* and *dest-mask* arguments indicate a destination MAC address and mask in xxxx-xxxx-xxxx format.

**lsap** *lsap-code lsap-wildcard*: Defines the DSAP and SSAP fields in the LLC encapsulation. The *lsap-code* argument is a 16-bit hexadecimal number indicating frame encapsulation. The *lsap-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard of the LSAP code.

**source-mac** *sour-addr source-mask*: Specifies a source MAC address range. The *sour-addr* and *sour-mask* arguments indicate a source MAC address and mask in xxxx-xxxx-xxxx format.

**time-range** *time-name*: Specifies the time range in which the rule can take effect. The *time-name* argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

**type** *type-code type-wildcard*: Defines a link layer protocol. The *type-code* argument is a 16-bit hexadecimal number indicating frame type. It is

corresponding to the type-code field in Ethernet\_II and Ethernet\_SNAP frames. The *type-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard.

**Description** Use the **rule** command to create an Ethernet frame header ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an Ethernet frame header ACL rule.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs, starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30.
- You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first order rather than by rule number.



*For an Ethernet frame header ACL to be referenced by a QoS policy for traffic classification, the **lsap** keyword is not supported.*

**Examples** # Create a rule to deny packets with the 802.1p priority of 3.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny cos 3
```

---

## rule comment

**Syntax** **rule** *rule-id* **comment** *text*

**undo rule** *rule-id* **comment**

**View** Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

**Parameters** *rule-id*: IPv4 ACL rule number in the range 0 to 65534.

*text*: IPv4 ACL rule description, a case-sensitive string of 1 to 127 characters.

**Description** Use the **rule comment** command to create a rule description for an existing ACL rule or modify the rule description of an ACL rule to, for example, describe the purpose of the ACL rule or the parameters it contains.

Use the **undo rule comment** command to remove the ACL rule description.

By default, no rule description is created.

**Examples** # Create a rule in ACL 2000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used in eth 2/0/1
```

# Create a rule in ACL 3000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 permit ip source 1.1.1.1 0
[Sysname-acl-adv-3000] rule 0 comment This rule is used in eth 2/0/1
```

# Create a rule in ACL 4000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule 0 deny cos 3
[Sysname-acl-ethernetframe-4000] rule 0 comment This rule is used in eth 2/0/1
```

## step

**Syntax** **step** *step-value*

**undo step**

**View** Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

**Parameters** *step-value*: IPv4 ACL rule numbering step, in the range 1 to 20.

**Description** Use the **step** command to set a rule numbering step.

Use the **undo step** command to restore the default.

By default, rule numbering step is five.

**Examples** # Set the rule numbering step to 2 for ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] step 2
```

# Set the rule numbering step to 2 for ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] step 2
```

# Set the rule numbering step to 2 for ACL 4000.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] step 2
```



# 63

## IPv6 ACL CONFIGURATION COMMANDS

---

### acl ipv6

**Syntax** `acl ipv6 number acl6-number [ name acl6-name ] [ match-order { auto | config } ]`

`undo acl ipv6 { all | name acl6-name | number acl6-number }`

**View** System view

**Parameters** **number**: Defines a numbered IPv6 ACL.

*acl6-number*: IPv6 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

**name acl6-name**: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**match-order**: Sets the order in which ACL rules are matched.

- **auto**: Performs depth-first match. For how depth-first match works, refer to the "IPv6 ACL Match Order" section in accompanied *ACL Configuration*.
- **config**: Performs matching against rules in the order in which they are configured.

**all**: All IPv6 ACLs.

**Description** Use the **acl ipv6** command to enter IPv6 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl ipv6** command to remove a specified or all IPv6 ACLs.

By default, the match order is **config**.

Note that:

- The match order setting is not available for simple IPv6 ACLs, because a simple IPv6 ACL can contain only one rule.

- You can specify a name for an IPv6 ACL only when you create the ACL. After creating an ACL, you cannot specify a name for it, nor can you change or remove the name of the ACL.
- The name of an IPv6 ACL must be unique among IPv6 ACLs. However, an IPv4 ACL and an IPv6 ACL can share the same name.
- If you specify both an ACL number and an ACL name in one command to enter the view of an existing ACL, be sure that the ACL number and ACL name identify the same ACL.
- You can also use this command to modify the match order of an existing IPv6 ACL but only when it is empty.

**Examples** # Create IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

# Create IPv6 ACL 2002, giving the ACL a name of flow.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2002 name flow
[Sysname-acl6-basic-2002-flow]
```

# Enter the view of an IPv6 ACL that has no name by specifying its number.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

# Enter the view of an IPv6 ACL that has a name by specifying its number.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2002
[Sysname-acl6-basic-2002-flow]
```

# Delete the IPv6 ACL with the number of 2000.

```
<Sysname> system-view
[Sysname] undo acl ipv6 number 2000
```

# Delete the IPv6 ACL named flow.

```
<Sysname> system-view
[Sysname] undo acl ipv6 name flow
```

---

## acl ipv6 copy

**Syntax** **acl ipv6 copy** { *source-acl6-number* | **name** *source-acl6-name* } **to** { *dest-acl6-number* | **name** *dest-acl6-name* }

**View** **System view**

<b>Parameters</b>	<p><i>source-acl6-number</i>: Number of an existing IPv6 ACL, which must be in the following ranges:</p> <ul style="list-style-type: none"> <li>■ 2000 to 2999 for basic IPv6 ACLs</li> <li>■ 3000 to 3999 for advanced IPv6 ACLs</li> </ul> <p><i>source-acl6-name</i>: Name of an existing IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.</p> <p><i>dest-acl6-number</i>: Number of a non-existent IPv6 ACL, which must be in the following ranges:</p> <ul style="list-style-type: none"> <li>■ 2000 to 2999 for basic IPv6 ACLs</li> <li>■ 3000 to 3999 for advanced IPv6 ACLs</li> </ul> <p><i>dest-acl6-name</i>: Name for the new IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion. The system will automatically assign the new ACL a sequence number which is the smallest one among the available ones in the ACL range for the ACL type.</p>
<b>Description</b>	<p>Use the <b>acl ipv6 copy</b> command to copy an existent IPv6 ACL (namely, the source IPv6 ACL) to generate a new one (namely, the destination IPv6 ACL), which is of the same type and has the same match order, match rules, rule numbering step and descriptions.</p> <p>Note that:</p> <ul style="list-style-type: none"> <li>■ The source IPv6 ACL and the destination IPv6 ACL must be of the same type.</li> <li>■ The generated IPv6 ACL does not take the name of the source IPv4 ACL.</li> </ul>
<b>Examples</b>	<pre># Copy IPv6 ACL 2008 to generate IPv6 ACL 2009. &lt;Sysname&gt; system-view [Sysname] acl ipv6 copy 2008 to 2009</pre>

---

## acl ipv6 name

<b>Syntax</b>	<b>acl ipv6 name</b> <i>acl6-name</i>
<b>View</b>	System view
<b>Parameters</b>	<i>acl6-name</i> : Name of the IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.
<b>Description</b>	Use the <b>acl ipv6 name</b> command to enter the view of an existing IPv6 ACL by specifying its name.

**Examples** # Enter the view of the IPv6 ACL named flow.

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2002-flow]
```

---

## description

**Syntax** **description** *text*

**undo description**

**View** Basic IPv6 ACL view, advanced IPv6 ACL view

**Parameters** *text*: ACL description, a case-sensitive string of 1 to 127 characters.

**Description** Use the **description** command to create an IPv6 ACL description, to describe the purpose of the ACL for example.

Use the **undo description** command to remove the IPv6 ACL description.

By default, no IPv6 ACL description is present.

**Examples** # Create a description for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This acl is used in eth 0
```

# Create a description for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] description This acl is used in eth 0
```

---

## display acl ipv6

**Syntax** **display acl ipv6** { *acl6-number* | **all** | **name** *acl6-name* }

**View** Any view

**Parameters** *acl6-number*: IPv6 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

**all**: All IPv6 ACLs.

**name** *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.



**Description** Use the **display acl ipv6** command to display information about specified or all IPv6 ACLs.

The output will be displayed in matching order.

**Examples** # Display information about IPv6 ACL 2001.

```
<Sysname> display acl ipv6 2001
Basic IPv6 ACL 2001, named flow, 1 rule,
ACL's step is 5
rule 0 permit source 1::2/128 (5 times matched)
rule 0 comment This rule is used in eth 2/0/1
```

**Table 225** Field descriptions of the display acl ipv6 command

Field	Description
Basic IPv6 ACL 2001	The displayed information is about the basic IPv4 ACL 2001.
named flow	The name of the ACL is flow.
1 rule	The ACL contains one rule.
ACL's step is 5	The rules in this ACL are numbered in steps of 5.
5 times matched	Five matches for the rule. Only ACL matches performed by software are counted. The field appears as long as one match is found.
rule 0 comment This rule is used in eth 2/0/1	The description of ACL rule 5 is "This rule is used in eth 2/0/1."

---

## reset acl ipv6 counter

**Syntax** **reset acl ipv6 counter** { *acl6-number* | **all** | **name** *acl6-name* }

**View** User view

**Parameters** **all**: All basic and advanced IPv6 ACLs.

*acl6-number*: IPv6 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

**name** *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**Description** Use the **reset acl ipv6 counter** command to clear statistics about a specified or all IPv6 ACLs that are referenced by upper layer software.

**Examples** # Clear statistics about IPv6 ACL 2001, which is referenced by upper layer software.

```
<Sysname> reset acl ipv6 counter 2001
```

# Clear statistics about the IPv6 ACL named flow, which is referenced by upper layer software.

```
<Sysname> reset acl ipv6 counter name flow
```

## rule

**Syntax** **rule** [ *rule-id* ] { **deny** | **permit** } [ **fragment** | **logging** | **source** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** } | **time-range** *time-name* ] \*

**undo rule** *rule-id* [ **fragment** | **logging** | **source** | **time-range** ] \*

**View** Basic IPv6 ACL view

**Parameters** *rule-id*: IPv6 ACL rule number in the range 0 to 65534.

**deny**: Defines a deny statement to drop matched packets.

**permit**: Defines a permit statement to allow matched packets to pass.

**fragment**: Specifies that the rule applies to only IP fragments.

**logging**: Specifies to log matched packets.

**source** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** }: Specifies a source address. The *ipv6-address* and *prefix-length* arguments specify a source IPv6 address, and its address prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 source address.

**time-range** *time-name*: Specifies the time range in which the rule takes effect. The *time-name* argument specifies a time range name with 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

**Description** Use the **rule** command to create an IPv6 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an IPv6 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest

rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30.

- You may use the **display acl ipv6** command to verify rules configured in an ACL. If the match order for this IPv6 ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.



For a basic IPv6 ACL to be referenced by a QoS policy for traffic classification, the **logging** and **fragment** keywords are not supported.

**Examples** # Create rules in IPv6 ACL 2000, to permit packets with source address being 2030:5060::9050/64 to pass.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2030:5060::9050/64
```

---

## rule

**Syntax** **rule** [ *rule-id* ] { **deny** | **permit** } *protocol* [ **destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [ *port2* ] | **dscp** *dscp* | **fragment** | **icmpv6-type** { *icmpv6-type icmpv6-code* | *icmpv6-message* } | **logging** | **source** { *source source-prefix* | *source/source-prefix* | **any** } | **source-port** *operator port1* [ *port2* ] | **time-range** *time-name* ] \*

**undo rule** *rule-id* [ **destination** | **destination-port** | **dscp** | **fragment** | **icmpv6-type** | **logging** | **source** | **source-port** | **time-range** ] \*

**View** Advanced IPv6 ACL view

**Parameters** *rule-id*: IPv6 ACL rule number in the range 0 to 65534.

**deny**: Defines a deny statement to drop matched packets.

**permit**: Defines a permit statement to allow matched packets to pass.

*protocol*: Protocol carried on IPv6. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), **udp** (17).

**Table 226** Match criteria and other rule information for advanced IPv6 ACL rules

Parameters	Function	Description
<b>source</b> { <i>source source-prefix</i>   <i>source/source-prefix</i>   <b>any</b> }	Specifies a source IPv6 address.	The <i>source</i> and <i>source-prefix</i> arguments specify an IPv6 source address and its prefix length in the range 1 to 128. The <b>any</b> keyword indicates any IPv6 source address.
<b>destination</b> { <i>dest dest-prefix</i>   <i>dest/dest-prefix</i>   <b>any</b> }	Specifies a destination IPv6 address.	The <i>dest</i> and <i>dest-prefix</i> arguments specify a destination IPv6 address, and its prefix length in the range 1 to 128. The <b>any</b> keyword indicates any IPv6 destination address.

**Table 226** Match criteria and other rule information for advanced IPv6 ACL rules

Parameters	Function	Description
<b>dscp</b> <i>dscp</i>	Specifies a DSCP preference	The <i>dscp</i> argument can be a number in the range 0 to 63, or in words, <b>af11</b> (10), <b>af12</b> (12), <b>af13</b> (14), <b>af21</b> (18), <b>af22</b> (20), <b>af23</b> (22), <b>af31</b> (26), <b>af32</b> (28), <b>af33</b> (30), <b>af41</b> (34), <b>af42</b> (36), <b>af43</b> (38), <b>cs1</b> (8), <b>cs2</b> (16), <b>cs3</b> (24), <b>cs4</b> (32), <b>cs5</b> (40), <b>cs6</b> (48), <b>cs7</b> (56), <b>default</b> (0), or <b>ef</b> (46).
<b>logging</b>	Specifies to log matched packets	--
<b>fragment</b>	Specifies that the rule applies to only IP fragments.	--
<b>time-range</b> <i>time-name</i>	Specifies the time range in which the rule can take effect.	The time-name argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

If the *protocol* argument is set to **tcp** or **udp**, you may define the parameters in the following table.

**Table 227** TCP/UDP-specific match criteria for advanced IPv6 ACL rules

Parameters	Function	Description
<b>source-port</b> <i>operator port1</i> [ <i>port2</i> ]	Defines the source port in the UDP/TCP packet.	The <i>operator</i> argument can be <b>lt</b> (lower than), <b>gt</b> (greater than), <b>eq</b> (equal to), or <b>range</b> (inclusive range).
<b>destination-port</b> <i>operator port1</i> [ <i>port2</i> ]	Defines the destination port in the UDP/TCP packet.	<p>The <i>port1</i> and <i>port2</i> arguments each specify a TCP or UDP port, represented by a number in the range 0 to 65535. TCP port number can be represented in words as follows:</p> <p><b>chargen</b> (19), <b>bgp</b> (179), <b>cmd</b> (514), <b>daytime</b> (13), <b>discard</b> (9), <b>domain</b> (53), <b>echo</b> (7), <b>exec</b> (512), <b>finger</b> (79), <b>ftp</b> (21), <b>ftp-data</b> (20), <b>gopher</b> (70), <b>hostname</b> (101), <b>irc</b> (194), <b>klogin</b> (543), <b>kshell</b> (544), <b>login</b> (513), <b>lpd</b> (515), <b>nntp</b> (119), <b>pop2</b> (109), <b>pop3</b> (110), <b>smtp</b> (25), <b>sunrpc</b> (111), <b>tacacs</b> (49), <b>talk</b> (517), <b>telnet</b> (23), <b>time</b> (37), <b>uucp</b> (540), <b>whois</b> (43), or <b>www</b> (80).</p> <p>UDP port number can be represented in words as follows: <b>biff</b> (512), <b>bootpc</b> (68), <b>bootps</b> (67), <b>discard</b> (9), <b>dns</b> (53), <b>dnsix</b> (90), <b>echo</b> (7), <b>mobilip-ag</b> (434), <b>mobilip-mn</b> (435), <b>nameserver</b> (42), <b>netbios-dgm</b> (138), <b>netbios-ns</b> (137), <b>netbios-ssn</b> (139), <b>ntp</b> (123), <b>rip</b> (520), <b>snmp</b> (161), <b>snmptrap</b> (162), <b>sunrpc</b> (111), <b>syslog</b> (514), <b>tacacs-ds</b> (65), <b>talk</b> (517), <b>tftp</b> (69), <b>time</b> (37), <b>who</b> (513), <b>xdmcp</b> (177).</p> <p>With the <b>range</b> operator, the value of <i>port2</i> does not need to be greater than that of <i>port1</i> because the switch can automatically judge the value range. If the two values are the same, the switch will convert the operator <b>range</b> to <b>eq</b>.</p> <p>Note that if you specify a combination of <b>lt 1</b> or <b>gt 65534</b>, the switch will convert it to <b>eq 0</b> or <b>eq 65535</b>.</p>

If the *protocol* argument is set to ICMPv6, you may define the parameters in the following table.

**Table 228** ICMPv6-specific match criteria for advanced IPv6 ACL rules

Parameters	Function	Description
<b>icmpv6-type</b> { <i>icmpv6-type</i> <i>icmpv6-code</i>   <i>icmpv6-message</i> }	Specifies the ICMPv6 message type and code	The <i>icmpv6-type</i> argument ranges from 0 to 255. The <i>icmpv6-code</i> argument ranges from 0 to 255. The <i>icmpv6-message</i> argument specifies a message name. For available ICMPv6 messages, see Table 229

The following table provides the ICMPv6 messages that you can specify in advanced IPv6 ACL rules.

**Table 229** Available ICMPv6 messages

ICMPv6 message	Type	Code
redirect	137	0
echo-request	128	0
echo-reply	129	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

**Description** Use the **rule** command to create an IPv6 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an IPv6 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs, starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.
- You may use the **display acl ipv6** command to verify rules configured in an IPv6 ACL. If the match order for this IPv6 ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.



*For an advanced IPv6 ACL to be referenced by a QoS policy for traffic classification*

- The **logging** and **fragment** keywords are not supported.
- The operator cannot be **neq** if the ACL is for the inbound traffic.
- The operator cannot be **gt**, **lt**, **neq**, or **range** if the ACL is for the outbound traffic.

**Examples** # Create a rule in IPv6 ACL 3000 to permit the TCP packets with the source address 2030:5060::9050/64 to pass.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::9050/64
```

---

## rule comment

**Syntax** **rule** *rule-id* **comment** *text*

**undo rule** *rule-id* **comment**

**View** Basic IPv6 ACL view, advanced IPv6 ACL view

**Parameters** *rule-id*: IPv6 ACL rule number in the range 0 to 65534.

*text*: IPv6 ACL rule description, a case-sensitive string of 1 to 127 characters.

**Description** Use the **rule comment** command to create a rule description for an existing ACL rule or modify the rule description of an ACL rule to, for example, describe the purpose of the ACL rule or its attributes.

Use the **undo rule comment** command to remove the IPv6 ACL rule description.

By default, no rule description is created.

**Examples** # Define a rule in IPv6 ACL 2000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule 0 comment This rule is used in eth 2/0/1
```

# Define a rule in IPv6 ACL 3000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 0 permit tcp source 2030:5060::9050/64
[Sysname-acl6-adv-3000] rule 0 comment This rule is used in eth 2/0/1
```

---

## step

**Syntax** `step step-value`

**undo step**

**View** Basic IPv6 ACL view, advanced IPv6 ACL view

**Parameters** *step-value*: The step in which the rules in the IPv6 ACL is numbered, in the range 1 to 20.

**Description** Use the **step** command to set a rule numbering step for the IPv6 ACL.

Use the **undo step** command to restore the default.

By default, the rule numbering step is five.

**Examples** # Set the rule numbering step to 2 for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

# Set the rule numbering step to 2 for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] step 2
```





# 64

## BANDWIDTH MANAGEMENT CONFIGURATION COMMANDS

---

### display qos lr interface

**Syntax** **display qos lr interface** [ *interface-type interface-number* ]

**View** Any view

**Parameters** *interface-type*: Port type.  
*interface-number*: Port number.

**Description** Use the **display qos lr interface** command to display the LR configuration information of a certain interface or all interfaces.

If the **interface** argument is not specified, this command will display the LR configuration information of all the interfaces.

**Examples** # Display the LR configuration and statistics information of all the interfaces.

```
<Sysname> display qos lr interface
Interface: Ethernet2/0/10
Direction: Outbound
CIR 64000 (kbps), CBS 4000000 (byte)
```

**Table 230** Field descriptions of the display qos lr command

Field	Description
Interface	Port name, composed of port type and port number
Direction	Specify the direction of limited rate as outbound
CIR	Committed information rate, in kbps
CBS	Committed burst size, in byte

---

### qos lr outbound

**Syntax** **qos lr outbound cir** *committed-information-rate* [ **cbs** *committed-burst-size* ]  
**undo qos lr outbound**

**View** Ethernet interface view, port group view

**Parameters** **outbound**: Limits the rate of the outbound traffic.

**cir** *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The range of CIR varies with port types as follows:

- Fast Ethernet port: 64 to 100000
- GigabitEthernet port: 64 to 1000000
- Ten-GigabitEthernet port: 64 to 10000000

Note that the *committed-information-rate* argument must be a multiple of 64.

**cbs** *committed-burst-size*: Specifies the committed burst size in bytes.

- The *committed-burst-size* argument ranges from 4000 to 16000000.
- If the **cbs** keyword is not used, the system uses the default committed burst size, that is, 500 ms x *committed-information-rate*, or 16000000 if the multiplication is more than 16000000.

**Description** Use the **qos lr outbound** command to limit the rate of outbound traffic via physical interfaces.

Use the **undo qos lr outbound** command to cancel the limit.

**Examples** # Limit the outbound traffic rate on Ethernet 2/0/1 within 640 kbps.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] qos lr outbound cir 640
```

# 65

## QoS TRAFFIC CLASSES CONFIGURATION COMMANDS

---

### display traffic classifier

**Syntax** **display traffic classifier user-defined** [ *classifier-name* ]

**View** Any view

**Parameters** *classifier-name*: Class name.

**Description** Use the **display traffic classifier** command to display the information about a class.

If no class name is provided, this command displays the information about all the user-defined classes.

**Examples** # Display the information about the user-defined classes.

```
<Sysname> display traffic classifier user-defined
 User Defined Classifier Information:
 Classifier: p
 Operator: AND
 Rule(s) : If-match acl 2001
```

**Table 231** Field descriptions of the display traffic classifier user-defined command

Field	Description
User Defined Classifier Information	The information about the user-defined classes is displayed.
Classifier	Class name and its contents, which could be of multiple types
Operator	Logical relationship among the classification rules
Rule	Classification rules

---

### if-match

**Syntax** **if-match** *match-criteria*

**undo if-match** *match-criteria*

**View** Class view

**Parameters** *match-criteria*: Matching rule to be defined. Table 232 describes the available forms of this argument.

**Table 232** The forms of the match-criteria argument

Field	Description
<b>acl</b> <i>access-list-number</i>	Specifies an ACL to match packets. The <i>access-list-number</i> argument is in the range 2000 to 4999.  In a class configured with the operator <b>and</b> , the logical relationship between rules defined in the referenced IPv4 ACL is <b>or</b> .
<b>acl ipv6</b> <i>access-list-number</i>	Specifies an IPv6 ACL to match IPv6 packets. The <i>access-list-number</i> argument is in the range 2000 to 3999.  In a class configured with the operator <b>and</b> , the logical relationship between rules defined in the referenced IPv6 ACL is <b>or</b> .
<b>any</b>	Specifies to match all packets.
<b>customer-dot1p</b> <i>8021p-list</i>	Specifies to match packets by 802.1p precedence of the customer network. The <i>8021p-list</i> argument is a list of CoS values. You can provide up to eight space-separated CoS values for this argument. CoS is in the range 0 to 7.
<b>dscp</b> <i>dscp-list</i>	Specifies to match packets by DSCP precedence. The <i>dscp-list</i> argument is a list of DSCP values. You can provide up to eight space-separated DSCP values for this argument. DSCP is in the range 0 to 63.
<b>destination-mac</b> <i>mac-address</i>	Specifies to match the packets with a specified destination MAC address.
<b>ip-precedence</b> <i>ip-precedence-list</i>	Specifies to match packets by IP precedence. The <i>ip-precedence-list</i> argument is a list of IP precedence values. You can provide up to eight space-separated IP precedence values for this argument. IP precedence is in the range 0 to 7.
<b>protocol</b> <i>protocol-name</i>	Specifies to match the packets of a specified protocol. The <i>protocol-name</i> argument can be IP or IPv6.
<b>service-dot1p</b> <i>8021p-list</i>	Specifies to match packets by 802.1p precedence of the service provider network. The <i>8021p-list</i> argument is a list of CoS values. You can provide up to eight space-separated CoS values for this argument. CoS is in the range 0 to 7.
<b>source-mac</b> <i>mac-address</i>	Specifies to match the packets with a specified source MAC address.
<b>customer-vlan-id</b> <i>vlan-id-list</i>	Specifies to match the packets of specified VLANs of user networks. The <i>vlan-id-list</i> argument specifies a list of VLAN IDs, in the form of <i>vlan-id to vlan-id</i> or multiple discontinuous VLAN IDs (separated by space). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range 1 to 4094.  In a class configured with the operator <b>and</b> , the logical relationship between the customer VLAN IDs specified for the <b>customer-vlan-id</b> keyword is <b>or</b> .
<b>service-vlan-id</b> <i>vlan-id-list</i>	Specifies to match the packets of specified VLANs of the operator's network. The <i>vlan-id-list</i> argument is a list of VLAN IDs, in the form of <i>vlan-id to vlan-id</i> or multiple discontinuous VLAN IDs (separated by space). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range 1 to 4094.  In a class configured with the operator <b>and</b> , the logical relationship between the service VLAN IDs specified for the <b>service-vlan-id</b> keyword is <b>or</b> .

**Description** Use the **if-match** command to define a rule to match a specific type of packets.  
Use the **undo if-match** command to remove a matching rule.



Suppose the logical relationship between classification rules is **and**. Note the following when using the **if-match** command to define matching rules.

- If multiple matching rules with the **acl** or **acl ipv6** keyword specified are defined in a class, the actual logical relationship between these rules is **or** when the policy is applied.
- If multiple matching rules with the **customer-vlan-id** or **service-vlan-id** keyword specified are defined in a class, the actual logical relationship between these rules is **or** when the policy is applied.

### Examples

# Define a rule for class1 to match the packets with their destination MAC addresses being 0050-ba27-bed3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

# Define a rule for class2 to match the packets with their source MAC addresses being 0050-ba27-bed2.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

# Define a rule for class1 to match the advanced IPv4 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101
```

# Define a rule for class1 to match the advanced IPv6 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 3101
```

# Define a rule for class1 to match all the packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match any
```

# Define a rule for class1 to match the packets with their DSCP precedence values being 1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match dscp 1
```

# Define a rule for class1 to match the packets with their IP precedence values being 1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ip-precedence 1
```

# Define a rule for class 1 to match IP packets.

```

<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol ip

Define a rule for class 1 to match the packets with the customer network 802.1p
precedence 2.

<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-dot1p 2

Define a rule for class 1 to match the packets with the service provider network
802.1p precedence 5.

<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-dot1p 5

Define a rule for class1 to match the packets of VLAN 1024 of the user
networks.

<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-vlan-id 1024

Define a rule for class1 to match the packets of VLAN 1000 of the operator's
network.

<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-vlan-id 1000

```

---

## traffic classifier

**Syntax** `traffic classifier classifier-name [ operator { and | or } ]`

`undo traffic classifier classifier-name`

**View** System view

**Parameters** **and**: Specifies the relationship among the rules in the class as logic AND. That is, a packet is matched only when it matches all the rules defined for the class.

**or**: Specifies the relationship among the rules in the class as logic OR. That is, a packet is matched if it matches a rule defined for the class.

*classifier-name*: Name of the class to be created.

**Description** Use the **traffic classifier** command to create a class. This command also leads you to class view.

Use the **undo traffic classifier** command to remove a class.

By default, a packet is matched only when it matches all the rules configured for the class.

**Examples** # Create a class named class 1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```





# 66

## TRAFFIC BEHAVIOR CONFIGURATION COMMANDS

---

### accounting

**Syntax** **accounting**

**undo accounting**

**View** Traffic behavior view

**Parameters** None

**Description** Use the **accounting** command to configure the traffic accounting action for a traffic behavior.

Use the **undo accounting** command to remove the traffic accounting action.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**

**Examples** # Configure the traffic accounting action for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting
```

---

### car

**Syntax** **car cir** *committed-information-rate* [ **cbs** *committed-burst-size* [ **ebs** *excess-burst-size* ] ] [ **pir** *peak-information-rate* ] [ **green** *action* ] [ **red** *action* ] [ **yellow** *action* ]

**undo car**

**View** Traffic behavior view

**Parameters** **cir** *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The *committed-information-rate* argument ranges from 64 to 10000000 and must be a multiple of 64.

**cbs** *committed-burst-size*: Specifies the committed burst size (CBS) in bytes. The *committed-burst-size* argument ranges from 4000 to 16000000, the default is 4000.

**ebs** *excess-burst-size*: Specifies excess burst size (EBS) in bytes. The *excess-burst-size* argument ranges from 0 to 16000000, the default is 4000.

**pir** *peak-information-rate*: Specifies the peak information rate (PIR) in kbps. The *peak-information-rate* argument ranges from 64 to 10000000 and must be a multiple of 64.

**green** *action*: Specifies the action to be conducted for the traffic conforming to CIR. The *action* argument can be:

- **discard**: Drops the packets.
- **pass**: Forwards the packets.
- **remark-dscp-pass** *new-dscp*: Marks the packets with a new DSCP precedence and forwards them to their destinations. The *new-dscp* argument is in the range 0 to 63.

By default, packets conforming to CIR are forwarded.

**red** *action*: Specifies the action to be conducted for the traffic conforms to neither CIR nor PIR. The *action* argument can be:

- **discard**: Drops the packets.
- **pass**: Forwards the packets.
- **remark-dscp-pass** *new-dscp*: Marks the packets with a new DSCP precedence and forwards them to their destinations. The *new-dscp* argument is in the range 0 to 63.

By default, packets conforming to neither CIR nor PIR are dropped.

**yellow** *action*: Specifies the action to be conducted for the traffic conforms to PIR but does not conform to CIR. The *action* argument can be:

- **discard**: Drops the packets.
- **pass**: Forwards the packets.
- **remark-dscp-pass** *new-dscp*: Marks the packets with a new DSCP precedence and forwards them to their destinations. The *new-dscp* argument is in the range 0 to 63.

By default, packets conforming to PIR but not conforming to CIR are dropped.

**Description** Use the **car** command to configure TP action for a traffic behavior.

Use the **undo car** command to remove the TP action.

Note that, if you configure the TP action for a traffic behavior for multiple times, only the last configuration takes effect.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**

**Examples** # Configure TP action for a traffic behavior. When the traffic rate is lower than 6400 kbps, packets are forwarded normally. When the traffic rate exceeds 6400 kbps, the packets beyond 6400 kbps are dropped.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 6400 red discard
```

---

## display traffic behavior

**Syntax** **display traffic behavior user-defined** [ *behavior-name* ]

**View** Any view

**Parameters** *behavior-name*: Name of a user defined traffic behavior.

**Description** Use the **display traffic behavior** command to display the information about a user defined traffic behavior.

If no behavior name is provided, this command displays the information about all the user-defined behaviors.

**Examples** # Display the information about all the user defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined
User Defined Behavior Information:
Behavior: test
Marking:
 Remark dot1p COS 4
Committed Access Rate:
 CIR 64 (kbps), CBS 4000 (byte), EBS 4000 (byte), PIR 640 (kbps)
Green Action: pass
Red Action: discard
Yellow Action: pass
```

**Table 233** Field descriptions of the display traffic behavior user-defined command

Field	Description
User Defined Behavior Information	The information about user defined traffic behaviors is displayed
Behavior	Name of a traffic behavior, which can be of multiple types
Marking	Information about priority marking
Committed Access Rate	Information about traffic rate limit
CIR	Committed information rate in bytes
CBS	Committed burst size in bytes
EBS	Excessive burst size in bytes
PIR	Peak information rate in bytes
Green Action	Action conducted to packets conforming to CIR
Red Action	Action conducted for packets conforming to neither CIR nor PIR
Yellow Action	Action conducted to packets conforming to PIR but not conforming to CIR

---

**filter****Syntax** `filter { deny | permit }``undo filter`**View** Traffic behavior view**Parameters** **deny**: Drops packets.**permit**: Forwards packets.**Description** Use the **filter** command to configure traffic filtering action for a traffic behavior.  
Use the **undo filter** command to remove the traffic filtering action.**Related commands:** **qos policy, traffic behavior, classifier behavior.****Examples** # Configure traffic filtering action for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

---

**nest****Syntax** `nest top-most vlan-id vlan-id``undo nest`**View** Traffic behavior view**Parameters** **vlan-id** *vlan-id*: ID of the VLAN. The *vlan-id* argument is in the range 1 to 4094.**Description** Use the **nest** command configure an outer VLAN tag for a traffic behavior.  
Use the **undo nest** command to remove the outer VLAN tag.

Note that the action of creating an outer VLAN tag cannot be configured simultaneously with any other action except the traffic filtering action or the action of setting 802.1p precedence in the same traffic behavior. And the action of creating an outer VLAN tag must be applied to basic QinQ-enabled ports or port groups. Otherwise, the corresponding QoS policy cannot be applied successfully.

**Related commands:** **qos policy, traffic behavior, classifier behavior.****Examples** # Configure an outer VLAN tag for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] nest top-most vlan-id 100
```

---

## redirect

**Syntax** **redirect** { **cpu** | **interface** *interface-type interface-number* | **link-aggregation group** *agg-id* | **next-hop** { *ipv4-add* [ *ipv4-add* ] | *ipv6-add* [ *interface-type interface-number* ] [ *ipv6-add* [ *interface-type interface-number* ] ] } }

**undo redirect**

**View** Traffic behavior view

**Parameters** **cpu**: Redirects traffic to the CPU.

**interface** *interface-type interface-number*: Redirects traffic to an interface identified by its type and number.

**link-aggregation group** *agg-id*: Redirects traffic to a manual aggregation group. The *agg-id* argument is an aggregation group ID. Note that the specified aggregation group must be an existing manual aggregation group.

**next-hop**: Specifies the next hop to redirect the traffic to.

*ipv4-add*: IPv4 address of the next hop.

*ipv6-add*: IPv6 address of the next hop. The *interface-type interface-number* argument is a VLAN interface number. If the IPv6 address is a link-local address, you must specify a VLAN interface for the IPv6 address of the next hop; if the IPv6 address is not a link-local address, you need not specify a VLAN interface for the IPv6 address of the next hop.

**Description** Use the **redirect** command to configure traffic redirecting action for a traffic behavior.

Use the **undo redirect** command to remove the traffic redirecting action.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**

**Examples** # Configure the redirecting action to redirect traffic to Ethernet2/0/1 port.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface Ethernet 2/0/1
```

---

## remark customer-vlan-id

**Syntax** **remark customer-vlan-id** *vlan-id-value*

**undo remark customer-vlan-id**

**View** Traffic behavior view

**Parameters** *vlan-id-value*: VLAN ID to be set for packets, in the range of 1 to 4094.

**Description** Use the **remark customer-vlan-id** command to configure the action of setting the customer network VLAN ID for a traffic behavior.

Use the **undo remark customer-vlan-id** command to remove the action of setting the customer network VLAN ID.

Note that the action of setting the customer network VLAN ID cannot be applied to a VLAN or applied globally.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**

**Examples** # Configure the action of setting the customer network VLAN ID to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark customer-vlan-id 2
```

## remark dot1p

**Syntax** **remark dot1p** *8021p*

**undo remark dot1p**

**View** Traffic behavior view

**Parameters** *8021p*: 802.1p precedence to be set for packets, in the range 0 to 7.

**Description** Use the **remark dot1p** command to configure the action of setting 802.1p precedence for a traffic behavior.

Use the **undo remark dot1p** command to remove the action of setting 802.1p precedence

Note that, when the **remark dot1p** command is used together with the **remark local-precedence** command, the 802.1p precedence to be set for packets must be the same as the local precedence to be set for packets. Otherwise, the corresponding policy cannot be applied successfully.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**

**Examples** # Configure the action to set 802.1p precedence to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

---

**remark drop-precedence**

**Syntax** **remark drop-precedence** *drop-precedence-value*

**undo remark drop-precedence**

**View** Traffic behavior view

**Parameters** *drop-precedence-value*: Drop precedence to be set for packets, in the range 0 to 2.

**Description** Use the **remark drop-precedence** command to configure the action of setting drop precedence for a traffic behavior.

Use the **undo remark drop-precedence** command to remove the action of setting drop precedence.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**

**Examples** # Configure the action to set drop precedence to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark drop-precedence 2
```

---

**remark dscp**

**Syntax** **remark dscp** *dscp-value*

**undo remark dscp**

**View** Traffic behavior view

**Parameters** *dscp-value*: DSCP precedence to be set for packets, in the range of 0 to 63. This argument can also be the keywords listed in Table 234.

**Table 234** DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28

**Table 234** DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

**Description** Use the **remark dscp** command to configure the action of setting DSCP precedence for a traffic behavior.

Use the **undo remark dscp** command to remove the action of setting DSCP precedence.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**

**Examples** # Configure the action to set DSCP precedence to 6 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

---

## remark ip-precedence

**Syntax** **remark ip-precedence** *ip-precedence-value*

**undo remark ip-precedence**

**View** Traffic behavior view

**Parameters** *ip-precedence-value*: IP precedence to be set for packets, in the range of 0 to 7.

**Description** Use the **remark ip-precedence** command to configure the action of setting IP precedence for a traffic behavior.

Use the **undo remark ip-precedence** command to remove the action of setting IP precedence.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**



**Examples** # Configure the action to set IP precedence to 6 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark ip-precedence 6
```

## remark local-precedence

**Syntax** **remark local-precedence** *local-precedence*  
**undo remark local-precedence**

**View** Traffic behavior view

**Parameters** *local-precedence*: Local precedence to be set for packets, in the range of 0 to 7.

**Description** Use the **remark local-precedence** command to configure the action of setting local precedence for a traffic behavior.

Use the **undo remark local-precedence** command to remove the action of remarking local precedence.

Note that, when the **remark dot1p** command is used together with the **remark local-precedence** command, the 802.1p precedence to be set for packets must be the same as the local precedence to be set for packets. Otherwise, the corresponding policy cannot be applied successfully.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**

**Examples** # Configure the action to set local precedence to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

## remark service-vlan-id

**Syntax** **remark service-vlan-id** *vlan-id-value*  
**undo remark service-vlan-id**

**View** Traffic behavior view

**Parameters** *vlan-id-value*: VLAN ID to be set for packets, in the range of 1 to 4094.

**Description** Use the **remark service-vlan-id** command to configure the action of setting the service provider network VLAN ID for a traffic behavior.

Use the **undo remark service-vlan-id** command to remove the action of setting the service provider network VLAN ID.

Note that:

- When the action of setting the service provider network VLAN ID is applied in the inbound direction, any other action except the traffic filtering action or the action of setting 802.1p precedence cannot be configured in the same traffic behavior. Otherwise, the corresponding QoS policy cannot be applied successfully.
- The action of setting the service provider network VLAN ID cannot be applied to a VLAN or applied globally.

**Related commands:** **qos policy, traffic behavior, classifier behavior.**

**Examples** # Configure the action of setting the service provider network VLAN ID to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark service-vlan-id 2
```

## traffic behavior

**Syntax** **traffic behavior** *behavior-name*

**undo traffic behavior** *behavior-name*

**View** System view

**Parameters** *behavior-name*: Name of the traffic behavior to be created.

**Description** Use the **traffic behavior** command to create a traffic behavior. This command also leads you to traffic behavior view.

Use the **undo traffic classifier** command to remove a traffic behavior.

**Related commands:** **qos policy, qos apply policy, classifier behavior.**

**Examples** # Define a traffic behavior named behavior1.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

# 67

## QoS POLICY CONFIGURATION COMMANDS

---

### classifier behavior

**Syntax** `classifier classifier-name behavior behavior-name`

`undo classifier classifier-name`

**View** Policy view

**Parameters** *classifier-name*: Name of an existing class.

*behavior-name*: Name of an existing traffic behavior.

**Description** Use the **classifier behavior** command to associate a traffic behavior with a class.

Use the **undo classifier** command to remove a class from a policy.

Note that each class can be associated with only one traffic behavior.

**Related commands:** **qos policy**.



*In a QoS policy with multiple class-to-traffic-behavior associations, if the action of creating an outer VLAN tag, the action of setting customer network VLAN ID, or the action of setting service provider network VLAN ID is configured in a **traffic behavior**, we recommend you not to configure any other action in this **traffic behavior**. Otherwise, the QoS policy may not function as expected after it is applied.*

**Examples** # Associate the behavior named *test* with the class named *database* in the policy *user1*.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
```

---

### display qos policy

**Syntax** `display qos policy user-defined [ policy-name [ classifier classifier-name ] ]`

**View** Any view

**Parameters** *policy-name*: Policy name. If it is not provided, the configuration of all the user defined policies is displayed.

*classifier-name*: Name of a class in the policy. If it is not provided, all the classes in the policy are specified.

**Description** Use the **display qos policy** command to display the configuration of a specified policy, including the configuration of the classes and the associated traffic behaviors in the policy.

**Examples** # Display the configuration of all the user specified policies.

```
<Sysname> display qos policy user-defined

User Defined QoS Policy Information:

Policy: test
Classifier: test
Behavior: test
Accounting Enable
Committed Access Rate:
 CIR 64 (kbps), CBS 4000 (byte), EBS 4000 (byte), PIR 640 (kbps)
Green Action: pass
Red Action: discard
Yellow Action: pass
```

**Table 235** Field descriptions of the display qos policy command

Field	Description
Policy	Policy name
Classifier	Class name and the corresponding configuration information
Behavior	Traffic behavior name and the corresponding configuration information

## display qos policy global

**Syntax** **display qos policy global** { **inbound** | **outbound** } [ **slot** *slot-id* ]

**View** Any view

**Parameters** **inbound**: Displays the QoS policy applied globally in the inbound direction of all ports.

**outbound**: Displays the QoS policy applied globally in the outbound direction of all ports.

**slot** *slot-number*: Displays the global QoS policy applied on a module. If the *slot-number* argument is not specified, the global QoS policy applied on the main control module are displayed.

**Description** Use the **display qos policy global** command to display information about a global QoS policy.

**Examples** # Display information about the global QoS policy in the inbound direction.

```

<Sysname> display qos policy global inbound

Direction: Inbound

Policy: test
Classifier: test
Operator: AND
Rule(s) : If-match acl 2000
Behavior: test
Accounting Enable:
 0 (Packets)
Committed Access Rate:
 CIR 640 (kbps), CBS 4000 (byte), EBS 4000 (byte)
Green Action: pass
Red Action: discard
Yellow Action: pass
Green : 0(Packets)

```

**Table 236** Field descriptions of the display qos policy global command

Field	Description
Direction	Direction in which the policy is applied globally
Policy	Policy name
Classifier	Class name
Behavior	Traffic behavior name

## display qos policy interface

**Syntax** **display qos policy interface** [ *interface-type interface-number* ] [ **inbound** | **outbound** ]

**View** Any view

**Parameters** *interface-type*: Port type.

*interface-number*: Port number.

**inbound**: Specifies the inbound direction.

**outbound**: Specifies the outbound direction.

**Description** Use the **display qos policy interface** command to display the configuration and statistics information about the policy applied on a port.

If no interface is provided, the configuration and statistics information about the policies applied on all the ports is displayed.

**Examples** # Display the configuration and statistics information about the policy applied on Ethernet2/0/1 port.

```

<Sysname> display qos policy interface Ethernet 2/0/1

Interface: Ethernet2/0/1

```

```

Direction: Inbound

Policy: test
Classifier: test
Operator: AND
Rule(s) : If-match acl 2000
Behavior: test
Marking:
 Remark dot1p COS 4
Committed Access Rate:
 CIR 64 (kbps), CBS 4000 (byte), EBS 4000 (byte), PIR 640 (kbps)
Green Action: pass
Red Action: discard
Yellow Action: pass
Green : 0(Packets)

```

**Table 237** Field descriptions of the display qos policy interface command

Field	Description
Interface	Port name, comprising of port type and port number
Direction	Direction of the port where the policy is applied
Policy	Name of the policy applied to the port
Classifier	Name of the class in the policy and its configuration
Operator	Logical relationship among the classification rules in a class
Rule(s)	Classification rules in the class
Behavior	Name of the behavior in the policy and its configuration

---

## display qos vlan-policy

**Syntax** `display qos vlan-policy { name policy-name | vlan [ vlan-id ] } [ slot slot-id ]`

**View** Any view

**Parameters** **name** *policy-name*: Specifies to display the information about the VLAN policy with the specified name.

**vlan** *vlan-id*: Specifies to display the information about the VLAN policy applied to the specified VLAN.

*slot-id*: Specifies to display the information about the VLAN policies applied to VLANs on the module seated in the specific slot. If the *slot-id* argument is not specified, this command displays the information about the VLAN policies applied to the Fabric.

**Description** Use the **display qos vlan-policy** command to display the information about VLAN policies.

If the *vlan-id* argument is not specified, the information about all the VLAN policies will be displayed.

**Examples** # Display the information about the VLAN policy named test.

```
<Sysname> display qos vlan-policy name test
 Policy test
 Vlan 300: inbound
```

**Table 238** Field descriptions of the display qos vlan-policy command

Field	Description
Policy	Name of the VLAN policy
Vlan 300	ID of the VLAN where the VLAN policy is applied
inbound	VLAN policy is applied in the inbound direction of the VLAN.

# Display the information about the VLAN policy applied to VLAN 300.

```
<Sysname> display qos vlan-policy vlan 300

 Vlan 300

 Direction: Inbound

 Policy: test
 Classifier: test
 Operator: AND
 Rule(s) : If-match customer-vlan-id 3
 Behavior: test
 Accounting Enable:
 0 (Packets)
 Committed Access Rate:
 CIR 6400 (kbps), CBS 4000 (byte), EBS 4000 (byte)
 Green Action: pass
 Red Action: discard
 Yellow Action: pass
 Green : 0(Packets)
```

**Table 239** Field descriptions of the display qos vlan-policy command

Field	Description
Vlan 300	ID of the VLAN where the VLAN policy is applied
Inbound	VLAN policy is applied in the inbound direction of the VLAN.
Classifier	Name of the class in the policy and its configuration
Behavior	Name of the behavior in the policy and its configuration

---

## qos apply policy

**Syntax** **qos apply policy** *policy-name* { **inbound** | **outbound** }

**undo qos apply policy** { **inbound** | **outbound** }

**View** Ethernet port view, port group view

**Parameters** **inbound**: Specifies the inbound direction.

**outbound**: Specifies the outbound direction.

*policy-name*: Specifies the policy name.

**Description** Use the **qos apply policy** command to apply a policy on a port or a port group.

Use the **undo qos apply policy** command to remove the policy applied on a port or a port group.

Note that, when you apply a policy by using the **qos apply policy** command, whether or not the **inbound/outbound** keyword can take effect depends on the actions defined in the traffic behavior and I/O Module types, as described in Table 240.

**Table 240** The support for the inbound direction and the outbound direction

I/O Module type	Action	SC I/O Module		SA I/O Module		EA I/O Module
		Inbound	Outbound	Inbound	Outbound	Inbound
Traffic accounting	Supported	Supported	Supported	Not supported	Supported	Not supported
TP	Supported	Supported	Supported	Not supported	Supported	Not supported
Traffic filtering	Supported	Supported	Supported	Not supported	Supported	Not supported
Traffic mirroring	Supported	Supported	Supported	Not supported	Supported	Not supported
Configuring the outer VLAN tag	Supported	Not supported	Supported	Not supported	Supported	Not supported
Traffic redirecting	Supported	Not supported	Supported	Not supported	Supported	Not supported
Remarking the customer network VLAN ID for packets	Not supported	Supported	Not supported	Not supported	Not supported	Not supported
Remarking the 802.1p precedence for packets	Supported	Supported	Supported	Not supported	Supported	Not supported
Remarking the drop precedence for packets	Supported	Not supported	Supported	Not supported	Supported	Not supported
Remarking the DSCP precedence for packets	Supported	Supported	Supported	Not supported	Supported	Not supported
Remarking the IP precedence for packets	Supported	Supported	Supported	Not supported	Supported	Not supported
Remarking the local precedence for packets	Supported	Not supported	Supported	Not supported	Supported	Not supported
Remarking the service provider network VLAN ID for packets	Supported	Supported	Supported	Not supported	Supported	Not supported



*SC I/O Modules include 0231A931 I/O Modules and so on, SA I/O Modules include LSQ13C16915SA I/O Modules and so on, EA I/O Modules include 0231A92P I/O Modules. For the detailed information about I/O Module types, refer to the installation manual.*



**CAUTION:** You can apply a QoS policy in the outbound direction of a basic QinQ-enabled port on an SA I/O Module or EA I/O Module to implement one-to-one VLAN mapping. In this policy, only one matching rule, **if-match service-vlan-id**, can be defined, and the action can only be **remark customer-vlan-id** or **remark customer-vlan-id** together with **remark dot1p**.

**Examples** # Apply the policy named test in the inbound direction of Ethernet2/0/1 port.



```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] qos apply policy test inbound
```

---

## qos apply policy global

**Syntax** **qos apply policy** *policy-name* **global** { **inbound** | **outbound** }  
**undo qos apply policy global** { **inbound** | **outbound** }

**View** System view

**Parameters** *policy-name*: Policy name.

**inbound**: Applies the QoS policy to the incoming packets on all ports.

**outbound**: Applies the QoS policy to the outgoing packets on all ports.

**Description** Use the **qos apply policy global** command to apply a QoS policy globally. A QoS policy applied globally takes effect on all inbound or outbound traffic depending on the direction in which the policy is applied.

Use the **undo qos apply policy global** command to cancel the global application of the QoS policy.

Note that, when you apply a QoS policy with the **qos apply policy global** command, support for the **inbound/outbound** keyword depends on the actions defined in the traffic behavior and I/O Module types, as described in Table 240.

**Examples** # Apply the QoS policy **user1** in the inbound direction globally.

```
<Sysname> system-view
[Sysname] qos apply policy user1 global inbound
```

---

## qos policy

**Syntax** **qos policy** *policy-name*  
**undo qos policy** *policy-name*

**View** System view

**Parameters** *policy-name*: Name of the policy to be created.

**Description** Use the **qos policy** command to create a policy. This command also leads you to policy view.

Use the **undo qos policy** command to remove a policy.

To remove a policy that is currently applied on a port, you need to disable it on the port first.

**Related commands:** **classifier behavior, qos apply policy.**

**Examples** # Create a policy named user1.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

## qos vlan-policy

**Syntax** **qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

**undo qos vlan-policy** **vlan** *vlan-id-list* { **inbound** | **outbound** }

**View** System view

**Parameters** *policy-name*: Policy name.

*vlan-id-list*: List of VLAN IDs, presented in the form of *vlan-id* **to** *vlan-id* or discontinuous VLAN IDs. Up to eight VLAN IDs can be specified at a time.

**inbound**: Specifies to apply the VLAN policy in the inbound direction of the VLAN.

**outbound**: Specifies to apply the VLAN policy in the outbound direction of the VLAN.

**Description** Use the **qos vlan-policy** command to apply the VLAN policy to the specific VLAN(s).

Use the **undo qos vlan-policy** command to remove the VLAN policy from the specific VLAN(s).

Note that, when you apply a QoS policy with the **qos vlan-policy** command, support for the **inbound/outbound** keyword varies with the actions defined in the traffic behavior and the type of the I/O Module to which the ports in the VLAN belong, as described in Table 240.



*Do not apply policies to a VLAN and the ports in the VLAN at the same time.*

**Examples** # Apply the VLAN policy named test in the inbound direction of VLAN 200, VLAN 300, VLAN 400, VLAN 500, VLAN 600, VLAN 700, VLAN 800, and VLAN 900.

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 600 700 800 900 inbound
```

---

## reset qos policy global

**Syntax** `reset qos policy global { inbound | outbound }`

**View** User view

**Parameters** **inbound**: Specifies the inbound direction.

**outbound**: Specifies the outbound direction.

**Description** Use the **reset qos vlan-policy** command to clear the statistics of a global QoS policy.

**Examples** # Clear the statistics of the global QoS policy in the inbound direction.  
`<Sysname> reset qos policy global inbound`

---

## reset qos vlan-policy

**Syntax** `reset qos vlan-policy [ vlan vlan-id ]`

**View** User view

**Parameters** *vlan-id*: VLAN ID, in the range 1 to 4,094.

**Description** Use the **reset qos vlan-policy** command to clear the statistics information about VLAN policies.

**Examples** # Clear the statistics information about the VLAN policy applied to VLAN 2.  
`<Sysname> reset qos vlan-policy vlan 2`



# 68

## CONGESTION MANAGEMENT CONFIGURATION COMMANDS

---

### display qos sp interface

**Syntax** **display qos sp interface** [ *interface-type interface-number* ]

**View** Any view

**Parameters** *interface-type*: Port type.

*interface-number*: Port number.

**Description** Use the **display qos sp interface** command to display the strict priority (SP) queuing configuration on a specified port.

If no port is specified, this command displays the SP queuing configuration on all ports.

**Related commands:** **qos sp.**

**Examples** # Display the SP queuing configuration on Ethernet 2/0/1.  

```
<Sysname> display qos sp interface Ethernet 2/0/1
Interface: Ethernet2/0/1
Output queue: Strict-priority queue
```

---

### display qos wrr interface

**Syntax** **display qos wrr interface** [ *interface-type interface-number* ]

**View** Any view

**Parameters** *interface-type*: Port type.

*interface-number*: Port number.

**Description** Use the **display qos wrr interface** command to display the configuration of weighted round robin (WRR) queues of a port.

If no port number is specified, the command displays the configurations of WRR queues of all ports.

**Related commands:** `qos wrr`.

**Examples** # Display the configuration of WRR queues of Ethernet 2/0/1.

```
<Sysname> display qos wrr interface Ethernet 2/0/1
Interface: Ethernet2/0/1
Output queue: Weighted round robin queue
Queue ID Group Weight

0 sp N/A
1 sp N/A
2 1 3
3 1 4
4 1 5
5 1 6
6 1 7
7 1 8
```

**Table 241** Field descriptions of the display qos wrr interface command

Field	Description
Interface	Port name, composed of port type and port number
Output queue	The type of the current output queue
Queue ID	ID of the queue
Group	Group ID, indicating which group a queue belongs to.
Weight	The weight of each queue during scheduling. N/A indicates that SP queue scheduling algorithm is adopted.

---

## qos sp

**Syntax** `qos sp`

`undo qos sp`

**View** Ethernet interface view, port group view

**Parameters** None

**Description** Use the `qos sp` command to configure SP queuing on the current port.

Use the `undo qos sp` command to restore the default queuing algorithm on the port.

By default, the switch adopts the SP queue-scheduling algorithm.

**Related commands:** `display qos sp interface`.

**Examples** # Configure SP queuing on Ethernet 2/0/1.

```
<S7900E> system-view
[S7900E] interface Ethernet 2/0/1
[S7900E-Ethernet2/0/1] qos sp
```

---

**qos wrr**

**Syntax** **qos wrr** *queue-id* **group** { **sp** | *group-id* **weight** *queue-weight* }

**undo qos wrr**

**View** Ethernet interface view, port group view

**Parameters** *queue-id*: ID of the queue, in the range of 0 to 7.

*group-id*: It can only be 1.

**weight** *schedule-value*: Specifies the scheduling weight of a queue, rang from 1 to 15.

**sp**: Configures SP queuing.

**Description** Use the **qos wrr** command to configure Weighted Round Robin (WRR) queue scheduling algorithm or the SP + WRR queue scheduling algorithm on a port or port group.

Use the **undo qos wrr** command to restore the default queue-scheduling algorithm on the port.

By default, the switch adopts the SP queue-scheduling algorithm.

As required, you can configure part of the queues on the port to adopt the SP queue-scheduling algorithm and parts of queues to adopt the WRR queue-scheduling algorithm. Through adding the queues on a port to the SP scheduling group and WRR scheduling group (namely, group 1), the SP + WRR queue scheduling is implemented. During the queue scheduling process, the queues in the SP scheduling group is scheduled preferentially. When no packet is to be sent in the queues in the SP scheduling group, the queues in the WRR scheduling group are scheduled. The queues in the SP scheduling group are scheduled according to the strict priority of each queue, while the queues in the WRR queue scheduling group are scheduled according the weight value of each queue.

**Related commands:** **display qos wrr interface.**

**Examples** # Configure SP+WRR queue scheduling algorithm on Ethernet 2/0/1 as follows: assign queue 0, queue 1, queue 2, and queue 3 to the SP scheduling group; and assign queue 4, queue 5, queue 5, and queue 7 to WRR scheduling group, with the weight 2, 4, 6, and 8.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] qos wrr
[Sysname-Ethernet2/0/1] qos wrr 0 group sp
[Sysname-Ethernet2/0/1] qos wrr 1 group sp
[Sysname-Ethernet2/0/1] qos wrr 2 group sp
[Sysname-Ethernet2/0/1] qos wrr 3 group sp
```

```
[Sysname-Ethernet2/0/1] qos wrr 4 group 1 weight 2
[Sysname-Ethernet2/0/1] qos wrr 5 group 1 weight 4
[Sysname-Ethernet2/0/1] qos wrr 6 group 1 weight 6
[Sysname-Ethernet2/0/1] qos wrr 7 group 1 weight 8
```



# 69

## PRIORITY MAPPING TABLE CONFIGURATION COMMANDS

---

### display qos map-table

**Syntax** `display qos map-table [ dot1p-dp | dot1p-lp | dscp-dot1p | dscp-dp | dscp-dscp ]`

**View** Any view

**Parameters** **dot1p-lp**: Specifies the 802.1p precedence-to-local precedence mapping table.  
**dot1p-dp**: Specifies the 802.1p precedence-to-drop precedence mapping table.  
**dscp-dp**: Specifies the DSCP-to-drop precedence mapping table.  
**dscp-dot1p**: Specifies the DSCP-to-802.1p precedence mapping table.  
**dscp-dscp**: Specifies the DSCP-to-DSCP mapping table.

**Description** Use the **display qos map-table** command to display the configuration of a priority mapping table.  
  
If the type of the priority mapping table is not specified, the configuration of all the priority mapping tables is displayed.

**Related commands:** **qos map-table**.

**Examples** # Display the configuration of the 802.1p precedence-to-drop precedence mapping table.

```
<Sysname> display qos map-table dot1p-dp
MAP-TABLE NAME: dot1p-dp TYPE: pre-define
IMPORT : EXPORT
 0 : 2
 1 : 2
 2 : 2
 3 : 1
 4 : 1
 5 : 1
 6 : 0
 7 : 0
```

**Table 242** Field descriptions of the display qos map-table command

Field	Description
MAP-TABLE NAME	Name of the mapping table

**Table 242** Field descriptions of the display qos map-table command

Field	Description
TYPE	Type of the mapping table
IMPORT	Input entries of the mapping table
EXPORT	Output entries of the mapping table

---

## qos map-table

**Syntax** `qos map-table { dot1p-dp | dot1p-lp | dscp-dot1p | dscp-dp | dscp-dscp }`

**View** System view

**Parameters** **dot1p-lp**: Specifies the 802.1p precedence-to-local precedence mapping table.  
**dot1p-dp**: Specifies the 802.1p precedence-to-drop precedence mapping table.  
**dscp-dp**: Specifies the DSCP-to-drop precedence mapping table.  
**dscp-dot1p**: Specifies the DSCP-to-802.1p precedence mapping table.  
**dscp-dscp**: Specifies the DSCP-to-DSCP mapping table.

**Description** Use the **qos map-table** command to enter specific priority mapping table view.

**Related commands:** **display qos map-table.**

**Examples** # Enter 802.1p precedence-to-drop precedence mapping table view.  

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp]
```

---

## import

**Syntax** `import import-value-list export export-value`  
`undo import { import-value-list | all }`

**View** Priority mapping table view

**Parameters** *import-value-list*: List of input parameters.  
*export-value*: Output parameter in the mapping table.  
**all**: Removes all the parameters in the priority mapping table.

**Description** Use the **import** command to configure entries for a priority mapping table, that is, to define one or more mapping rules.

Use the **undo import** command to restore specific entries of a priority mapping table to the default.

Note that, you cannot configure to map any DSCP value to drop precedence 1.

**Related commands:** **display qos map-table.**

**Examples** # Configure the 802.1p precedence-to-drop precedence mapping table to map 802.1p precedence 4 and 5 to drop precedence 1.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp] import 4 5 export 1
```



# 70

## PORT PRIORITY CONFIGURATION COMMANDS

---

### qos priority

**Syntax** `qos priority priority-value`

`undo qos priority`

**View** Ethernet port view, port group view

**Parameters** *priority-value*: Port priority to be configured. This argument is in the range 0 to 7.

**Description** Use the **qos priority** command to set the port priority for a port.

Use the **undo qos priority** command to restore the default port priority.

By default, the port priority is 0.

Note that, if a port receives packets without an 802.1q tag, the switch takes the priority of the receiving port as the 802.1p precedence of the packets and then searches the **dot1p-dp/lp** mapping table for the local/drop precedence for the packets according to the priority of the receiving port.

**Examples** # Set the port priority of Ethernet2/0/1 port to 2.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] qos priority 2
```



# 71

## PORT PRIORITY TRUST MODE CONFIGURATION COMMANDS

---

### display qos trust interface

**Syntax** `display qos trust interface [ interface-type interface-number ]`

**View** Any view

**Parameters** *interface-type*: Port type.

*interface-number*: Port number.

**Description** Use the **display qos trust interface** command to display the port priority trust mode of a port.

If no port is specified, this command displays the port priority trust modes of all the ports.

**Examples** # Display the port priority trust mode of Ethernet2/0/1 port.

```
<Sysname> display qos trust interface Ethernet 2/0/1
Interface: Ethernet2/0/1
Port priority information
Port priority :0
Port priority trust type : dscp
```

**Table 243** Field descriptions of the display qos trust interface command

Field	Description
Interface	Port name, comprising of port type and port number
Port priority	Port priority
Port priority trust type	Port priority trust mode <ul style="list-style-type: none"><li>dscp indicates that the DSCP precedence of the received packets is trusted</li><li>untrust indicates that the 802.1p precedence of the received packets is trusted</li></ul>

---

### qos trust

**Syntax** `qos trust dscp`

`undo qos trust`

**View** Ethernet port view, port group view

**Parameters** **dscp**: Specifies to trust DSCP precedence carried in the packet and adopt this priority for priority mapping.

**Description** Use the **qos trust** command to configure the port priority trust mode.  
Use the **undo qos trust** command to restore the default port priority trust mode.  
By default, the 802.1p precedence of the received packets is trusted.

**Examples** # Specify to trust the DSCP precedence carried in packets on Ethernet 2/0/1 port.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] qos trust dscp
```



# 72

## TRAFFIC MIRRORING CONFIGURATION COMMANDS

---

### mirror-to

**Syntax** **mirror-to** { **cpu** | **interface** *interface-type interface-number* }  
**undo mirror-to** { **cpu** | **interface** *interface-type interface-number* }

**View** Traffic behavior view

**Parameters** **cpu**: Redirects packets to the CPU.  
**interface** *interface-type interface-number*: Port type and port number of the destination port for the traffic mirroring action.

**Description** Use the **mirror-to** command to configure traffic mirroring action for a traffic behavior.

Use the **undo mirror-to** command to remove the traffic mirroring action.

Note that when the action of mirroring traffic is applied in the outbound direction, any other action cannot be configured in the same traffic behavior. Otherwise, the corresponding QoS policy cannot be applied successfully.

**Examples** # Configure traffic behavior 1 and define the action of mirroring traffic to Ethernet2/0/2 in the traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to interface Ethernet 2/0/2
```



# 73

## PORT MIRRORING CONFIGURATION COMMANDS

---

### display mirroring-group

**Syntax** `display mirroring-group { group-id | all | local | remote-destination | remote-source }`

**View** Any view

**Parameters** *group-id*: Port mirroring group number, in the range of 1 to 4.

**all**: Specifies all the port mirroring groups.

**local**: Specifies local port mirroring groups.

**remote-destination**: Specifies remote destination port mirroring groups.

**remote-source**: Specifies remote source port mirroring groups.

**Description** Use the **display mirroring-group** command to display the information about a port mirroring group or multiple port mirroring groups.

The output information varies with port mirroring group type and is organized by mirroring group numbers.

**Examples** # Display the information about all the port mirroring groups.

```
<Sysname> display mirroring-group all
mirroring-group 1:
 type: local
 status: active
 mirroring port:
 Ethernet2/0/1 both
 monitor port: Ethernet2/0/10
mirroring-group 2:
 type: remote-source
 status: active
 mirroring port:
 Ethernet2/0/3 both
 monitor egress port: Ethernet2/0/11
 remote-probe vlan: 200
```

**Table 244** Field descriptions of the display mirroring-group command

Field	Description
mirroring-group	Port mirroring group number

**Table 244** Field descriptions of the display mirroring-group command

Field	Description
type	Port mirroring group type, which can be local, remote-source, and remote-destination.
status	Status of a port mirroring group. "active" for already effective, and "inactive" for not effective yet.
mirroring port	Source mirroring port
monitor port	Destination mirroring port
monitor egress port	Outbound mirroring port
remote-probe vlan	Remote mirroring VLAN

---

## mirroring-group

**Syntax** **mirroring-group** *group-id* { **local** | **remote-destination** | **remote-source** }

**undo mirroring-group** { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

**View** System view

**Parameters** *group-id*: Port mirroring group number, in the range of 1 to 4.

**all**: Removes All the port mirroring groups.

**local**: Creates/Removes a local port mirroring group.

**remote-destination**: Creates/Removes a remote destination port mirroring group.

**remote-source**: Creates/Removes a remote source port mirroring group.

**Description** Use the **mirroring-group** command to create a port mirroring group.

Use the **undo mirroring-group** command to remove a port mirroring group.

You need to specify the type of the port mirroring group to be created when creating it.

- Use the keyword **local** to create a local port mirroring group.
- Use the keyword **remote-destination** to create a remote destination port mirroring group.
- Use the keyword **remote-source** to create a remote source port mirroring group.

You need to specify the port mirroring group type or the mirroring group number when removing a port mirroring group:

- Use the *group-id* argument to specify the port mirroring group to be removed.
- Use the **all** keyword to remove all the port mirroring groups.

- Use the **local** keyword to remove all the local port mirroring groups.
- Use the **remote-destination** keyword to remove all the remote destination port mirroring groups.
- Use the **remote-source** keyword to remove all the remote source mirroring groups.

**Examples** # Create a local port mirroring group numbered 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
```

# Create remote destination mirroring group numbered 2.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
```

---

## mirroring-group mirroring-port

**Syntax** **mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

**undo mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

**View** System view

**Parameters** *group-id*: Port mirroring group number, in the range of 1 to 4.

*mirroring-port-list*: List of ports to be added to the port mirroring group. You can specify multiple ports by providing this argument in the form of { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-8>, where the *interface-type* argument is port type, the *interface-number* argument is the port number, and &<1-8> means that you can provide up to eight port indexes/port index lists for this argument.

**both**: Specifies to duplicate both inbound and outbound packets.

**inbound**: Specifies to duplicate inbound packets only.

**outbound**: Specifies to duplicate outbound packets only.

**Description** Use the **mirroring-group mirroring-port** command to configure source ports for a port mirroring group.

Use the **undo mirroring-group mirroring-port** command to remove source ports from a port mirroring group.

Note that:

- The source port cannot be a member port of the current mirroring group.
- A remote destination mirroring group cannot contain source mirroring ports.

**Examples** # Add ports to port mirroring group 1 as source ports (assuming that port mirroring group 1 already exists).

```
<Sysname> system-view
[Sysname] mirroring-group 1 mirroring-port Ethernet 2/0/1 to Ethernet 2/0/5 both
```

# Remove source mirroring ports from port mirroring group 1.

```
[Sysname] undo mirroring-group 1 mirroring-port Ethernet 2/0/1 to Ethernet 2/0/3 both
```

## mirroring-group monitor-egress

**Syntax** In system view:

**mirroring-group** *group-id* **monitor-egress** *monitor-egress-port-id*

**undo mirroring-group** *group-id* **monitor-egress** *monitor-egress-port-id*

In Ethernet port view:

**mirroring-group** *group-id* **monitor-egress**

**undo mirroring-group** *group-id* **monitor-egress**

**View** System view, Ethernet port view

**Parameters** *group-id*: Port mirroring group number, in the range of 1 to 4.

*monitor-egress-port-id*: Index of the port to be configured as the outbound mirroring port. You need to provide this argument in the format of { *interface-type interface-number* }, where *interface-type* is port type and *interface-number* is port number.

**Description** Use the **mirroring-group monitor-egress** command to configure a port as the outbound mirroring port of a remote port mirroring group.

Use the **undo mirroring-group monitor-egress** command to remove the outbound mirroring port configured from a remote port mirroring group.

Note that:

- Only remote source port mirroring groups can have outbound mirroring ports. A port mirroring group can have only one outbound mirroring port.
- The outbound port cannot be a member port of the current mirroring group.
- It is not recommended to configure STP, RSTP, MSTP, 802.1x, IGMP Snooping, static ARP and MAC address learning on the outbound mirroring port; otherwise, the mirroring function may be affected.

**Examples** # Configure port Ethernet 2/0/1 as the outbound mirroring port of remote port mirroring group 1 in system view.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 monitor-egress Ethernet 2/0/1
```

# Configure port Ethernet 2/0/2 as the outbound mirroring port of remote port mirroring group 2 in Ethernet port view.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] mirroring-group 2 monitor-egress
```

---

## mirroring-group monitor-port

**Syntax** **mirroring-group** *group-id* **monitor-port** *monitor-port-id*

**undo mirroring-group** *group-id* **monitor-port** *monitor-port-id*

**View** System view

**Parameters** *group-id*: Port mirroring group number, in the range of 1 to 4.

*monitor-port-id*: Port index. You need to provide this argument in the form of *interface-type interface-number*, where *interface-type* is the port type and *interface-number* is the port number.

**Description** Use the **mirroring-group monitor-port** command to configure the destination port for a port mirroring group.

Use the **undo mirroring-group monitor-port** command to remove the destination port from a port mirroring group.

Note that:

- A port mirroring group can contain only one destination port.
- The destination port cannot be a member port of the current mirroring group.
- The destination mirroring port can be an access, trunk, or hybrid port. It must be assigned to the remote mirroring VLAN.
- A remote source port mirroring group cannot contain destination ports.
- Before configuring the destination port for a port mirroring group, make sure the port mirroring group exists.
- Do not enable STP, RSTP, or MSTP on the destination port. Otherwise, the mirroring function may be affected.
- Do not use the destination mirroring port for any purpose other than port mirroring.

**Examples** # Configure Ethernet 2/0/1 as the destination port of port mirroring group 1 (a remote destination port mirroring group).

```

<Sysname> system-view
[Sysname] mirroring-group 1 remote-destination
[Sysname] mirroring-group 1 monitor-port Ethernet 2/0/1

```

---

## mirroring-group remote-probe vlan

**Syntax** `mirroring-group group-id remote-probe vlan rprobe-vlan-id`

`undo mirroring-group group-id remote-probe vlan rprobe-vlan-id`

**View** System view

**Parameters** *group-id*: Port mirroring group number, in the range of 1 to 4.

*rprobe-vlan-id*: ID of the VLAN to be configured as the remote mirroring VLAN. Note that the VLAN must be an existing static VLAN.

**Description** Use the **mirroring-group remote-probe vlan** command to specify a VLAN as the mirroring VLAN for a remote source port mirroring group or a remote destination port mirroring group.

Use the **undo mirroring-group remote-probe vlan** command to remove the remote mirroring VLAN from a remote source mirroring group or a remote destination mirroring group.

Note that:

- Only remote source port mirroring groups or remote destination port mirroring groups can have remote mirroring VLANs. A port mirroring group can have only one remote mirroring VLAN.
- To remove a VLAN operating as a remote port mirroring VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.
- You are recommended to use a remote mirroring VLAN for remote mirroring only.

**Examples** # Specify VLAN 2 as the remote mirroring VLAN of port mirroring group 1 (assuming that VLAN 2 already exists).

```

<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 remote-probe vlan 2

```

---

## mirroring-port

**Syntax** `[ mirroring-group group-id ] mirroring-port { inbound | outbound | both }`

`undo [ mirroring-group group-id ] mirroring-port { inbound | outbound | both }`



<b>View</b>	Ethernet port view
<b>Parameters</b>	<p><i>group-id</i>: Port mirroring group number, in the range of 1 to 4.</p> <p><b>both</b>: Duplicates both inbound and outbound packets.</p> <p><b>inbound</b>: Duplicates the inbound packets only.</p> <p><b>outbound</b>: Duplicates the outbound packets only.</p>
<b>Description</b>	<p>Use the <b>mirroring-port</b> command to configure a port as a source mirroring port of a port mirroring group.</p> <p>Use the <b>undo mirroring-port</b> command to remove a source mirroring port from a port mirroring group.</p> <p>Note that:</p> <ul style="list-style-type: none"> <li>■ If you do not specify the <b>mirroring-group</b> <i>group-id</i> keyword-argument combination, these two commands apply to port mirroring group 1.</li> <li>■ The source port cannot be a member port of the current mirroring group.</li> <li>■ A remote destination mirroring group cannot contain source mirroring ports.</li> </ul>
<b>Examples</b>	<pre># Configure Ethernet 2/0/1 as a source mirroring port of remote source port mirroring group 2.  &lt;Sysname&gt; system-view [Sysname] mirroring-group 2 remote-source [Sysname] interface Ethernet 2/0/1 [Sysname-Ethernet2/0/1] mirroring-group 2 mirroring-port both</pre>

---

## monitor-port

<b>Syntax</b>	<p>[ <b>mirroring-group</b> <i>group-id</i> ] <b>monitor-port</b></p> <p><b>undo</b> [ <b>mirroring-group</b> <i>group-id</i> ] <b>monitor-port</b></p>
<b>View</b>	Ethernet port view
<b>Parameters</b>	<i>group-id</i> : Port mirroring group number, in the range of 1 to 4.
<b>Description</b>	<p>Use the <b>monitor-port</b> command to configure a port as the destination mirroring port of a port mirroring group.</p> <p>Use the <b>undo monitor-port</b> command to remove the destination mirroring port from a port mirroring group.</p> <p>If you do not specify the <b>mirroring-group</b> <i>group-id</i> keyword-argument combination, the <b>monitor-port</b> command adds the current port to port mirroring group 1.</p>

Note that:

- If you do not specify the **mirroring-group** *group-id* keyword-argument combination, these two commands apply to port mirroring group 1.
- A remote source mirroring group cannot contain destination mirroring ports.
- Member ports of existing port mirroring groups cannot be destination ports.
- The remote destination mirroring port can be an access, trunk, or hybrid port. It must be assigned to the remote mirroring VLAN.
- Before adding the destination port for a port mirroring group, make sure the port mirroring group exists.
- Do not enable STP, RSTP, or MSTP on the destination port. Otherwise, the mirroring function may be affected.
- Do not use the destination mirroring port for any purpose other than port mirroring.

**Examples** # Add port Ethernet 2/0/1 to port mirroring group 1 (a local port mirroring group) as the destination port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] monitor-port
```

# 74

## SNMP CONFIGURATION COMMANDS

---

### display snmp-agent local-switch fabricid

**Syntax** `display snmp-agent local-switch fabricid`

**View** Any view

**Parameters** None

**Description** Use the **display snmp-agent local-switch fabricid** command to display the local SNMP agent switch fabric ID.

SNMP switch fabric ID identifies an SNMP entity uniquely within an SNMP domain. SNMP switch fabric is an indispensable part of an SNMP entity. It provides the SNMP message allocation, message handling, authentication, and access control.

**Examples** # Display the local SNMP agent switch fabric ID.

```
<Sysname> display snmp-agent local-switch fabricid
SNMP local EngineID: 000063A27F000001000071DA
```

---

### display snmp-agent community

**Syntax** `display snmp-agent community [ read | write ]`

**View** Any view

**Parameters** **read**: Displays the information of communities with read-only access right.

**write**: Displays the information of communities with read and write access right.

**Description** Use the **display snmp-agent community** command to display community information for SNMPv1 or SNMPv2c.

**Examples** # Display the information for all the current communities.

```
<Sysname> display snmp-agent community
Community name: aa
Group name: aa
Acl:2001
Storage-type: nonVolatile
```

```
Community name: bb
Group name: bb
Storage-type: nonVolatile
```

**Table 245** Descriptions on the fields of display snmp-agent community

Field	Description
Community name	Community name
Group name	SNMP group name
Acl	The number of the ACL in use
Storage-type	Storage type, which could be: <ul style="list-style-type: none"> <li>■ <i>volatile</i>: Information will be lost if the system is rebooted</li> <li>■ <i>nonVolatile</i>: Information will not be lost if the system is rebooted</li> <li>■ <i>permanent</i>: Modification permitted, but deletion forbidden</li> <li>■ <i>readOnly</i>: Read only, that is, no modification, no deletion</li> <li>■ <i>other</i>: Other storage types</li> </ul>

## display snmp-agent group

**Syntax** `display snmp-agent group [ group-name ]`

**View** Any view

**Parameters** *group-name*: Specifies the SNMP group name, a string of 1 to 32 characters, case sensitive.

**Description** Use the **display snmp-agent group** command to display information for the SNMP agent group, including group name, security model, MIB view, storage type, and so on. Absence of the *group-name* parameter indicates that information for all groups will be displayed.

**Examples** # Display the information of all SNMP agent groups.

```
<Sysname> display snmp-agent group
Group name: aa
Security model: v3 noAuthnoPriv
Readview: ViewDefault
Writeview: <no specified>
Notifyview: <no specified>
Storage-type: nonVolatile
```

**Table 246** Descriptions on the fields of the display snmp-agent group command

Field	Description
Group name	SNMP group name
Security model	Security model of the SNMP group, which can be: authPriv (authentication with privacy), authNoPriv (authentication without privacy), or noAuthNoPriv (no authentication no privacy).
Readview	The read only MIB view associated with the SNMP group
Writeview	The writable MIB view associated with the SNMP group

**Table 246** Descriptions on the fields of the display snmp-agent group command

Field	Description
Notifyview	The notify MIB view associated with the SNMP group, the view with entries that can generate Trap messages
Storage-type	Storage type, which includes: volatile, nonVolatile, permanent, readOnly, and other. For detailed information, refer to Table 245.

---

## display snmp-agent mib-view

**Syntax** `display snmp-agent mib-view [ exclude | include | viewname view-name ]`

**View** Any view

**Parameters** **exclude**: Specifies to display SNMP MIB views of the **excluded** type.

**include**: Specifies to display SNMP MIB views of the **included** type.

**viewname** *view-name*: Displays view with a specified name, where *view-name* is the name of the specified MIB view.

**Description** Use the **display snmp-agent mib-view** command to display SNMP MIB view information. Absence of the *view-name* parameter indicates that information for all MIB views will be displayed.

**Examples** # Display the current SNMP MIB views.

```
<Sysname> display snmp-agent mib-view
View name:ViewDefault
MIB Subtree:iso
Subtree mask:
Storage-type: nonVolatile
View Type:included
View status:active

View name:ViewDefault
MIB Subtree:snmpUsmMIB
Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active

View name:ViewDefault
MIB Subtree:snmpVacmMIB
Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active

View name:ViewDefault
MIB Subtree:snmpModules.18
Subtree mask:
Storage-type: nonVolatile
```

```
View Type:excluded
View status:active
```

**Table 247** Descriptions on the fields of the display snmp-agent mib-view command

Field	Description
View name	MIB view name
MIB Subtree	MIB subtree corresponding to the MIB view
Subtree mask	MIB subtree mask
Storage-type	Storage type
View Type	View type, which can be included or <b>excluded</b> Included indicates that all nodes of the MIB tree are included in current view. Excluded indicates that not all nodes of the MIB tree are included in current view.
View status	The status of MIB view

## display snmp-agent statistics

**Syntax** `display snmp-agent statistics`

**View** Any view

**Parameters** None

**Description** Use the **display snmp-agent statistics** command to display SNMP statistics.

**Examples** # Display the statistics on the current SNMP.

```
<Sysname> display snmp-agent statistics
 0 Messages delivered to the SNMP entity
 0 Messages which were for an unsupported version
 0 Messages which used a SNMP community name not known
 0 Messages which represented an illegal operation for the community supplied
 0 ASN.1 or BER errors in the process of decoding
 0 Messages passed from the SNMP entity
 0 SNMP PDUs which had badValue error-status
 0 SNMP PDUs which had genErr error-status
 0 SNMP PDUs which had noSuchName error-status
 0 SNMP PDUs which had tooBig error-status (Maximum packet size 1500)
 0 MIB objects retrieved successfully
 0 MIB objects altered successfully
 0 GetRequest-PDU accepted and processed
 0 GetNextRequest-PDU accepted and processed
 0 GetBulkRequest-PDU accepted and processed
 0 GetResponse-PDU accepted and processed
 0 SetRequest-PDU accepted and processed
 0 Trap PDUs accepted and processed
 0 Alternate Response Class PDUs dropped silently
 0 Forwarded Confirmed Class PDUs dropped silently
```

**Table 248** Descriptions on the fields of the display snmp-agent statistics command

Field	Description
Messages delivered to the SNMP entity	Number of packets delivered to the SNMP agent

**Table 248** Descriptions on the fields of the display snmp-agent statistics command

Field	Description
Messages which were for an unsupported version	Number of packets from a device with an SNMP version that is not supported by the current SNMP agent
Messages which used a SNMP community name not known	Number of packets that use an unknown community name
Messages which represented an illegal operation for the community supplied	Number of packets with operations that breach the access right of a community
ASN.1 or BER errors in the process of decoding	Number of packets with ASN.1 or BER errors in the process of decoding
Messages passed from the SNMP entity	Number of packets sent by an SNMP Agent
SNMP PDUs which had badValue error-status	Number of SNMP PDUs with a badValue error
SNMP PDUs which had genErr error-status	Number of SNMP PDUs with a genErr error
SNMP PDUs which had noSuchName error-status	Number of PDUs with a noSuchName error
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	Number of PDUs with a tooBig error (the maximum packet size is 1,500 bytes)
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved
MIB objects altered successfully	Number of MIB objects that have been successfully modified
GetRequest-PDU accepted and processed	Number of get requests that have been received and processed
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed
Trap PDUs accepted and processed	Number of Trap messages that have been received and processed
Alternate Response Class PDUs dropped silently	Number of dropped response packets
Forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped

---

## display snmp-agent sys-info

**Syntax** `display snmp-agent sys-info [ contact | location | version ] *`

**View** Any view

**Parameters** **contact:** Displays the contact information of the current network administrator.

**location:** Displays the location information of the current device.

**version:** Displays the version of the current SNMP agent.

**Description** Use the **display snmp-agent sys-info** command to display the current SNMP system information.

If no keyword is specified, all SNMP agent system information will be displayed.

**Examples** # Display the current SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
 The contact person for this managed node:
 Hangzhou 3Com Technologies Co., Ltd.
 The physical location of this node:
 Marlborough, MA
 SNMP version running in the system:
 SNMPv3
```

---

## display snmp-agent trap-list

**Syntax** **display snmp-agent trap-list**

**View** Any view

**Parameters** None

**Description** Use the **display snmp-agent trap-list** command to display the modules that can send the Trap messages and whether their Trap sending is enabled or not. If a module comprises of multiple sub-modules, then as long as one sub-module has the sending of Trap messages enabled, the whole module will be displayed as being enabled with the Trap sending.

**Related commands:** **snmp-agent trap enable.**

**Examples** # Display the modules that can send the Trap messages and whether their Trap sending is enabled or not.

```
<Sysname> display snmp-agent trap-list
 bgp trap enable
 configuration trap enable
 flash trap enable
 ospf trap enable
 standard trap enable
 system trap enable
 vrrp trap enable

 Enable traps: 7; Disable traps: 0
```

In the above output, enable indicates that the module is enabled with the Trap sending whereas disable indicates the Trap sending is disabled. By default, Trap sending is enabled on all modules that can send Trap messages. Use the **snmp-agent trap enable** command to manually configure whether the Trap sending is enabled or not.



---

## display snmp-agent usm-user

**Syntax** **display snmp-agent usm-user** [ **switch fabricid** *switch fabricid* | **username** *user-name* | **group** *group-name* ] \*

**View** Any view

**Parameters** **switch fabricid** *switch fabricid*: Displays SNMPv3 user information for a specified switch fabric ID, where *switch fabricid* indicates the SNMP switch fabric ID.

**username** *user-name*: Displays SNMPv3 user information for a specified user name. It is case sensitive.

**group** *group-name*: Displays SNMPv3 user information for a specified SNMP group name. It is case sensitive.

**Description** Use the **display snmp-agent usm-user** command to display SNMPv3 user information.

**Examples** # Display SNMPv3 information for the user **aa**.

```
<Sysname> display snmp-agent usm-user username aa
 User name: aa
 Group name: mygroupv3
 Engine ID: 000063A27F000001000071DA
 Storage-type: nonVolatile
 UserStatus: active
```

**Table 249** Descriptions on the fields of the display snmp-agent usm-user command

Field	Description
User name	SNMP user name
Group name	SNMP group name
Engine ID	Engine ID for an SNMP entity
Storage-type	Storage type
UserStatus	SNMP user status

---

## enable snmp trap updown

**Syntax** **enable snmp trap updown**  
**undo enable snmp trap updown**

**View** Interface view

**Parameters** None

**Description** Use the **enable snmp trap updown** command to enable the sending of Trap messages for interface state change (linkup/linkdown Trap messages).

Use the **undo enable snmp trap updown** command to disable the sending of linkup/linkdown SNMP Trap messages on an interface.

By default, the sending of linkup/linkdown SNMP Trap messages is enabled.

Note that:

To enable an interface to send SNMP Traps when its state changes, you need to enable the Link up/down Trap packet transmission function on an interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable [ standard [ linkdown | linkup ] \* ]** command to enable this function globally.

**Related commands:** **snmp-agent target-host**, **snmp-agent trap enable**.

**Examples** # Enable the sending of linkup/linkdown SNMP Trap messages on the port Ethernet 2/0/1 and use the community name **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet 2/0/1] enable snmp trap updown
```

---

## snmp-agent calculate-password

**Syntax** **snmp-agent calculate-password** *plain-password* **mode** { **md5** | **sha** }  
{ **local-switch fabricid** | **specified-switch fabricid** *string* }

**View** System view

**Parameters** *plain-password*: Plain text password to be encrypted.

**mode**: Specifies to encrypt a plain text password by authentication.

- **md5**: Specifies the authentication protocol to be HMAC-MD5-96.
- **sha**: Specifies the authentication protocol to be HMAC-SHA-96.

**local**: Represents a local SNMP entity user.

**local-switch fabricid**: Specifies to use local switch fabric ID to calculate cipher text password.

**specified-switch fabricid**: Specifies to use user-defined switch fabric ID to calculate cipher text password.

*string*: The switch fabric ID string, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

**Description** Use the **snmp-agent calculate-password** command to convert the user-defined plain text password to a cipher text password using the specified authentication mode.

Note that the cipher text password converted with the **sha** keyword specified in this command is a string of 40 hexadecimal characters. For an authentication password, all of the 40 hexadecimal characters are valid; while for a privacy password, only the first 32 hexadecimal characters are valid.

**Related commands:** **snmp-agent usm-user v3**.

**Examples** # Use local switch fabric ID and MD5 authentication protocol to convert the plain text password **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode md5 local-switch fabricid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

## snmp-agent

**Syntax** **snmp-agent**  
**undo snmp-agent**

**View** System view

**Parameters** None

**Description** Use the **snmp-agent** command to enable SNMP agent.  
Use the **undo snmp-agent** command to disable SNMP agent.  
By default, SNMP agent is disabled.

**Examples** # Disable the current SNMP agent.

```
<Sysname> system-view
[Sysname] undo snmp-agent
```

## snmp-agent community

**Syntax** **snmp-agent community** { **read** | **write** } *community-name* [ **acl** *acl-number* | **mib-view** *view-name* ] \*  
**undo snmp-agent community** *community-name*

**View** System view

**Parameters** **read**: Indicates that the community has read only access right to the MIB objects, that is, the community can only inquire MIB information.

**write:** Indicates that the community has read and write access right to the MIB objects, that is, the community can configure MIB information.

*community-name:* Community name, a string of 1 to 32 characters.

*acl acl-number:* ACL for the community name, with *acl-number* indicating the ACL number, in the range 2,000 to 2,999.

*mib-view view-name:* Specifies the MIB view name associated with *community-name*, where *view-name* represents the MIB view name, a string of 1 to 32 characters. If no keyword is specified, the default view is ViewDefault (The view created by the system after SNMP agent is enabled).

**Description** Use the **snmp-agent community** command to configure a new SNMP community. Parameters to be configured include access right, community name, ACL, and accessible MIB views.

Use the **undo snmp-agent community** command to delete a specified community.

The community name configured with this command is only valid for the SNMP v1 and v2c agent.

**Examples** # Configure a community with the name of **comaccess** that has read-only access right.

```
<Sysname> system-view
[Sysname] snmp-agent community read comaccess
```

# Delete the community **comaccess**.

```
<Sysname> system-view
[Sysname] undo snmp-agent community comaccess
```

---

## snmp-agent group

**Syntax** The following syntax applies to SNMPv1 and SNMP v2c:

```
snmp-agent group { v1 | v2c } group-name [read-view read-view]
[write-view write-view] [notify-view notify-view] [acl acl-number]
```

```
undo snmp-agent group { v1 | v2c } group-name
```

The following syntax applies to SNMPv3:

```
snmp-agent group v3 group-name [authentication | privacy] [read-view
read-view] [write-view write-view] [notify-view notify-view] [acl
acl-number]
```

```
undo snmp-agent group v3 group-name [authentication | privacy]
```

**View** System view

- Parameters**
- v1:** SNMPv1.
  - v2c:** SNMPv2c.
  - v3:** SNMPv3.
  - group-name:* Group name, a string of 1 to 32 characters.
  - authentication:** Specifies the security model of the SNMP group to be authentication only (without privacy).
  - privacy:** Specifies the security model of the SNMP group to be authentication and privacy.
  - read-view** *read-view:* Read view, a string of 1 to 32 characters.
  - write-view** *write-view:* Write view, a string of 1 to 32 characters.
  - notify-view** *notify-view:* Notify view, for sending Trap messages, a string of 1 to 32 characters.
  - acl** *acl-number:* Specifies an ACL by its number, in the range 2000 to 2999.

- Description**
- Use the **snmp-agent group** command to configure a new SNMP group and specify its access right.
  - Use the **undo snmp-agent group** command to delete a specified SNMP group.
  - By default, SNMP groups configured by the **snmp-agent group v3** command use a no-authentication-no-privacy security model.

**Related commands:** **snmp-agent mib-view**, **snmp-agent usm-user v3**.

- Examples**
- ```
# Create an SNMP group group1 on an SNMPv3 enabled device, no
authentication, no privacy.
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

snmp-agent local-switch fabricid

- Syntax** **snmp-agent local-switch fabricid** *switch fabricid*
undo snmp-agent local-switch fabricid

View System view

- Parameters** *switch fabricid:* Engine ID, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

- Description** Use the **snmp-agent local-switch fabricid** command to configure a local switch fabric ID for an SNMP entity.
- Use the **undo snmp-agent local-switch fabricid** command to restore the default.
- By default, the switch fabric ID of a device is the combination of company ID and device ID. Device ID varies by product; it could be an IP address, a MAC address, or a self-defined string of hexadecimal numbers.
- Notice that if the newly configured switch fabric ID is not the same as the one used for creating the USM user, the user is invalid.

Related commands: **snmp-agent usm-user { v1 | v2c }, snmp-agent usm-user v3.**

Examples # Configure the local switch fabric ID as **123456789A**.

```
<Sysname> system-view
[Sysname] snmp-agent local-switch fabricid 123456789A
```

snmp-agent log

- Syntax** **snmp-agent log { all | get-operation | set-operation }**
- undo snmp-agent log { all | get-operation | set-operation }**
- View** System view
- Parameters** **all:** Enables logging of SNMP GET and SET operations.
- get-operation:** Enables logging of SNMP GET operation.
- set-operation:** Enables logging of SNMP SET operation.
- Description** Use the **snmp-agent log** command to enable SNMP logging.
- Use the **undo snmp-agent log** command to restore the default.
- By default, SNMP logging is disabled.
- If a specified SNMP logging is enabled, when NMS performs a specified operation to SNMP Agent, the latter records the operation-related information and saves it to the information center.
- Examples** # Enable logging of SNMP GET operation.
- ```
<Sysname> system-view
[Sysname] snmp-agent log get-operation
```
- # Enable logging of SNMP SET operation.

```
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

---

## snmp-agent mib-view

**Syntax** **snmp-agent mib-view** { **excluded** | **included** } *view-name* *oid-tree* [ **mask** *mask-value* ]

**undo snmp-agent mib-view** *view-name*

**View** System view

**Parameters** **excluded**: Indicates that not all nodes of the MIB tree are included in current view.

**included**: Indicates that all nodes of the MIB tree are included in current view.

*view-name*: View name, a string of 1 to 32 characters.

*oid-tree*: MIB subtree. It can only be an OID string, such as 1.4.5.3.1, or an object name string, such as "system". OID is made up of a series of integers, which marks the position of the node in the MIB tree and uniquely identifies a MIB object.

**mask** *mask-value*: Mask for an object tree, in the range 1 to 32 hexadecimal digits. It must be an even digit.

**Description** Use the **snmp-agent mib-view** command to create or update MIB view information so that MIB objects can be specified.

Use the **undo snmp-agent mib-view** command to delete the current configuration.

By default, MIB view name is ViewDefault.

You can use the **display snmp-agent mib-view** command to view the access right of the default view. Also, you can use the **undo snmp-agent mib-view** command to remove the default view, after that, however, you may not be able to read or write all MIB nodes on Agent.

**Related commands:** **snmp-agent group**.

**Examples** # Create a MIB view **mibtest**, which includes all objects of the subtree **mib-2**.

```
<Sysname> system-view
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1
```

---

## snmp-agent packet max-size

**Syntax** **snmp-agent packet max-size** *byte-count*

**undo snmp-agent packet max-size**

<b>View</b>	System view
<b>Parameters</b>	<i>byte-count</i> : Maximum number of bytes of an SNMP packet that can be received or sent by an agent, in the range 484 to 17,940. The default value is 1,500 bytes.
<b>Description</b>	Use the <b>snmp-agent packet max-size</b> command to configure the maximum number of bytes in an SNMP packet that can be received or sent by an agent.  Use the <b>undo snmp-agent packet max-size</b> command to restore the default packet size.
<b>Examples</b>	# Configure the maximum number of bytes that can be received or sent by an SNMP agent as 1,042 bytes.  <pre>&lt;Sysname&gt; system-view [Sysname] snmp-agent packet max-size 1042</pre>

---

## snmp-agent sys-info

<b>Syntax</b>	<b>snmp-agent sys-info</b> { <b>contact</b> <i>sys-contact</i>   <b>location</b> <i>sys-location</i>   <b>version</b> { <b>all</b>   { <b>v1</b>   <b>v2c</b>   <b>v3</b> }* } }
	<b>undo snmp-agent sys-info</b> { <b>contact</b>   <b>location</b>   <b>version</b> { <b>all</b>   { <b>v1</b>   <b>v2c</b>   <b>v3</b> }* } }
<b>View</b>	System view
<b>Parameters</b>	<b>contact</b> <i>sys-contact</i> : A string of 1 to 200 characters that describes the contact information for system maintenance.  <b>location</b> <i>sys-location</i> : A string of 1 to 200 characters that describes the location of the device.  <b>version</b> : The SNMP version in use. <ul style="list-style-type: none"> <li>■ <b>all</b>: Specifies SNMPv1, SNMPv2c, and SNMPv3.</li> <li>■ <b>v1</b>: SNMPv1.</li> <li>■ <b>v2c</b>: SNMPv2c.</li> <li>■ <b>v3</b>: SNMPv3.</li> </ul>
<b>Description</b>	Use the <b>snmp-agent sys-info</b> command to configure system information, including the contact information, and the location, and enable the specified SNMP version.  Use the <b>undo snmp-agent sys-info</b> command to restore the default system information and disable the specified SNMP version.  By default, the location information is Marlborough, MA, version is SNMPv3, and the contact is Hangzhou 3Com Technologies Co., Ltd.



**Related commands:** **display snmp-agent sys-info.**



Network maintenance switch fabricers can use the system contact information to get in touch with the manufacturer in case of network failures. The system location information is a management variable under the system branch as defined in RFC1213-MIB, it identifies the location of the managed object.

**Examples** # Configure the contact information as "Dial System Operator at beeper # 27345".

```
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator at beeper # 27345
```

## snmp-agent target-host

**Syntax** **snmp-agent target-host trap address udp-domain** { *ip-address* | **ipv6** *ipv6-address* } [ **udp-port** *port-number* ] [ **vpn-instance** *vpn-instance-name* ]  
**params securityname** *security-string* [ **v1** | **v2c** | **v3** [ **authentication** | **privacy** ] ]

**undo snmp-agent target-host** { *ip-address* | **ipv6** *ipv6-address* } **securityname** *security-string* [ **vpn-instance** *vpn-instance-name* ]

**View** System view

**Parameters** **trap**: Specifies the host to be the Trap host.

**address**: Specifies the IP address of the target host for the SNMP messages.

**udp-domain**: Indicates that the Trap message is transmitted using UDP.

*ip-address*: The IPv4 address of the Trap host.

**ipv6** *ipv6-address*: Specifies that the target host that receives Trap messages uses the IPv6 address.

**vpn-instance** *vpn-instance-name*: Specifies the VPN where the host receiving Traps reside, where *vpn-instance-name* indicates the VPN instance name and is a string of 1 to 31 characters. It is case sensitive and is applicable only in a network supporting IPv4.

**udp-port** *port-number*: Specifies the number of the port that receives Trap messages.

**params securityname** *security-string*: Specifies authentication related parameters, which is SNMPv1 or SNMPv2c community name or an SNMPv3 user name, a string of 1 to 32 characters.

**v1**: SNMPv1.

**v2c**: SNMPv2c.

**v3**: SNMPv3.

**authentication:** Specifies the security model to be authentication without privacy.

**privacy:** Specifies the security model to be authentication with privacy.

**Description** Use the **snmp-agent target-host** command to configure the related settings for a Trap target host.

Use the **undo snmp-agent target-host** command to remove the current settings.

To enable the device to send Traps, you need to use the **snmp-agent target-host** command in combination with the **snmp-agent trap enable** and the **enable snmp trap updown** commands.

**Related commands:** **enable snmp trap updown, snmp-agent trap enable, snmp-agent trap source, snmp-agent trap life.**

**Examples** # Enable the device to send SNMP Traps to 10.1.1.1, using the community name of **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
```

# Enable the device to send SNMP Traps to the device which is in VPN 1 and has an IP address of 10.1.1.1, using the community name of **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 vpn-instance vpn1 params securityname public
```

---

## snmp-agent trap enable

**Syntax** **snmp-agent trap enable** [ **bgp** | **configuration** | **flash** | **ospf** [ *process-id* ] [ *ospf-trap-list* ] | **standard** [ **authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart** ]\* | **system** | **vrrp** [ **authfailure** | **newmaster** ] ]

**undo snmp-agent trap enable** [ **bgp** | **configuration** | **flash** | **ospf** [ *process-id* ] [ *ospf-trap-list* ] | **standard** [ **authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart** ]\* | **system** | **vrrp** [ **authfailure** | **newmaster** ] ]

**View** System view

**Parameters** **bgp:** Enables the sending of BGP Trap messages.

**configuration:** Enables the sending of configuration Trap messages.

**flash:** Enables the sending of FLASH Trap messages.

**ospf** [ *process-id* ] [ *ospf-trap-list* ]: Enables the sending of OSPF Trap messages. The parameter *process-id* is the process ID and *spf-trap-list* is the Trap packet list.

**standard:** Enables the sending of standard Trap messages.

- **authentication:** Enables the sending of authentication failure Trap messages in the event of authentication failure.
- **coldstart:** Sends coldstart Trap messages when the device restarts.
- **linkdown:** Sends linkdown Trap messages when the port is in a linkdown status. It should be configured globally.
- **linkup:** Sends linkup Trap messages when the port is in a linkup status. It should be configured globally.
- **warmstart:** Sends warmstart Trap messages when the SNMP restarts.

**system:** Sends 3Com-SYS-MAN-MIB (a private MIB) Trap messages.

**vrrp [ authfailure | newmaster ]:** Sends VRRP Trap messages.

- **authfailure:** Sends authentication failure VRRP Trap messages.
- **newmaster:** Enables the sending of VRRP newmaster Trap messages when the device becomes the Master.

**Description** Use the **snmp-agent trap enable** command to enable the device to send Trap messages globally.

Use the **undo snmp-agent trap enable** command to disable the device from sending Trap messages.

By default, the device is enabled to send all types of Trap messages.

Note that:

To enable an interface to send SNMP Traps when its state changes, you need to enable the Link up/down Trap packet transmission function on an interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable [ standard [ linkdown | linkup ] \* ]** command to enable this function globally.

**Related commands:** **snmp-agent target-host, enable snmp trap updown.**

**Examples** # Enable the device to send SNMP authentication failure packets to 10.1.1.1, using the community name of **public**.

```
<Sysname> system-view
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
[Sysname] snmp-agent trap enable standard authentication
```

---

## snmp-agent trap if-mib link extended

**Syntax** **snmp-agent trap if-mib link extended**

**undo snmp-agent trap if-mib link extended**

<b>View</b>	System view
<b>Parameters</b>	None
<b>Description</b>	<p>Use the <b>snmp-agent trap if-mib link extended</b> command to extend the standard linkUp/linkDown Trap messages defined in RFC. The extended linkUp/linkDown Trap messages comprise the standard linkUp/linkDown Trap messages defined in RFC plus interface description and interface type.</p> <p>Use the <b>undo snmp-agent trap if-mib link extended</b> command to restore the default.</p> <p>By default, standard linkUp/linkDown Trap messages defined in RFC are used.</p> <p>Note that after this command is configured, the device sends extended linkUp/linkDown Trap messages. If the extended messages are not supported on NMS, the device may not be able to resolute the messages.</p>
<b>Examples</b>	<p># Extend standard linkUp/linkDown Trap messages defined in RFC.</p> <pre>&lt;Sysname&gt; system-view [Sysname] snmp-agent trap if-mib link extended</pre>

---

## snmp-agent trap life

<b>Syntax</b>	<p><b>snmp-agent trap life</b> <i>seconds</i></p> <p><b>undo snmp-agent trap life</b></p>
<b>View</b>	System view
<b>Parameters</b>	<i>seconds</i> : Time-out time, in the range 1 to 2,592,000 seconds.
<b>Description</b>	<p>Use the <b>snmp-agent trap life</b> command to configure the life time for Traps, which will be discarded when their life time expires.</p> <p>Use the <b>undo snmp-agent trap life</b> command to restore the default life time for Trap messages.</p> <p>By default, the life time for SNMP Traps is 120 seconds.</p>
<b>Related commands:</b>	<b>snmp-agent trap enable, snmp-agent target-host.</b>
<b>Examples</b>	<p># Configure the life time for Trap messages as 60 seconds.</p> <pre>&lt;Sysname&gt; system-view [Sysname] snmp-agent trap life 60</pre>

---

## snmp-agent trap queue-size

**Syntax** **snmp-agent trap queue-size** *size*  
**undo snmp-agent trap queue-size**

**View** System view

**Parameters** *size*: The queue size for the Trap messages, in the range 1 to 1,000.

**Description** Use the **snmp-agent trap queue-size** command to configure the size of the Trap queue.

Use the **undo snmp-agent trap queue-size** command to restore the default queue size.

By default, up to 100 Trap messages can be stored in the Trap queue.

**Related commands:** **snmp-agent trap enable**, **snmp-agent target-host**, **snmp-agent trap life**.

**Examples** # Configure the size of the Trap queue as 200.  

```
<Sysname> system-view
[Sysname] snmp-agent trap queue-size 200
```

---

## snmp-agent trap source

**Syntax** **snmp-agent trap source** *interface-type interface-number*  
**undo snmp-agent trap source**

**View** System view

**Parameters** *interface-type interface-number*: Specifies the interface type and interface number.

**Description** Use the **snmp-agent trap source** command to specify the source IP address contained in the Trap message.

Use the **undo snmp-agent trap source** command to restore the default.

By default, SNMP chooses the IP address of an interface to be the source IP address of the Trap message.

Use this command to trace a specific event by the source IP address of a Trap message.

Note: Before you can configure the IP address of a particular interface as the source IP address of the Trap message, ensure that the interface already exists and

that it has a legal IP address. Otherwise, it is likely that the configurations will either fail or be invalid.

**Related commands:** **snmp-agent trap enable, snmp-agent target-host.**

**Examples** # Configure the IP address for the port VLAN-interface 1 as the source address for Trap messages.

```
<Sysname> system-view
[Sysname] snmp-agent trap source Vlan-interface 1
```

## snmp-agent usm-user { v1 | v2c }

**Syntax** **snmp-agent usm-user { v1 | v2c } user-name group-name [ acl acl-number ]**

**undo snmp-agent usm-user { v1 | v2c } user-name group-name**

**View** System view

**Parameters** **v1:** SNMPv1.

**v2c:** SNMPv2c.

*user-name:* User name, a string of 1 to 32 characters. It is case sensitive.

*group-name:* Group name, a string of 1 to 32 characters. It is case sensitive.

**acl** *acl-number:* Basic ACL, in the range 2,000 to 2,999.

**Description** Use the **snmp-agent usm-user { v1 | v2c }** command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user { v1 | v2c }** command to delete a user from an SNMP group.

Execution of this command means adding of a new SNMP group.

**Related commands:** **snmp-agent group, snmp-agent community, snmp-agent usm-user v3.**

**Examples** # Create a read community **readCom**.

```
<Sysname> system-view
[Sysname] snmp-agent community read readCom
```

# Create a v2c usm user **userV2c** based on the created **readCom**.

```
[Sysname] snmp-agent usm-user v2c userV2c readCom
```

---

**snmp-agent usm-user v3**

**Syntax** **snmp-agent usm-user v3** *user-name group-name* [ [ **cipher** ] **authentication-mode** { **md5** | **sha** } *auth-password* [ **privacy-mode** { **des56** | **aes128** } *priv-password* ] ] [ **acl** *acl-number* ]

**undo snmp-agent usm-user v3** *user-name group-name* { **local** | **switch fabricid** *switch fabricid-string* }

**View** System view

**Parameters** *user-name*: User name, a string of 1 to 32 characters. It is case sensitive.

*group-name*: Group name, a string of 1 to 32 characters. It is case sensitive.

**cipher**: Specifies that *auth-password* and *priv-password* are cipher text passwords.

**authentication-mode**: Specifies the security model to be authentication.

- **md5**: Specifies the authentication protocol to be HMAC-MD5-96.
- **sha**: Specifies the authentication protocol to be HMAC-SHA-96.

*auth-password*: Authentication password. If the **cipher** keyword is not specified, *auth-password* indicates a plain text password, which is a string of 1 to 64 visible characters. If the **cipher** keyword is specified, *auth-password* indicates a cipher text password. If the **md5** keyword is specified, *auth-password* is a string of 32 hexadecimal characters. If the **sha** keyword is specified, *auth-password* is a string of 40 hexadecimal characters.

**privacy-mode**: Specifies the security model to be privacy.

- **des56**: Specifies the privacy protocol to be data encryption standard (DES).
- **aes128**: Specifies the privacy protocol to be advanced encryption standard (AES).

*priv-password*: The privacy password. If the **cipher** keyword is not specified, *priv-password* indicates a plain text password, which is a string of 1 to 64 characters. If the **cipher** keyword is specified, *priv-password* indicates a cipher text password. If the **md5** keyword is specified, *priv-password* is a string of 32 hexadecimal characters. If the **sha** keyword is specified, *priv-password* is a string of 40 hexadecimal characters.

**acl** *acl-number*: Basic ACL, in the range 2,000 to 2,999.

**local**: Represents a local SNMP entity user.

**switch fabricid** *switch fabricid-string*: The switch fabric ID string, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

**Description** Use the **snmp-agent usm-user v3** command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user v3** command to delete a user from an SNMP group.

- If you specify the **cipher** keyword, the system considers the arguments *auth-password* and *priv-password* as cipher text passwords. In this case, the command supports copy and paste, meaning if the switch fabric IDs of the two devices are the same, you can copy and paste the SNMPv3 configuration commands in the configuration file on device A to device B and execute the commands on device B. The cipher text password and plain text password on the two devices are the same.
- If you do not specify the **cipher** keyword, the system considers the arguments *auth-password* and *priv-password* as plain text passwords. In this case, if you perform the copy and paste operation, the system will encrypt these two passwords, resulting in inconsistency of the cipher text and plain text passwords of the two devices.

Note that:

- If you use the **snmp-agent usm-user v3 cipher** command, the *priv-password* argument in this command can be obtained by the **snmp-agent calculate-password** command. To make the calculated cipher text password applicable to the **snmp-agent usm-user v3 cipher** command and have the same effect as that in the **snmp-agent usm-user v3 cipher** command, ensure that the same privacy protocol is specified for the two commands and the local switch fabric ID specified in the **snmp-agent usm-user v3 cipher** command is consistent with the SNMP entity switch fabric ID specified in the **snmp-agent calculate-password** command.
- If you execute the command without specifying the **cipher** keyword, the **display current-configuration | include snmp** command displays garbled characters of the cipher text password; if you execute the command with the **cipher** keyword specified, the **display current-configuration | include snmp** command displays the cipher text password.
- If you execute this command repeatedly to configure the same user, the last configuration takes effect.

**Related commands:** **snmp-agent calculate-password**, **snmp-agent group**, **snmp-agent usm-user { v1 | v2c }**.

**Examples** # Add a user **testUser** to the SNMPv3 group **testGroup**. Configure the security model as **authentication**, the authentication protocol as MD5, the privacy protocol as DES56, the authentication plain text password as **authkey**, and the authentication cipher text password as **prikey**.

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey privacy-mode des56 prikey
```

# Add a user **testUser** to the SNMPv3 group **testGroup** with the **cipher** keyword specified. Configure the security model as **authentication and privacy**, the authentication protocol as MD5, the privacy protocol as DES56, the authentication plain text password as **authkey**, and the authentication cipher text password as **prikey**



```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode md5 local-switch fabricid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
[Sysname] snmp-agent calculate-password prikey mode md5 local-switch fabricid
The secret key is: 800D7F26E786C4BECE61BF01E0A22705
[Sysname] snmp-agent usm-user v3 testUser testGroup cipher authentication-mode md5
09659EC5A9AE91BA189E5845E1DDE0CC privacy-mode des56 800D7F26E786C4BECE61BF01E0A22705
```



# 75

## RMON CONFIGURATION COMMANDS

---

### display rmon alarm

**Syntax** `display rmon alarm [ entry-number ]`

**View** Any view

**Parameters** *entry-number*: Index of an RMON alarm entry, in the range 1 to 65535. If no entry is specified, the configuration of all alarm entries is displayed.

**Description** Use the **display rmon alarm** command to display the configuration of the specified or all RMON alarm entries.

**Related commands:** **rmon alarm.**

**Examples** # Display the configuration of all RMON alarm table entries.

```
<Sysname> display rmon alarm
Alarm table 1 owned by user1 is VALID.
 Samples type : absolute
 Variable formula : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
 Sampling interval : 10(sec)
 Rising threshold : 50(linked with event 1)
 Falling threshold : 5(linked with event 2)
 When startup enables : risingOrFallingAlarm
 Latest value : 0
```

**Table 250** Field descriptions of the display rmon alarm command

Field	Description
Alarm table	Alarm entry index, 1 in this example
owned by	Owner of the entry, user1 in this example
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry and with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.)
Samples type	The sampling type (absolute in this example)
Variable formula	Formula for the sampling value
Sampling interval	Sampling interval
Rising threshold	Alarm rising threshold (When the sampling value is bigger than or equal to this threshold, a rising alarm is triggered.)
Falling threshold	Alarm falling threshold (When the sampling value is smaller than or equal to this threshold, a falling alarm is triggered.)
When startup enables	How an alarm can be triggered

**Table 250** Field descriptions of the display rmon alarm command

Field	Description
Latest value	The last sampled value

---

## display rmon event

**Syntax** **display rmon event** [ *entry-number* ]

**View** Any view

**Parameters** *entry-number*: Index of an RMON event entry, in the range 1 to 65535. If no entry is specified, the configuration of all event entries is displayed.

**Description** Use the **display rmon event** command to display the configuration of the specified or all RMON event entries.

Displayed information includes event index, event owner, event description, action triggered by the event (such as sending log or trap messages), and last time the event occurred (the elapsed time since system initialization/startup) in seconds.

**Related commands:** **rmon event**.

**Examples** # Display the configuration of RMON event table.

```
<Sysname> display rmon event
Event table 1 owned by user1 is VALID.
 Description: null.
 Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

**Table 251** Field descriptions of the display rmon event command

Field	Description
Event table	Event entry number
owned by	Owner of the entry
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry and with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.)
Description	Description for the event
cause log-trap when triggered	The event will trigger logging and trapping.
last triggered at	Last time the event was triggered

---

## display rmon eventlog

**Syntax** **display rmon eventlog** [ *entry-number* ]

**View** Any view

**Parameters** *entry-number*: Index of an event entry, in the range 1 to 65535. If no entry number is specified, the log information for all event entries is displayed.

**Description** Use the **display rmon eventlog** command to display log information for the specified or all event entries.

If you use the **rmon event** command to specify that the action of an entry includes logging, then when this event is triggered, the event log is retained in the RMON log list. You can use the **display rmon eventlog** command to display detailed log information including event index, current event state, time the event was logged (the elapsed time in seconds since system initialization/startup), and event description.

**Examples** # Display the RMON log information for event entry 1.

```
<Sysname> display rmon eventlog 1
Event table 1 owned by user1 is VALID.
Generates eventLog 1.1 at 0days 00h:01m:39s.
Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
Generates eventLog 1.2 at 0days 00h:02m:27s.
Description: The alarm formula defined in private alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
```

**Table 252** Field descriptions of the display rmon eventlog command

Field	Description
Event table	Event index
owned by	Owner of the entry
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry and with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.)
Generates eventLog at	Time the log was created
Description	Log description

---

## display rmon history

**Syntax** **display rmon history** [ *interface-type interface-number* ]

**View** Any view

**Parameters** *interface-type interface-number*: Specifies a port by its type and number.

**Description** Use the **display rmon history** command to display RMON history control entry and last history sampling information, including bandwidth utilization, number of bad packets, and total packet number.

**Related commands:** **rmon history**.

**Examples** # Display RMON history entry information for interface Ethernet 2/0/1.

```

<Sysname> display rmon history Ethernet 2/0/1
History control entry 1 owned by user1 is VALID
 Samples interface : Ethernet 2/0/1<ifEntry.642>
 Sampling interval : 10(sec) with 10 buckets max
 Latest sampled values :
 Dropevents :0 , octets :0
 packets :0 , broadcast packets :0
 multicast packets :0 , CRC alignment errors :0
 undersize packets :0 , oversize packets :0
 fragments :0 , jabbers :0
 collisions :0 , utilization :0

```

**Table 253** Field descriptions of the display rmon history command

Field	Description
History control entry	Index of the history control entry for the interface, 1 in this example
owned by	Owner of the entry
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry and with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.)
Samples Interface	The sampled interface
Sampling interval	Sampling interval
buckets max	History table size for the entry, if the specified value of the <b>buckets</b> argument exceeds the history table size supported by the device the latter is displayed.
Latest sampled values	The latest sampled values
Dropevents	Dropped packets during the sampling period
octets	Number of octets received during the sampling period
packets	Number of packets received during the sampling period
broadcastpackets	Number of broadcasts received during the sampling period
multicastpackets	Number of multicasts received during the sampling period
CRC alignment errors	Number of packets received with CRC alignment errors during the sampling period
undersize packets	Number of undersize packets received during the sampling period
oversize packets	Number of oversize packets received during the sampling period
fragments	Number of fragments received during the sampling period
jabbers	Number of jabbers received during the sampling period
collisions	Number of colliding packets received during the sampling period
utilization	Bandwidth utilization during the sampling period

---

## display rmon prialarm

**Syntax** **display rmon prialarm** [ *entry-number* ]

**View** Any view

**Parameters** *entry-number*: Private alarm entry index, in the range 1 to 65535. If no entry is specified, the configuration of all private alarm entries is displayed.

**Description** Use the **display rmon prialarm** command to display the configuration of the specified or all private alarm entries.

**Related commands:** **rmon prialarm.**

**Examples** # Display the configuration of all private alarm entries.

```
<Sysname> display rmon prialarm
Prialarm table 5 owned by user1 is UNDERCREATION.
 Samples type : changeratio
 Variable formula : ((.1.3.6.1.2.1.16.1.1.1.5.1-.1.3.6.1.2.1.16.1.1.1.6.1)*100/.1.3.6.1.2.1.16.1.1.1.5.1)
 Description : ifUtilization. Ethernet 2/0/1
 Sampling interval : 10(sec)
 Rising threshold : 892340484(linked with event 1)
 Falling threshold : 889783312(linked with event 2)
 When startup enables : risingOrFallingAlarm
 This entry will exist : forever
 Latest value : 0
```

**Table 254** Field descriptions of the display rmon prialarm command

Field	Description
Prialarm table	Index of the prialarm table
owned by	Owner of the entry, user1 in this example
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry and with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.)
Samples type	Samples type
Variable formula	Variable formula
Sampling interval	Sampling interval
Rising threshold	Alarm rising threshold. An alarm event is triggered when the sampled value is greater than or equal to this threshold.
Falling threshold	Alarm falling threshold. An alarm event is triggered when the sampled value is less than or equal to this threshold.
linked with event	Event index associated with the prialarm
When startup enables	How can an alarm be triggered
This entry will exist	The lifetime of the entry, which can be forever or span the specified period
Latest value	The last sampled value

## display rmon statistics

**Syntax** **display rmon statistics** [ *interface-type interface-number* ]

**View** Any view

**Parameters** *interface-type interface-number*: Specifies a port by its type and number.

**Description** Use the **display rmon statistics** command to display RMON statistics.

**Related commands:** **rmon statistics.**

**Examples** # Display RMON statistics for interface Ethernet 3/0/3.

```

<Sysname> display rmon statistics Ethernet 3/0/3
Statistics entry 6 owned by aa is VALID.
 Interface : Ethernet3/0/3<ifIndex.5>
 etherStatsOctets : 0 , etherStatsPkts : 0
 etherStatsBroadcastPkts : 0 , etherStatsMulticastPkts : 0
 etherStatsUndersizePkts : 0 , etherStatsOversizePkts : 0
 etherStatsFragments : 0 , etherStatsJabbers : 0
 etherStatsCRCAlignErrors : 0 , etherStatsCollisions : 0
 etherStatsDropEvents (insufficient resources): 0
 Packets received according to length:
 64 : 0 , 65-127 : 0 , 128-255 : 0
 256-511: 0 , 512-1023: 0 , 1024-1518: 0

```

**Table 255** Field descriptions of the display rmon statistics command

Field	Description
Statistics entry	Statistics table entry index
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry and with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.)
Interface	Interface on which statistics are gathered
etherStatsOctets	Number of octets received by the interface during the statistical period
etherStatsPkts	Number of packets received by the interface during the statistical period
etherStatsBroadcastPkts	Number of broadcast packets received by the interface during the statistical period
etherStatsMulticastPkts	Number of multicast packets received by the interface during the statistical period
etherStatsUndersizePkts	Number of undersize packets received by the interface during the statistical period
etherStatsOversizePkts	Number of oversize packets received by the interface during the statistical period
etherStatsFragments	Number of undersize packets with CRC errors received by the interface during the statistical period
etherStatsJabbers	Number of oversize packets with CRC errors received by the interface during the statistical period
etherStatsCRCAlignErrors	Number of packets with CRC errors received on the interface during the statistical period
etherStatsCollisions	Number of collisions received on the interface during the statistical period
etherStatsDropEvents	Total number of drop events received on the interface during the statistical period
Packets received according to length:	Statistics of packets received according to length during the statistical period



---

**rmon alarm**

**Syntax** **rmon alarm** *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [ **owner text** ]

**undo rmon alarm** *entry-number*

**View** System view

**Parameters** *entry-number*: Alarm entry index, in the range 1 to 65535.

*alarm-variable*: Alarm variable, a string of 1 to 256 characters. It can be in dotted object identifier (OID) format, such as 1.3.6.1.2.1.2.1.10.1 or a node name (such as ifInOctets.1). Only variables that can be parsed into INTEGER (INTEGER, Counter, Gauge, or Time Ticks) in the ASN.1 can be used for the *alarm-variable* argument.

*sampling-interval*: Sampling interval, in the range 5 to 65,535 seconds.

**absolute**: Sets the sampling type to **absolute**.

**delta**: Sets the sampling type to **delta**.

**rising-threshold** *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range -2,147,483,648 to +2,147,483,647, and *event-entry 1* represents the index of the event triggered when the rising threshold is reached. It ranges from 0 to 65,535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

**falling-threshold** *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range -2,147,483,648 to +2,147,483,647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. It ranges from 1 to 65,535.

**owner text**: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

**Description** Use the **rmon alarm** command to create an entry in the RMON alarm table.

Use the **undo rmon alarm** command to remove a specified entry from the RMON alarm table.

This command defines alarms. The generation and notification of an alarm however, is controlled by the event entry associated with it.

The following is how the system handles alarm entries:

- 1 Samples the alarm variables at the specified interval.
- 2 Compares the sampled values with the predefined threshold and does the following:

- 3 If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
- 4 If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.



- Before creating an alarm entry, define the events to be referenced in the event table with the **rmon event** command.
- When you create an entry, if the values of the specified alarm variable (*alarm-variable*), sampling interval (*sampling-interval*), sampling type (**absolute** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) are identical to those of the existing alarm entry, the system considers their configurations the same and the creation fails.
- You can create up to 60 alarm entries.
- The rising alarm and falling alarm are alternate.

**Examples** # Add entry 1 in the alarm table and sample the node 1.3.6.1.2.1.16.1.1.1.4.1 at a sampling interval of 10 seconds in absolute sampling type. Generate event 1 when the sampled value is greater than or equal to the rising threshold of 50, and event 2 when the sampled value is lower than or equal to the falling threshold of 5. Set the owner of the entry to be **user1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet 2/0/1] rmon statistics 1
[Sysname-Ethernet 2/0/1] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising_t
hreshold 50 1 falling_threshold 5 2 owner user1
```

# Remove the alarm table entry with the index of 15.

```
<Sysname> system-view
[Sysname] undo rmon alarm 15
```

---

## rmon event

**Syntax** **rmon event** *entry-number* [ **description** *string* ] { **log** | **log-trap** *log-trapcommunity* | **none** | **trap** *trap-community* } [ **owner** *text* ]

**undo rmon event** *entry-number*

**View** System view

**Parameters** *entry-number*: Event entry index, in the range 1 to 65,535.

**description** *string*: Event description, a string of 1 to 127 characters.

**log**: Logs the event when it occurs.

**log-trap** *log-trapcommunity*: Log and trap events. The system performs both logging and trap sending when the event occurs. *log-trapcommunity* indicates the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

**none**: Performs no action when the event occurs.

**trap** *trap-community*: Trap event. The system sends a trap with the community name being *trap-community* when the event occurs. *trap-community* represents network management station community to which traps are sent, a string of 1 to 127 characters.

**owner** *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

**Description** Use the **rmon event** command to create an entry in the RMON event table.

Use the **undo rmon event** command to remove a specified entry from the RMON event table.

When an event is triggered by its associated alarm in the alarm table, the event group allows you to log it, send a trap, do both, or do neither at all. This helps control the generation and notification of events.



- *When you create an entry, if the values of the specified event description (**description** string), event type (**log**, **trap**, **logtrap** or **none**), and community name (*trap-community* or *log-trapcommunity*) are identical to those of the existing event entry, the system considers their configurations the same and the creation fails.*
- *You can create up to 60 alarm entries.*

**Examples** # Create event 10 in the RMON event table.

```
<Sysname> system-view
[Sysname] rmon event 10 log owner user1
```

---

## rmon history

**Syntax** **rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [ **owner** *text* ]

**undo rmon history** *entry-number*

**View** Ethernet port view

**Parameters** *entry-number*: History control entry index, in the range 1 to 65535.

**buckets** *number*: History table size for the entry, in the range 1 to 65,535. The number varies by device.

**interval** *sampling-interval*: Sampling interval, in the range 5 to 3600 seconds.

**owner** *text-string*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

**Description** Use the **rmon history** command to create an entry in the RMON history control table.

Use the **undo rmon history** command to remove a specified entry from the RMON history control table.

This command enables RMON to periodically sample and save for an interface data such as bandwidth utilization, errors, total number of packets for later retrieval.

When you create an entry in the history table, if the specified history table size exceeds that supported by the device, the entry will be created. However, the validated value of the history table size corresponding with the entry is that supported by the device.



- When you create an entry, if the value of the specified sampling interval (**interval** *sampling-interval*) is identical to that of the existing history entry, the system considers their configurations the same and the creation fails.
- You can create up to 100 alarm entries.

**Related commands:** **display rmon history.**

**Examples** # Create RMON history control entry 1 for interface Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet 2/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

# Remove history control entry 15.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet 2/0/1] undo rmon history 15
```

---

## rmon prialarm

**Syntax** **rmon prialarm** *entry-number* *prialarm-formula* *prialarm-des* *sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1* *event-entry1* **falling-threshold** *threshold-value2* *event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [ **owner** *text* ]

**undo rmon prialarm** *entry-number*

**View** System view

**Parameters** *entry-number*: Index of a private alarm entry, in the range 1 to 65535.

*prialarm-formula*: Private alarm variable formula, a string of 1 to 256 characters. The variables in the formula must be represented in OID format that starts with a

point ".", the formula (.1.3.6.1.2.1.2.1.10.1)\*8 for example. You may perform the basic operations of addition, subtraction, multiplication, and division on these variables. The operations should yield a long integer. To prevent errors, make sure that the result of each calculating step falls into the value range for long integers.

*prialarm-des*: Private alarm entry description, a string of 1 to 127 characters.

*sampling-interval*: Sampling interval, in the range 10 to 65,535 seconds.

**absolute | changeratio | delta**: Sets the sampling type to absolute, delta, or change ratio.

**rising-threshold** *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range -2,147,483,648 to +2,147,483,647, and *event-entry 1* represents the index of the event triggered when the rising threshold is reached. It ranges from 0 to 65,535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

**falling-threshold** *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range -2,147,483,648 to +2,147,483,647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. It ranges from 1 to 65,535.

**forever**: Indicates that the lifetime of the private alarm entry is infinite.

**cycle** *cycle-period*: Sets the lifetime period of the private alarm entry, in the range 0 to 2,147,483,647 seconds.

**owner text**: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

**Description** Use the **rmon prialarm** command to create an entry in the private alarm table of RMON.

Use the **undo rmon prialarm** command to remove a private alarm entry from the private alarm table of RMON.

The system handles private alarm entries in the following order:

- 1 Samples the private alarm variables in the private alarm formula at the specified sampling interval.
- 2 Performs calculation on the sampled values with the formula.
- 3 Compares the calculation result with the predefined thresholds and does the following:
- 4 If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
- 5 If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.



- Before creating an alarm entry, define the events to be referenced in the event table with the **rmon event** command.

- When you create an entry, if the values of the specified alarm variable formula (*prialarm-formula*), sampling type (**absolute** **changeratio** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) are identical to those of the existing alarm entry, the system considers their configurations the same and the creation fails.
- You can create up to 50 *pri-alarm* entries.
- The rising alarm and falling alarm are alternate.

**Examples** # Create entry 5 in the private alarm table. Calculate the private alarm variables with the (1.3.6.1.2.1.16.1.1.1.4.1\*100) formula and sample the corresponding variables at intervals of 10 seconds to get the percentage of broadcasts received on Ethernet 2/0/1 in the total packets. When this ratio reaches or is bigger than the rising threshold of 50, trigger event 1; when this ratio reaches or drops under the falling threshold, trigger event 2. Set the lifetime of the entry to forever and owner to **user 1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet 2/0/1] rmon statistics 1
[Sysname-Ethernet 2/0/1] quit
[Sysname] rmon prialarm 5 ((.1.3.6.1.2.1.16.1.1.1.4.1)*100)
Test 10 absolute rising-threshold 50 1 falling-threshold 5 2 entryty
pe forever owner user1
```

# Remove private alarm entry 10.

```
<Sysname> system-view
[Sysname] undo rmon prialarm 10
```

---

## rmon statistics

**Syntax** **rmon statistics** *entry-number* [ **owner text** ]

**undo rmon statistics** *entry-number*

**View** Ethernet port view

**Parameters** *entry-number*: Index of statistics entry, in the range 1 to 65535.

**owner text**: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

**Description** Use the **rmon statistics** command to create an entry in the RMON statistics table.

Use the **undo rmon statistics** command to remove a specified entry from the RMON statistics table.

The RMON statistics group collects information on how a monitored port is being used and records errors. Statistics include number of collisions, CRC alignment

errors, number of undersize or oversize packets, number of broadcasts, number of multicasts, number of bytes received, number of packets received.

To display information for the RMON statistics table, use the **display rmon statistics** command.



- *Only one statistics entry can be created on one interface.*
- *You can create up to 100 statistics entries.*

**Examples** # Create an entry in the RMON statistics table for interface Ethernet 2/0/1. The index of the entry is 20.

```
<Sysname> system-view
[Sysname] interface Ethernet2/0/1
[Sysname-Ethernet2/0/1] rmon statistics 20 owner user1
```

# Remove the entry in the RMON statistics table for interface Ethernet 2/0/1. The index of the entry is 20.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] undo rmon statistics 20
```





# 76

## NTP CONFIGURATION COMMANDS

---

### display ntp-service sessions

**Syntax** display ntp-service sessions [ verbose ]

**View** Any view

**Parameters** **verbose**: Displays the detailed information of all NTP sessions.

**Description** Use the **display ntp-service sessions** command to view the information of all NTP sessions. Without the **verbose** keyword, this command will display only the brief information of all NTP service sessions.

**Examples** # View the brief information of NTP service sessions.

```
<Sysname> display ntp-service sessions
 source reference stra reach poll now offset delay disper

[12345]192.168.0.65 127.127.1.0 2 1 64 - -9.7 18.8 0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```

**Table 256** Field descriptions of the display ntp-service sessions command

Field	Description
source	IP address of the clock source
reference	Reference clock ID of the clock source <ol style="list-style-type: none"><li>1 If the reference clock is the local clock, the value of this field is related to the value of the <b>stra</b> field:</li><li>2 When the value of the <b>stra</b> field is 0 or 1, this field will be "LOCL";</li><li>3 When the <b>stra</b> field has another value, this field will be the IP address of the local clock</li><li>4 If the reference clock is the clock of another device on the network, the value of this field will be the IP address of that device.</li></ol>
stra	Stratum level of the clock source
reach	Reachability count of the clock source. 0 indicates that the clock source is unreachable
poll	Poll interval, namely the maximum interval between successive NTP messages.
now	The length of time in minutes from when the last NTP message was received or when the local clock was last updated to the current time  The time is in second by default. If the time length is greater than 2048 seconds, it is displayed in minute; if greater than 300 minutes, in hour; if greater than 96 hours, in day.

**Table 256** Field descriptions of the display ntp-service sessions command

Field	Description
offset	The offset of the system clock relative to the reference clock, in milliseconds
delay	the roundtrip delay from the local device to the clock source, in milliseconds
disper	The maximum error of the system clock relative to the reference source.
[12345]	1: Clock source selected by the system, namely the current reference source, with a system clock stratum level of ,â§ 15 2: Stratum level of this system source is ,â§ 15 3: This clock source has passed the clock selection process 4: This clock source is a candidate clock source 5: This clock source was created by a configuration command
Total associations	Total number of associations



*When a device is working in the NTP broadcast/multicast server mode, the display ntp-service sessions command executed on the device will not display the NTP session information corresponding to the broadcast/multicast server, but the sessions will be counted in the total number of associations.*

## display ntp-service status

**Syntax** `display ntp-service status`

**View** Any view

**Parameters** None

**Description** Use the **display ntp-service status** command to view the NTP service status information.

**Examples** # View the NTP service status information.

```
<Sysname> display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^17
Clock offset: 0.0000 ms
Root delay: 0.00 ms
Root dispersion: 0.00 ms
Peer dispersion: 0.00 ms
Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

**Table 257** Field descriptions of the display ntp-service status command

Field	Description
Clock status	Status of the system clock

**Table 257** Field descriptions of the display ntp-service status command

Field	Description
Clock stratum	Stratum level of the local clock
Reference clock ID	After the system clock is synchronized to a remote time server or a local reference source, this field indicates the address of the remote time server or the identifier of the local clock source respectively: <ul style="list-style-type: none"> <li>■ When the local clock has a stratum level of 1, the value of this field is "LOCL";</li> <li>■ When the stratum of the local clock has another value, the value of this field is the IP address of the local clock.</li> </ul>
Nominal frequency	The nominal frequency of the local system hardware clock
Actual frequency	The actual frequency of the local system hardware clock
Clock precision	The precision of the system clock
Clock offset	The offset of the system clock relative to the reference source
Root delay	The roundtrip delay from the local device to the primary reference source
Root dispersion	The maximum error of the system clock relative to the primary reference source
Peer dispersion	The maximum error of the system clock relative to the reference source
Reference time	Reference timestamp

---

## display ntp-service trace

**Syntax** `display ntp-service trace`

**View** Any view

**Parameters** None

**Description** Use the **display ntp-service trace** command view the brief information of each NTP server along the NTP server chain from the local device back to the primary reference source.

The **display ntp-service trace** command is available only if the local device can ping through all the devices on the NTP server chain; otherwise, this command will fail to display all the NTP servers on the NTP chain due to timeout.

**Examples** # View the brief information of each NTP server from the local device back to the primary reference source.

```
<Sysname> display ntp-service trace
server 127.0.0.1, stratum 2, offset -0.013500, synch distance 0.03154
server 133.1.1.1, stratum 1, offset -0.506500, synch distance 0.03429
refid LOCL
```

The information above shows an NTP server chain for the server 127.0.0.1: The server 127.0.0.1 is synchronized to the server 133.1.1.1, and the server 133.1.1.1 is synchronized to the local clock source.

**Table 258** Field descriptions of the display ntp-service trace command

Field	Description
server	IP address of the NTP server
stratum	The stratum level of the corresponding system clock
offset	The clock offset relative to the upper-level clock
synch distance	The synchronization distance relative to the upper-level clock
refid	Identifier of the primary reference source. When the stratum level of the primary reference clock is 0, it is displayed as LOCL; otherwise, it is displayed as the IP address of the primary reference clock.

---

## ntp-service access

**Syntax** `ntp-service access { peer | query | server | synchronization } acl-number`

`undo ntp-service access { peer | query | server | synchronization }`

**View** System view

**Parameters** **peer**: Specifies to permit full access.

**query**: Specifies to permit control query.

**server**: Specifies to permit server access and query.

**synchronization**: Specifies to permit server access only.

*acl-number*: Basic ACL number, in the range of 2000 to 2999

**Description** Use the **ntp-service access** command to configure the NTP service access-control right to the local device.

Use the **undo ntp-service access** command to remove the configured NTP service access-control right to the local device.

By default, the local NTP service access-control right is set to **peer**.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will perform an access-control right match and will use the first matched right.



- *The ntp-service access command provides only a minimum degree of security protection. A more secure method is identity authentication.*
- *Before specifying an ACL number in the ntp-service access command, make sure you have already created and configured this ACL.*

**Examples** # Configure devices on the subnet 10.10.0.0/16 to have the full access right to the local device.

```
<Sysname> system-view
[Sysname] acl number 2001
```

```
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ntp-service access peer 2001
```

---

## ntp-service authentication enable

**Syntax** **ntp-service authentication enable**  
**undo ntp-service authentication enable**

**View** System view

**Parameters** None

**Description** Use the **ntp-service authentication enable** command to enable NTP authentication.

Use the **undo ntp-service authentication enable** command to disable NTP authentication.

By default, NTP authentication is disabled.

**Examples** # Enable NTP authentication.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
```

---

## ntp-service authentication-keyid

**Syntax** **ntp-service authentication-keyid** *keyid* authentication-mode md5 *value*  
**undo ntp-service authentication-keyid** *keyid*

**View** System view

**Parameters** *keyid*: Authentication key ID, in the range of 1 to 4294967295.

**authentication-mode md5** *value*: Specifies to use the MD5 algorithm for key authentication, where *value* represents authentication key and is a string of 1 to 32 characters.

**Description** Use the **ntp-service authentication-keyid** command to set the NTP authentication key.

Use the **undo ntp-service authentication-keyid** command to remove the set NTP authentication key.

By default, no NTP authentication key is set.

**CAUTION:**

- Presently the system supports only the MD5 algorithm for key authentication.
- You can set a maximum of 1,024 keys for each device.
- If an NTP authentication key is specified as a trusted key, the key automatically changes to not trusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

**Examples**

# Set an MD5 authentication key, with the key ID of 10 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication-keyid 10 authentication-mode md
5 BetterKey
```

**ntp-service broadcast-client**

**Syntax** ntp-service broadcast-client  
undo ntp-service broadcast-client

**View** VLAN interface view

**Parameters** None

**Description** Use the **ntp-service broadcast-client** command to configure the device to work in the NTP broadcast client mode.

Use the **undo ntp-service broadcast-client** command to remove the device as an NTP broadcast client.

**Examples**

# Configure the device to work in the broadcast client mode and receive NTP broadcast messages on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-client
```

**ntp-service broadcast-server**

**Syntax** ntp-service broadcast-server [ authentication-keyid *keyid* | version *number* ] \*  
undo ntp-service broadcast-server

**View** VLAN interface view

**Parameters** **authentication-keyid** *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

**version number:** Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

**Description** Use the **ntp-service broadcast-server** command to configure the device to work in the NTP broadcast server mode.

Use the **undo ntp-service broadcast-server** command to remove the device as an NTP broadcast server.

**Examples** # Configure the device to work in the broadcast server mode and send NTP broadcast messages on VLAN-interface 1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 3
```

---

## ntp-service in-interface disable

**Syntax** **ntp-service in-interface disable**

undo ntp-service in-interface disable

**View** VLAN interface view

**Parameters** None

**Description** Use the **ntp-service in-interface disable** command to disable an interface from receiving NTP messages.

Use the **undo ntp-service in-interface disable** command to restore the default.

By default, all interfaces are enabled to receive NTP messages.

**Examples** ■ On an Ethernet interface:

# Disable interface Ethernet 2/0/1 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] ntp-service in-interface disable
```

■ On a VLAN interface:

# Disable VLAN-interface 1 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service in-interface disable
```

---

## ntp-service max-dynamic-sessions

- Syntax** `ntp-service max-dynamic-sessions number`  
**undo ntp-service max-dynamic-sessions**
- View** System view
- Parameters** *number*: Maximum number of dynamic NTP sessions that allowed to be established, in the range of 0 to 100.
- Description** Use the **ntp-service max-dynamic-sessions** command to set the maximum number of dynamic NTP sessions that allowed to be established locally.
- Use the **undo ntp-service max-dynamic-sessions** command to restore the maximum number of dynamic NTP sessions to the system default.
- By default, the number is 100.
- Examples** # Set the maximum number of dynamic NTP sessions allowed to be established to 50.
- ```
<Sysname> system-view  
[Sysname] ntp-service max-dynamic-sessions 50
```

ntp-service multicast-client

- Syntax** `ntp-service multicast-client [ip-address]`
undo ntp-service multicast-client [*ip-address*]
- View** VLAN interface view
- Parameters** *ip-address*: Multicast IP address, defaulting to 224.0.1.1. It is in the range 224.0.1.0 to 224.0.1.255.
- Description** Use the **ntp-service multicast-client** command to configure the device to work in the NTP multicast client mode.
- Use the **undo ntp-service multicast-client** command to remove the device as an NTP multicast client.
- Examples** # Configure the device to work in the multicast client mode and receive NTP multicast messages on VLAN 1, and set the multicast address to 224.0.1.1.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```



---

## ntp-service multicast-server

**Syntax** ntp-service multicast-server [ *ip-address* ] [ authentication-keyid *keyid* | ttl *tll-number* | version *number* ] \*

undo ntp-service multicast-server [ *ip-address* ]

**View** VLAN interface view

**Parameters** *ip-address*: Multicast IP address, defaulting to 224.0.1.1. It is in the range 224.0.1.0 to 224.0.1.255.

**authentication-keyid** *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

**tll** *tll-number*: Specifies the TTL of NTP multicast messages, where *tll-number* is in the range of 1 to 255 and defaults to 16.

**version** *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

**Description** Use the **ntp-service multicast-server** command to configure the device to work in the NTP multicast server mode.

Use the **undo ntp-service multicast-server** command to remove the device as an NTP multicast server.

**Examples** # Configure the device to work in the multicast server mode and send NTP multicast messages on VLAN-interface 1 to the multicast address 224.0.1.1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 3 authentication-keyid 4
```

---

## ntp-service refclock-master

**Syntax** ntp-service refclock-master [ *ip-address* ] [ *stratum* ]

undo ntp-service refclock-master [ *ip-address* ]

**View** System view

**Parameters** *ip-address*: IP address of the local clock, which is 127.127.1.u, where u is the NTP process ID, in the range of 0 to 3. If you do not specify *ip-address*, it defaults to 127.127.1.0.

*stratum*: Stratum level of the local clock, in the range of 1 to 15 and defaulting to 8.

**Description** Use the **ntp-service refclock-master** command to configure the local clock as a reference source for other devices.

Use the **undo ntp-service refclock-master** command to remove the local clock as a reference source.



*The stratum level of a clock defines the clock precision. The value range is 1 to 16. The clock precision decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized and cannot be used as a reference clock.*

**Examples** # Specify the local clock as the reference source, with the stratum level of 3.

```
<Sysname> system-view
[Sysname] ntp-service refclock-master 3
```

## ntp-service reliable authentication-keyid

**Syntax** ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

**View** System view

**Parameters** *keyid*: Authentication key number, in the range of 1 to 4294967295.

**Description** Use the **ntp-service reliable authentication-keyid** command to specify that the created authentication key is a trusted key. When NTP authentication enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Use the **ntp-service reliable authentication-keyid** command to remove an authentication key as a trusted key.

No authentication key is configured to be trusted by default.

**Examples** # Enable NTP authentication, specify to use MD5 encryption algorithm, with the key ID of 37 and key value of **BetterKey**, and specify that this key is a trusted key.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
[Sysname] ntp-service reliable authentication-keyid 37
```

## ntp-service source-interface

**Syntax** ntp-service source-interface *interface-type interface-number*

**undo ntp-service source-interface****View** System view**Parameters** *interface-type interface-number*: Specifies an interface by its interface type and interface number.**Description** Use the **ntp-service source-interface** command to specify an interface for sending NTP messages.Use the **undo ntp-service source-interface** command to remove the configured interface for sending NTP messages.

If you do not wish the IP address of a certain interface on the local device to become the destination address of response messages, you can use this command to specify a particular interface for sending all NTP messages, so that the source address in all NTP messages is the primary IP address of this interface.

**Examples** # Specify that all NTP messages are to be sent out from VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service source-interface vlan-interface 1
```

**ntp-service unicast-peer****Syntax** **ntp-service unicast-peer** { *ip-address* | *peer-name* } [ **authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number* ] \***undo ntp-service unicast-peer** { *ip-address* | *peer-name* }**View** System view**Parameters** *ip-address*: IP address of the symmetric-passive peer. It must be a host address, rather than a broadcast address, a multicast address or the IP address of the local clock.*peer-name*: Host name of the symmetric-passive peer, a string of 1 to 20 characters.**authentication-keyid** *keyid*: Specifies the key ID to be used for sending NTP messages to the peer, where *keyid* is in the range of 1 to 4294967295.**priority**: Specifies the peer designated by *ip-address* or *peer-name* as the first choice under the same condition.**source-interface** *interface-type interface-number*: Specifies an interface for sending NTP messages. In an NTP message the local device sends to its peer, the source IP address is the primary IP address of this interface. *interface-type interface-number* represents the interface type and number.

**version number:** Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

**Description** Use the **ntp-service unicast-peer** command to designate a symmetric-passive peer for the device.

Use the **undo ntp-service unicast-peer** command to remove the symmetric-passive peer designated for the device.

No symmetric-passive peer is designated for the device by default.

**Examples** # Designate the device with the IP address of 10.1.1.1 as the symmetric-passive peer of the device, and configure the device to run NTP version 3, and send NTP messages through VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 3 source-interface vlan-interface 1
```

## ntp-service unicast-server

**Syntax** **ntp-service unicast-server** { *ip-address* | *server-name* } [ **authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number* ] \*

**undo ntp-service unicast-server** { *ip-address* | *server-name* }

**View** System view

**Parameters** *ip-address*: IP address of the NTP server. It must be a host address, rather than a broadcast address, a multicast address or the IP address of the local clock.

*server-name*: Host name of the NTP server, a string of 1 to 20 characters.

**authentication-keyid** *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server, where *keyid* is in the range of 1 to 4294967295.

**priority**: Specifies this NTP server as the first choice under the same condition.

**source-interface** *interface-type interface-number*: Specifies an interface for sending NTP messages. In an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface.

*interface-type interface-number* represents the interface type and number.

**version** *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

**Description** Use the **ntp-service unicast-server** command to designate an NTP server for the device.

Use the **undo ntp-service unicast-server** command to remove an NTP server designated for the device.

No NTP server is designated for the device by default.

**Examples** # Designate the device with the IP address of as 10.1.1.1 an NTP server for the device.

```
<Sysname> system-view
[Sysname] ntp-service unicast-server 10.1.1.1 version 3
```



# 77

## DNS CONFIGURATION COMMANDS



*This document only covers IPv4 DNS configuration commands. For introduction to IPv6 DNS configuration commands, refer to "IPv6 Basics Configuration Commands" on page 579.*

---

### display dns domain

**Syntax** `display dns domain [ dynamic ]`

**View** Any view

**Parameters** **dynamic**: Displays the domain name suffixes dynamically obtained through DHCP or other protocols.

**Description** Use the **display dns domain** command to display the domain name suffixes.

**Related commands:** **dns domain**.

**Examples** # Display domain name suffixes.  
`<Sysname> display dns domain`  
Type:  
D:Dynamic S:Static

No.	Type	Domain-name
1	S	com

**Table 259** Description on fields of the display dns domain command

Field	Description
No	Sequence number
Type	Type of domain name suffix: S represents a statically configured domain name suffix, and D represents a domain name suffix obtained dynamically through DHCP.
Domain-name	Domain name suffix

---

### display dns dynamic-host

**Syntax** `display dns dynamic-host`

**View** Any view

**Parameters** None

**Description** Use the **display dns dynamic-host** command to display the information of the dynamic domain name resolution cache.

**Examples** # Display the information of the dynamic domain name resolution cache.

```
<Sysname> display dns dynamic-host
No Host IP Address TTL
1 www.baidu.com 202.108.249.134 63000
2 www.yahoo.akadns.net 66.94.230.39 24
3 www.hotmail.com 207.68.172.239 3585
4 www.eyou.com 61.136.62.70 3591
```

**Table 260** Description on the field of the display dns dynamic-host command

Field	Description
No	Sequence number
Domain-name	Domain name
IP Address	IP address for the corresponding domain name
TTL	Time that a mapping can be stored in the cache (in seconds).



A domain name in the **display dns dynamic-host** command contains 21 characters at most. If a domain name consists of more than 21 characters, only the first 21 characters are displayed.

---

## display dns proxy table

**Syntax** **display dns proxy table**

**View** Any view

**Parameters** None

**Description** Use the **display dns proxy table** command to display the DNS proxy table.

**Examples** # Display the DNS proxy table.

```
<Sysname> display dns proxy table
Source IP Source Port Trans ID Server IP Aging
192.168.0.98 1030 24580 192.168.111.244 35
```

**Table 261** Field descriptions of the display dns proxy table command

Field	Description
Source IP	Source IP address of the DNS request, that is, the IP address of the DNS client.
Source Port	Source port number of the DNS request
Trans ID	Transaction ID of the DNS request
Server IP	IP address of the DNS server
Aging	Aging time of the DNS proxy table entry in seconds



---

## display dns server

**Syntax** `display dns server [ dynamic ]`

**View** Any view

**Parameters** **dynamic**: Displays the DNS server information dynamically obtained through DHCP or other protocols

**Description** Use the **display dns server** command to display the DNS server information.

**Related commands:** **dns server**.

**Examples** # Display the DNS server information.

```
<Sysname> display dns server
Type:
 D:Dynamic S:Static

DNS Server Type IP Address
 1 S 169.254.65.125
```

**Table 262** Description on fields of the display dns server command

Field	Description
DNS Server	Sequence number of the DNS server, configured automatically by the device, starting from 1.
Type	Type of domain name server: S represents a statically configured DNS server, and D represents a DNS server obtained dynamically through DHCP.
IP Address	IP address of the DNS server

---

## display ip host

**Syntax** `display ip host`

**View** Any view

**Parameters** None

**Description** Use the **display ip host** command to display the host names and corresponding IP addresses in the static domain name resolution table.

**Examples** # Display the host names and corresponding IP addresses in the static domain name resolution table.

```
<Sysname> display ip host
Host Age Flags Address
My 0 static 1.1.1.1
Aa 0 static 2.2.2.4
```

**Table 263** Description on fields of the display ip host command

Field	Description
Host	Host name
Age	Time to live. 0 means that the static mapping will never age out. You can only manually remove the mappings between host names and IP addresses.
Flags	Indicates the mapping type, static or dynamic. Static represents static domain name resolution.
Address	Host IP address

---

## dns domain

**Syntax** **dns domain** *domain-name*

**undo dns domain** [ *domain-name* ]

**View** System view

**Parameters** *domain-name*: Domain name suffix, consisting of character strings separated by a dot (for example, aabbcc.com). Each separated string contains no more than 63 characters. A domain name suffix may include case-insensitive letters, digits, hyphens (-), underscores (\_), and dots (.), with a total length of 238 characters.

**Description** Use the **dns domain** command to configure a domain name suffix. The system can automatically add the suffix to part of the domain name you entered for resolution.

Use the **undo dns domain** command to delete a domain name suffix (with a domain name suffix specified) or all domain name suffixes (with no domain name suffix specified).

No domain name suffix is configured by default.

You can configure a maximum of 10 domain name suffixes.

**Related commands:** **display dns domain**.

**Examples** # Configure com as a DNS suffix.

```
[Sysname] dns domain com
```

---

## dns proxy enable

**Syntax** **dns proxy enable**

**undo dns proxy enable**

**View** System view

<b>Parameters</b>	None
<b>Description</b>	Use the <b>dns proxy enable</b> command to enable DNS proxy. Use the <b>undo dns proxy enable</b> command to disable DNS proxy. By default, DNS proxy is disabled.
<b>Examples</b>	# Enable DNS proxy. <pre>&lt;Sysname&gt; system-view [Sysname] dns proxy enable</pre>

## dns resolve

<b>Syntax</b>	<b>dns resolve</b> <b>undo dns resolve</b>
<b>View</b>	System view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>dns resolve</b> command to enable dynamic domain name resolution. Use the <b>undo dns resolve</b> command to disable dynamic domain name resolution. Dynamic domain name resolution is disabled by default.
<b>Examples</b>	# Enable dynamic domain name resolution. <pre>[Sysname] dns resolve</pre>

## dns server

<b>Syntax</b>	<b>dns server</b> <i>ip-address</i> <b>undo dns server</b> [ <i>ip-address</i> ]
<b>View</b>	System view
<b>Parameters</b>	<i>ip-address</i> : IP address of the DNS server.
<b>Description</b>	Use the <b>dns server</b> command to specify a DNS server. Use the <b>undo dns server</b> to remove DNS server(s). No DNS server is specified by default.

You can configure a maximum of six DNS servers.

**Related commands:** **display dns server.**

**Examples** # Specify the DNS server 172.16.1.1.  
 [Sysname] dns server 172.16.1.1

## ip host

**Syntax** **ip host** *hostname ip-address*  
**undo ip host** *hostname [ ip-address ]*

**View** System view

**Parameters** *Hostname*: Host name, consisting of 1 to 20 characters, including case-insensitive letters, numbers, hyphens (-), or dots (.). The host name must include at least one letter.

*ip-address*: IP address of the specified host in dotted decimal notation.

**Description** Use the **ip host** command to create a host name to IP address mapping in the static resolution table.

Use the **undo ip host** command to remove a mapping.

No mappings are created by default.

You can configure only one mapping for a host name. A mapping newly configured for the host name will overwrite the previous one if there is any.

**Related commands:** **display ip host.**

**Examples** # Map the IP address 10.110.0.1 to the host name aaa.  
 [Sysname] ip host aaa 10.110.0.1

## reset dns dynamic-host

**Syntax** **reset dns dynamic-host**

**View** User view

**Parameters** None

**Description** Use the **reset dns dynamic-host** command to clear the dynamic domain name resolution information.

**Related commands:** `display dns dynamic-host`.

**Examples** # Clear the dynamic domain name resolution information.

```
<Sysname> reset dns dynamic-host
```



# 78

## FILE SYSTEM CONFIGURATION COMMANDS



Throughout this document, a filename can be entered as either of the following

- A fully qualified filename with the path included to indicate a file under a specific path. The filename can be 1 to 135 characters in length, excluding the ending character.
- A short filename with the path excluded to indicate a file in the current working path. The filename can be 1 to 91 characters in length.

---

### cd

**Syntax** `cd directory`

**View** User view

**Parameters** *directory*: Name of the target directory.

**Description** Use the **cd** command to change the current directory.

**Examples** # Change the current directory to the Flash.

```
<Sysname> cd flash:
```

# Return to the upper directory.

```
<Sysname> cd ..
```

# Return to the root directory.

```
<Sysname> cd /
```

---

### copy

**Syntax** `copy fileurl-source fileurl-dest`

**View** User view

**Parameters** *fileurl-source*: Name of the source file.

*fileurl-dest*: Name of the target file.

**Description** Use the **copy** command to copy a file.

**Examples** # Copy file testcfg.cfg and save it as tt.cfg.

```
<Sysname> copy testcfg.cfg tt.cfg
Copy flash:/testcfg.cfg to flash:/tt.cfg?[Y/N]:y
....
%Copy file flash:/testcfg.cfg to flash:/tt.cfg...Done.
```

## delete

**Syntax** **delete** [ **/unreserved** ] *file-url*

**View** User view

**Parameters** **/unreserved**: Permanently deletes the specified file, and the deleted file can never be restored.

*file-url*: Name of the file to be deleted. Asterisks (\*) are acceptable as wild cards. For example, to remove files with the expansion of txt, you may use the **delete \*.txt** command.

**Description** Use the **delete** command to remove a specified file from the storage device to the recycle bin, where you can restore the file with the **undelete** command or permanently delete it with the **reset recycle-bin** command.

The **dir /all** command displays the files removed to the recycle bin. These files are enclosed in pairs of brackets.

This command supports the wildcard \*.



**CAUTION:** *If you delete two files in different directories but with the same filename, only the last one is retained in the recycle bin.*

**Examples** # Remove the file tt.cfg from the root directory.

```
<Sysname> delete tt.cfg
.
Delete flash:/ tt.cfg?[Y/N]:y
.
%Delete file flash:/ tt.cfg...Done.
```

## dir

**Syntax** **dir** [ **/all** | *file-url* ]

**View** User view

**Parameters** **/all**: Displays all files (including those in the recycle bin).



*file-url*: Name of the file or directory to be displayed. Asterisks (\*) are acceptable as wild cards. For example, to display files with the .txt extension under the current directory, you may use the **dir \*.txt** command.

**Description** Use the **dir** command to display information about all visible files and folders in the current directory.

Use the **dir /all** command to display information about all files and folders on your device, including hidden files, hidden subfiles and those in the recycle bin. The names of these deleted files are enclosed in pairs of brackets ([ ]).

The **dir file-url** command displays information about a file or folder.

This command supports the wildcard \*.

**Examples** # Display information about all files and folders.

```
<Sysname> dir /all
Directory of flash:/
 0 -rw- 6985954 Apr 26 2005 21:06:29 mainup.bin
 1 -rwh 1842 Apr 27 2005 04:37:17 private-data.txt
 2 -rw- 1518 Apr 26 2005 12:05:38 config.cfg
 3 -rw- 2045 May 04 2005 15:50:01 backcfg.cfg
 4 -rwh 428 Apr 27 2005 16:41:21 hostkey
 5 -rwh 572 Apr 27 2005 16:41:31 serverkey
 6 -rw- 2737556 Oct 12 2005 01:31:44 [a.app]

64389 KB total (16166 KB free)
```

[ ] indicates this file is in the recycle bin.

---

## execute

**Syntax** **execute** *filename*

**View** System view

**Parameters** *filename*: Name of a batch file with a .bat extension.

**Description** Use the **execute** command to execute the specified batch file.

Batch files are command line files. Executing a batch file is to execute a set of command lines in the file.

You should not include invisible characters in a batch file. If an invisible character is found during the execution, the batch process will abort and the commands that have been executed cannot be cancelled.

Not every command in a batch file is sure to be executed. For example, if a certain command is not correctly configured, the system omits this command and goes to the next one.

A batch file does not support hot backup.

Each configuration command in a batch file must be a standard configuration command, meaning the valid configuration information which can be displayed with the **display current-configuration** command after this command is configured successfully; otherwise, this command may not be executed correctly.

**Examples** # Execute the batch file test.bat in the root directory.

```
<Sysname> system-view
[Sysname] execute test.bat
```

## file prompt

**Syntax** **file prompt** { **alert** | **quiet** }

**View** System view

**Parameters** **alert**: Enables the system to warn you about operations that may bring undesirable results such as file corruption or data loss.

**quiet**: Disables the system to warn you about any operation.

**Description** Use the **file prompt** command to set a prompt mode for file operations.

By default, the prompt mode is **alert**.

Note that when the prompt mode is set to **quiet**, the system does not warn for any file operation. To prevent undesirable consequents resulted from misoperations, the **alert** mode is preferred.

**Examples** # Set the file operation prompt mode to **alert**.

```
<Sysname> system-view
[Sysname] file prompt alert
```

## fixdisk

**Syntax** **fixdisk** *device*

**View** User view

**Parameters** *device*: Storage device name.

**Description** Use the **fixdisk** command to restore the space of a storage device when it becomes unavailable because of some abnormal operation.

**Examples** # Restore the space of the Flash.

```
<Sysname> fixdisk flash:
Fixdisk flash: may take some time to complete.
%Fixdisk flash: completed.
```

---

## format

**Syntax** `format device`

**View** User view

**Parameters** *device*: Storage device name (for example flash or cf).

**Description** Use the **format** command to format a storage device.



**CAUTION:** *Formatting a device results in loss of all the files and these files cannot be restored. In particular, if there is startup configuration file on a storage device, formatting the storage device results in loss of the startup configuration file.*

**Examples** # Format the Flash.

```
<Sysname> format flash:
All data on flash: will be lost, proceed with format ? [Y/N]:y
./
%Format flash: completed.
```

---

## mkdir

**Syntax** `mkdir directory`

**View** User view

**Parameters** *directory*: Name of a subdirectory.

**Description** Use the **mkdir** command to create a subdirectory under the specified directory on the storage device.

The name of the subdirectory to be created must be unique under the specified directory.

This command does not allow you to create multiple directory levels at one time. For instance, to create a subdirectory "flash:/test/mytest", the test directory must have been created.

**Examples** # Create a directory named test.

```
<Sysname> mkdir test
...
% Created dir flash:/test
```

# create a subdirectory named mytest under test.

```
<Sysname>mkdir test/mytest
.
%Created dir flash:/test/mytest
```

---

## more

**Syntax** `more file-url`

**View** User view

**Parameters** *file-url*: File name.

**Description** Use the **more** command to display the contents of the specified file.

So far, this command is valid only for .txt files.

**Examples** # Display the contents of file test.txt.

```
<Sysname> more test.txt
AppWizard has created this test application for you.
This file contains a summary of what you will find in each of the fi
les that make up your test application.
Test.dsp
This file (the project file) contains information at the project lev
el and is used to build a single project or subproject. Other users
can share the project (.dsp) file, but they should export the makefi
les locally.
```

---

## mount

**Syntax** `mount device`

**View** User view

**Parameters** *device*: Storage device name (for example flash or cf).

**Description** Use the **mount** command to mount a hot swappable storage device, such as a CF module, a USB device, etc (excluding Flash). This command is effective only when the device is in unmounted state.

By default, a storage device is in the mounted state, that is, you can use it without mounting it.

Note that:

- Do not remove the storage device or swap the module when mounting or unmounting the device, or when you are processing files on the storage device. Otherwise, the file system could be damaged.

- When a storage device is connected to a low version system, the system may not be able to recognize the device automatically, you need to use the **mount** command for the storage device to function normally.
- Before removing a mounted storage device from the system, you should first unmount it to avoid damaging the device.

**Related commands:** **umount.**

**Examples** # Mount a CF module of the main module.

```
<Sysname> mount cf:
% Mount cf: successfully.
%Apr 23 01:50:00:628 2003 System VFS/4/LOG:
cf: mounted into slot 4.
```

# Mount a CF module of the backup module (assume the backup module is in slot 5).

```
<Sysname> mount slot5#cf:

% Mount slot5#cf: successfully.
%Apr 23 01:50:00:628 2003 System VFS/5/LOG:
cf: mounted into slot 5.
```

## move

**Syntax** **move** *fileurl-source fileurl-dest*

**View** User view

**Parameters** *fileurl-source*: Name of the source file.

*fileurl-dest*: Name of the target file.

**Description** Use the **move** command to move a file.

**Examples** # Move the file flash:/test/sample.txt to flash:/sample.txt.

```
<Sysname> move flash:/test/sample.txt flash:/sample.txt
Move flash:/test/sample.txt to flash:/sample.txt ?[Y/N]:y

...
%Moved file flash:/test/sample.txt to flash:/sample.txt
```

## pwd

**Syntax** **pwd**

**View** User view

<b>Parameters</b>	None
<b>Description</b>	Use the <b>pwd</b> command to display the current path. If the current path is not set, the operation will fail.
<b>Examples</b>	# Display the current path. <pre>&lt;Sysname&gt; pwd flash:</pre>

**rename**

<b>Syntax</b>	<b>rename</b> <i>fileurl-source fileurl-dest</i>
<b>View</b>	User view
<b>Parameters</b>	<i>fileurl-source</i> : Name of the source file or directory. <i>fileurl-dest</i> : Name of the target file or directory.
<b>Description</b>	Use the <b>rename</b> command to rename a file or directory. The target file name must be unique under the current path.
<b>Examples</b>	# Rename the file sample.txt as sample.bak. <pre>&lt;Sysname&gt; rename sample.txt sample.bak Rename flash:/sample.txt to flash:/sample.bak?[Y/N]:y ... % Renamed file flash:/sample.txt to flash:/sample.bak</pre>

**reset recycle-bin**

<b>Syntax</b>	<b>reset recycle-bin</b> [ <b>/force</b> ]
<b>View</b>	User view
<b>Parameters</b>	<b>/force</b> : Empties the recycle bin.
<b>Description</b>	Use the <b>reset recycle-bin</b> command to permanently remove deleted file or files from the recycle bin.  Unlike this command, the <b>delete file-url</b> command only moves files to the recycle bin.
<b>Examples</b>	# Empty the recycle bin. <pre>&lt;Sysname&gt; reset recycle-bin Clear flash:/~/test2.txt ?[Y/N]:y</pre>

```
Clearing files from flash may take a long time. Please wait...
...
%Cleared file flash:/~/test2.txt...
```

---

## rmdir

**Syntax** `rmdir directory`

**View** User view

**Parameters** *directory*: Name of the directory.

**Description** Use the **rmdir** command to remove a directory.

The directory must be an empty one. If it is not, first delete all files and subdirectory under it with the **delete** command.

**Examples** # Remove directory mydir.

```
<Sysname> rmdir mydir
Rmdir flash:/mydir?[Y/N]:y
...
%Removed directory flash:/mydir.
```

---

## umount

**Syntax** `umount device`

**View** User view

**Parameters** *device*: Storage device name (for example flash or cf).

**Description** Use the **umount** command to unmount a hot swappable storage device, such as a CF module or a USB device, excluding Flash. This command is effective only when the device is in mounted state.

By default, a storage device is in the mounted state, that is, you can use it without mounting it.

Note that:

- Do not remove the storage device or swap the module when mounting or unmounting the device, or when you are processing files on the storage device. Otherwise, the file system could be damaged.
- When a storage device is connected to a low version system, the system may not be able to recognize the device automatically, you need to use the mount command for the storage device to function normally.

- Before removing a mounted storage device from the system, you should first unmount it to avoid damaging the device. By default, a storage device is in the mounted state. You can use it without mounting it.

**Related commands:** **mount.**

**Examples** # Unmount a CF module of the main board

```
<Sysname> umount cf:
% Umount cf: successfully.
%Apr 23 01:49:20:929 2003 System VFS/5/LOG:
cf: unmounted from slot 4.
```

# Unmount a CF module of the backup module (assume the backup module is in slot 5).

```
<Sysname> umount slot5#cf:
% Umount slot5#cf: successfully.
%Apr 23 01:49:20:929 2003 System VFS/5/LOG:
cf: unmounted from slot 5.
```

## undelete

**Syntax** **undelete** *file-url*

**View** User view

**Parameters** *filename*: Name of the file to be restored.

**Description** Use the **undelete** command to restore a file from the recycle bin.

If another file with the same name exists under the same path, the undelete operation will cause it to be overwritten and the system will ask you whether to continue.

**Examples** # Restore file sample.bak from the recycle bin.

```
<Sysname> undelete sample.bak
Undelete flash:/sample.bak ?[Y/N]:y
.....
% Undeleted file flash:/sample.bak
```



# 79

## CONFIGURATION FILE MANAGEMENT COMMANDS

---

### backup startup-configuration

**Syntax** `backup startup-configuration to dest-addr [ dest-filename ]`

**View** User view

**Parameters** *dest-addr*: IP address or name of a TFTP server. The address cannot be an IPv6 address.

*dest-filename*: Target filename used to save the next startup configuration file on the server.

**Description** Use the **backup startup-configuration** command to backup the startup configuration file (for next startup) using a filename you specify. If you do not specify this filename, the original filename is used.

- This command only backs up the configuration file of the main module for next startup.
- This command backs up the configuration file for next startup.

Presently, the device uses TFTP to backup configuration files.

**Examples** # Backup the configuration file for next startup on the TFTP server with IP address 2.2.2.2, using the filename config.cfg.

```
<Sysname> backup startup-configuration to 2.2.2.2 config.cfg
Backup next startup-configuration file to 2.2.2.2, please wait...
finished!
<Sysname>
```

---

### display saved-configuration

**Syntax** `display saved-configuration [ by-linenum ]`

**View** Any view

**Parameters** **by-linenum**: Identifies each line of displayed information with a line number.

**Description** Use the **display saved-configuration** command to display the initial configuration file saved in the storage device.

In case the device malfunctions after being powered on, if you find some configurations are not validated or incorrect, you may use this command to identify the problem.

If you do not use the configuration file when the device starts up, meaning the displayed startup configuration file is NULL after you execute the **display startup** command, no information is displayed when you execute the **display saved-configuration** command; if you have saved the configuration file after the device starts up, the information last saved in the configuration file is displayed.

**Related commands:** **save**, **reset saved-configuration**, **display current-configuration** on page 1165.

**Examples** # Display the configuration file saved in the storage device.

```
<Sysname> display saved-configuration
#
version 5.00, 0000
#
sysname Mydevice
#
local-user abc password simple abc
#
tcp window 8
#
interface Aux1/0
link-protocol ppp
#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface Ethernet1/3
ip address 10.110.101.17 255.255.255.0
#
interface NULL0
#
ospf 1
#
ip route-static 10.12.0.0 255.255.0.0 Ethernet 1/0
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
authentication-mode none
#
return
```

The configurations are displayed in the order of global, port, and user interface.

---

## display startup

**Syntax** **display startup**

<b>View</b>	Any view
<b>Parameters</b>	None
<b>Description</b>	<p>Use the <b>display startup</b> command to display the configuration file used at this startup and the one used for next startup.</p> <p>Note that:</p> <ul style="list-style-type: none"> <li>■ The SMB is started and run based on the current configurations of the AMB; therefore the current startup configuration files displayed on the AMB and SMB are always the same.</li> <li>■ After switchover between the AMB and SMB, the new AMB does not restart from the configuration file and runs with the current configuration instead. Therefore, when you use the <b>display startup</b> command to view the configuration file, the current startup configuration file of the new AMB is NULL and that of the new SMB is also NULL to keep consistent with the new AMB.</li> </ul>

**Related commands:** **startup saved-configuration.**

**Examples** # Display the configuration file used at this startup and the one used for next startup.

```
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: flash:/testcfg.cfg
 Next startup saved-configuration file: flash:/testcfg.cfg
```

---

## reset saved-configuration

<b>Syntax</b>	<b>reset saved-configuration</b>
<b>View</b>	User view
<b>Parameters</b>	.None
<b>Description</b>	<p>Use the <b>reset saved-configuration</b> command to erase the configuration file saved in the storage device.</p> <p>Note that:</p> <ul style="list-style-type: none"> <li>■ The <b>reset saved-configuration</b> command erases the configuration file which has the main attribute only; while for the configuration file which has both the main and backup attributes, the command erases its main attribute.</li> <li>■ The <b>reset saved-configuration</b> command erases the configuration file which has the backup attribute only; while for the configuration file which has both the main and backup attributes, the command erases its backup attribute.</li> </ul>



**CAUTION:** This command will permanently delete the configuration file on the device. Use it with caution.

**Related commands:** **save, display saved-configuration.**

**Examples** # Erase the configuration file saved in the storage device.

```
<Sysname> reset saved-configuration
The saved configuration will be erased.
Are you sure? [Y/N]:y
Configuration in the device is being cleared.
Please wait
Configuration in the device is cleared.
```

---

## restore startup-configuration

**Syntax** **restore startup-configuration from** *src-addr src-filename*

**View** User view

**Parameters** *src-addr*: IP address or name of a TFTP server. The address cannot be an IPv6 address.

*src-filename*: Filename of the configuration file to be downloaded from the specified server.

**Description** Use the **restore startup-configuration** command to download the configuration file from the specified TFTP server for the next startup of the device.

- This command downloads the configuration file to the main module and meanwhile copies the file to the backup module.
- This command downloads the configuration file for next startup.

If the file to be downloaded has the same filename as an existing file on the main or backup module, you will be prompted whether you want to overwrite the existing file or not. In addition, both the main module and the backup module are assumed to use the storage device of the same type when checking filename or downloading the configuration file (both to the root directory of the main module or backup module), otherwise, the restoration fails.

**Examples** # Download the configuration file config.cfg for the next startup from the TFTP server whose IP address is 2.2.2.2.

```
<Sysname>restore startup-configuration from 2.2.2.2 config.cfg
Restore next startup-configuration file from 2.2.2.2. Please wait...finished!
Now restore next startup-configuration file from main to slave board, Please wait...finished!
```

---

## save

**Syntax** **save** [ *file-name* | [ **safely** ]

**View** Any view

**Parameters** *file-name*: File name, whose suffix must be .cfg.

**safely**: Sets the configuration saving mode to safe. If this argument is not specified, the configuration file is saved in fast mode.

**Description** Use the **save** command to save the current configuration to the specified configuration file. If no filename is specified, the system saves the configuration file in an interactive way. In this way, you can use the default path (the configuration file for next startup) or enter a filename to specify a new path, but the suffix of the filename must be ".cfg" and the path must be the path of the storage device on the active main module (AMB).

Note that:

- If you specify the filename, the SMB does not save the current configuration into its configuration file, even if the configuration file saving synchronization function is enabled. If no filename is specified, the SMB automatically saves the current configuration when the AMB is executing the **save** command.
- If no filename is specified, the system saves the configuration file in an interactive way. In this way, the system automatically sets the file as the configuration file for next startup if you use a non-default path (that is, enter a new filename.).

The default filename is startup.cfg.

**Related commands:** **reset saved-configuration, display current-configuration, display saved-configuration.**

**Examples** # Save the current configuration file to the default directory

```
<Sysname> save
The current configuration will be written to the device.
Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/testcfg.cfg](To leave the
existing filename unchanged, press the enter key):
flash:/testcfg.cfg exists, overwrite?[Y/N]:y

Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration flash:/testcfg.cfg. Please wait...
.
Configuration is saved to flash successfully.
<Sysname>
```

---

## slave auto-update config

**Syntax** **slave auto-update config**

**undo slave auto-update config**

<b>View</b>	System view
<b>Parameters</b>	None
<b>Description</b>	<p>Use the <b>slave auto-update config</b> command to enable auto-update between the AMB and SMB (standby main module).</p> <p>Use the <b>undo slave auto-update config</b> command to disable auto-update between the AMB and SMB.</p> <p>By default, auto-update between the AMB and SMB is enabled.</p>
<b>Examples</b>	<pre># Enable the auto-update between the AMB and SMB. &lt;Sysname&gt; system-view [Sysname] slave auto-update config</pre>

## startup saved-configuration

<b>Syntax</b>	<pre>startup saved-configuration <i>cfgfile</i> undo startup saved-configuration</pre>
<b>View</b>	User view
<b>Parameters</b>	<i>cfgfile</i> : Configuration file name.
<b>Description</b>	<p>Use the <b>startup saved-configuration</b> command to specify a configuration file for next startup.</p> <p>Use the <b>undo startup saved-configuration</b> command to start up with an empty configuration, which means startup with the initial configuration of the system.</p> <p>The specified file must be ended with a .cfg extension and saved in the root directory of the storage device.</p>
<b>Related commands:</b>	<b>display startup.</b>
<b>Examples</b>	<pre># Specify a configuration file for next startup. &lt;Sysname&gt; startup saved-configuration testcfg.cfg Please wait ..... Done!</pre>

# 80

## FTP SERVER CONFIGURATION COMMANDS

---

### display ftp-server

**Syntax** `display ftp-server`

**View** Any view

**Parameters** None

**Description** Use the **display ftp-server** command to display the FTP server configuration of the device.

After configuring FTP parameters, you may verify them with this command.

**Related commands:** **ftp timeout, ftp update.**

**Examples** # Display the FTP server configuration.

```
<Sysname> display ftp-server
 FTP server is running
 Max user number: 1
 User count: 1
 Timeout value(in minute): 30
 Put Method: fast
```

The output indicates that the FTP server is running with support to only one concurrent login user; now one logged-in user is present; timeout of the user is 30 minutes, and FTP update mode is **fast**.

---

### display ftp-user

**Syntax** `display ftp-user`

**View** Any view

**Parameters** None

**Description** Use the **display ftp-user** command to display the detailed information of current FTP users.

**Examples** # Display the detailed information of FTP users.

```
<Sysname> display ftp-user
 UserName HostIP Port Idle HomeDir
 ftp 192.168.1.54 1190 0 flash:
```

**Table 264** Field descriptions of the display ftp-user command

Field	Description
UserName	Name of the present logged-in user
HostIP	IP address of the present logged-in user
Port	Port which the present logged-in user is using
Idle	Duration time of the current FTP connection
HomeDir	Specified path of the present logged-in user

---

## free ftp user

**Syntax** **free ftp user** *username*

**View** User view

**Parameters** *username*: Username used when the FTP connection to be released is established.

**Description** Use the **free ftp user** command to manually release the FTP connection established with the specified username.

Note that if the user to be released is transmitting a file, the connection between the user and the FTP server is terminated after the file transmission.

**Examples** # Manually release the FTP connection established with username of **ftpuser**.

```
<Sysname> free ftp user ftpuser
Are you sure to free FTP user ftpuser? [Y/N]:y
<Sysname>
```

---

## ftp server enable

**Syntax** **ftp server enable**

**undo ftp server**

**View** System view

**Parameters** None

**Description** Use the **ftp server enable** command to enable the FTP server.

Use the **undo ftp server** command to disable the FTP server.

By default, the FTP server is disabled to prevent attacks.



**Examples** # Disable the FTP server.

```
<Sysname> system-view
[Sysname] undo ftp server
% Close FTP server
```

## ftp timeout

**Syntax** **ftp timeout** *minute*

**undo ftp timeout**

**View** System view

**Parameters** *minute*: Idle-timeout timer in minutes, in the range 1 to 35791. The default is 30 minutes.

**Description** Use the **ftp timeout** command to set the idle-timeout timer.

Use the **undo ftp timeout** command to restore the default.

After you log onto the FTP server, you set up an FTP connection. When the connection is disrupted, the FTP server, if not notified, cannot realize that and maintains the connection all the same. To address this problem, you can set an idle-timeout timer to have the FTP server disconnected if no information is received or/and transmitted before the timer expires.

**Examples** # Set the idle-timeout timer to 36 minutes.

```
<Sysname> system-view
[Sysname] ftp timeout 36
```

## ftp update

**Syntax** **ftp update** { **fast** | **normal** }

**undo ftp update**

**View** System view

**Parameters** **fast**: Fast update.

**normal**: Normal update.

**Description** Use the **ftp update** command to set the file update mode that the FTP server uses while receiving data.

Use the **undo ftp update** command to restore the default, namely, the normal mode.

**Examples** # Set the FTP update mode to **normal**.

```
<Sysname> system-view
[Sysname] ftp update normal
```

# 81

## FTP CLIENT CONFIGURATION COMMANDS



- *The prompt information in this section is that in the network where the 3Com S7900E Ethernet switches act as the FTP server. If you use other devices as the FTP server, PC for example, the prompt information may be different.*
- *You must use the **ftp** command to enter FTP client view for configurations under this view. For details, refer to “ftp” on page 1108.*

---

### ascii

**Syntax** `ascii`

**View** FTP client view

**Parameters** None

**Description** Use the **ascii** command to set the file transfer mode to ASCII for the FTP connection.

FTP provides two file transfer modes: ASCII and binary. To transfer text files, use the ASCII mode; to transfer program files, use the binary mode.

By default, the file transfer mode is ASCII.

**Examples** # Set the file transfer mode to ASCII.

```
[ftp]ascii
200 Type set to A.
```

---

### binary

**Syntax** `binary`

**View** FTP client view

**Parameters** None

**Description** Use the **binary** command to set the file transfer mode to binary (also called flow mode).

FTP provides two file transfer modes: ASCII and binary. To transfer text files, use the ASCII mode; to transfer program files, use the binary mode.

By default, the transfer mode is ASCII mode.

**Examples** # Set the file transfer mode to **binary**.

```
[ftp]binary
200 Type set to I.
```

## bye

**Syntax** **bye**

**View** FTP client view

**Parameters** None

**Description** Use the **bye** command to disconnect from the remote FTP server and exit to user view.

**Examples** # Terminate the connection with the remote FTP server and exit to user view.

```
[ftp]bye
221 Server closing.
<Sysname>
```

## cd

**Syntax** **cd** *pathname*

**View** FTP client view

**Parameters** *pathname*: Path name.

**Description** Use the **cd** command to change the current working directory on the remote FTP server.

You can use this command to access another authorized directory on the FTP server.

**Examples** # Change the current working directory to flash:/logfile.

```
[ftp]cd flash:/logfile
250 CWD command successful.
```

---

**cdup**

<b>Syntax</b>	<b>cdup</b>
<b>View</b>	FTP client view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>cdup</b> command to exit the current directory and enter the upper directory of the FTP server.
<b>Examples</b>	<pre># Change the current working directory path to the upper directory. [ftp]cdup 200 CDUP command successful.</pre>

---

**close**

<b>Syntax</b>	<b>close</b>
<b>View</b>	FTP client view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>close</b> command to terminate the connection to the FTP server, but remain in FTP client view.  This command is equal to the <b>disconnect</b> command.
<b>Examples</b>	<pre># Terminate the connection to the FTP server and remain in FTP client view. [ftp] close 221 Server closing. [ftp]</pre>

---

**debugging**

<b>Syntax</b>	<b>debugging</b> <b>undo debugging</b>
<b>View</b>	FTP client view
<b>Default Level</b>	3: Manage level
<b>Parameters</b>	None

**Description** Use the **debugging** command to enable FTP client debugging.

Use the **undo debugging** command to disable FTP client debugging.

By default, FTP client debugging is disabled.

**Examples** # The device serves as the FTP client. Enable FTP client debugging and use the active mode to download file **sample.file** from the current directory of the FTP server.

```
<Sysname> terminal monitor
<Sysname> terminal debugging
<Sysname> ftp 192.168.1.46
Trying 192.168.1.46 ...
Press CTRL+K to abort
Connected to 192.168.1.46.
220 FTP service ready.
User(192.168.1.46:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.

[ftp]undo passive
[ftp] debugging
[ftp] get sample.file

---> PORT 192,168,1,44,4,21
200 Port command okay.
The parsed reply is 200
---> RETR sample.file
150 Opening ASCII mode data connection for /sample.file.
The parsed reply is 150
FTPC: File transfer started with the signal light turned on.
FTPC: File transfer completed with the signal light turned off.
.226 Transfer complete.
FTP: 3304 byte(s) received in 4.889 second(s), 675.00 byte(s)/sec.

[ftp]
```

**Table 265** debugging command output description

Field	Description
The parsed reply is	The received reply code, which is defined in RFC 959.
FTPC: File transfer started with the signal light turned on.	File transfer starts, and the signal light is turned on.
FTPC: File transfer completed with the signal light turned off.	File transfer is completed, and the signal light is turned off.

---

## delete

**Syntax** **delete** *remotefile*

**View** FTP client view

**Parameters** *remotefile*: File name.

**Description** Use the **delete** command to delete a specified file on the remote FTP server.  
To do this, you must be a user with the delete permission on the FTP server.

**Examples** # Delete file temp.c.  
[ftp]delete temp.c  
250 DELE command successful.

## dir

**Syntax** **dir** [ *remotefile* [ *localfile* ] ]

**View** FTP client view

**Parameters** *remotefile*: Name of the file or directory on the remote FTP server.  
*localfile*: Name of the local file to save the displayed information.

**Description** Use the **dir** command to view detailed information of the files and subdirectories under the current directory on the remote FTP server.

Use the **dir remotefile** command to display the detailed information of the specified file or directory on the remote FTP server.

Use the **dir remotefile localfile** command to display the detailed information of the specified file or directory on the remote FTP server, and save the displayed information into a local file specified by the *localfile* argument.



*The **ls** command can only display the names of files and directories, whereas the **dir** command can display other related information of the files and directories, such as the size, the date they were created.*

**Examples** # View the information of the file startup.cfg, and save the result to aa.txt.  
[ftp] dir startup.cfg aa.txt  
227 Entering Passive Mode (2,2,2,2,4,7).  
125 ASCII mode data connection already open, transfer starting for s  
tartup.cfg.  
...226 Transfer complete.  
FTP: 68 byte(s) received in 6.180 second(s), 11.00 byte(s)/sec.

## disconnect


**Syntax** **disconnect**

**View** FTP client view

<b>Parameters</b>	None
<b>Description</b>	Use the <b>disconnect</b> command to disconnect from the remote FTP server but remain in FTP client view.  This command is equal to the <b>close</b> command.
<b>Examples</b>	# Disconnect from the remote FTP server but remain in FTP client view. <pre>[ftp] disconnect 221 Server closing. [ftp]</pre>

---

## display ftp client configuration

<b>Syntax</b>	<b>display ftp client configuration</b>
<b>View</b>	Any view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>display ftp client configuration</b> command to display the configuration information of the FTP client.
	<i>Currently this command displays the configuration information of the source address. If the currently valid source address is the source IP address, this command displays the configured source IP address; if it is the source interface, this command displays the configured source interface.</i>
<b>Related commands:</b>	<b>ftp client source.</b>
<b>Examples</b>	# Display the current configuration information of the FTP client. <pre>&lt;Sysname&gt; display ftp client configuration The source IP address is 192.168.0.123</pre>

---

## ftp

<b>Syntax</b>	<b>ftp</b> [ <i>server-address</i> [ <i>service-port</i> ] [ <b>source</b> { <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>ip</b> <i>source-ip-address</i> } ] ]
<b>View</b>	User view
<b>Parameters</b>	<i>server-address</i> : IP address or host name of a remote FTP server.  <i>service-port</i> : Port number of the remote FTP server, in the range 0 to 65535. The default value is 21.



**interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on this interface is the source address of the transmitted packets. If no primary IP address is configured on the source interface, the connection fails.

**ip source-ip-address**: The source IP address of the current FTP client. This source address must be the one that has been configured on the device.

**Description** Use the **ftp** command to log onto the remote FTP server and enter FTP client view.

Note that:

- This command applies to IPv4 network.
- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging onto the FTP server.
- If you specify the parameter, you will be asked to enter the username and password for accessing the FTP server.
- The priority of the source address specified with this command is higher than that with the **ftp client source** command. If you specify the source address with the **ftp client source** command first and then with the **ftp** command, the source address specified with the **ftp** command is used to communicate with the FTP server.

**Related commands:** **ftp client source**.

**Examples** # Log from the current device **Sysname1** onto the device **Sysname2** with the IP address of 192.168.0.211. The source IP address of the packets sent is 192.168.0.212.

```
<Sysname1> ftp 192.168.0.211 source ip 192.168.0.212
Trying 192.168.0.211 ...
Press CTRL+K to abort
Connected to 192.168.0.211.
220 FTP Server ready
User(192.168.0.211:(none)):abc
331 Password required for abc
Password:
230 Login OK
[ftp]
```

---

## ftp client source

**Syntax** **ftp client source** { **interface** *interface-type interface-number* | **ip source-ip-address** }

**undo ftp client source**

**View** System view

**Parameters** **interface** *interface-type interface-number*: Source interface for the FTP connection, including interface type and interface number. The primary IP address

configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the connection fails.

**ip source-ip-address:** Source IP address of the FTP connection. It must be an IP address that has been configured on the device.

**Description** Use the **ftp client source** command to configure the source address of the transmitted FTP packets from the FTP client.

Use the **undo telnet client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the routing protocol as the source IP address to communicate with an FTP server.

Note that:

- The source address includes the source interface and the source IP address. If you use the **ftp client source** command to specify the source interface and the source IP address, the newly specified source IP address overwrites the original one and vice versa.
- If the source address is specified with the **ftp client source** command and then with the **ftp** command, the source address specified with the latter one is used to communicate with the FTP server.
- The source address specified with the **ftp client source** command is valid for all **ftp** connections and the source address specified with the **ftp** command is valid only for the current **ftp** connection.

**Related commands:** **display ftp client configuration.**

**Examples** # Specify the source IP address of the FTP client as 2.2.2.2.

```
<Sysname> system-view
[Sysname] ftp client source ip 2.2.2.2
```

# Specify the source interface of the FTP client as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ftp client source interface vlan-interface 1
```

---

## ftp ipv6

**Syntax** **ftp ipv6** [ *server-address* [ *service-port* ] [ **source ipv6** *source-ipv6-address* ] [ **-i** *interface-type interface-number* ] ]

**View** User view

**Parameters** *server-address*: IP address or host name of the remote FTP server.

*service-port*: Port number of the FTP server, in the range 0 to 65535. The default value is 21.

**source ipv6** *source-ipv6-address*: Specifies a source IPv6 address for transmitted FTP packets. This address must be an IPv6 address that has been configured on the device.

**-i** *interface-type interface-number*: Specifies the type and number of the egress interface. This parameter can be used only in case that the FTP server address is the link local address and the specified egress interface must have a link local address (For the configuration of link local address, see *IPv6 Configuration*).

**Description** Use the **ftp ipv6** command to log onto the FTP server and enter FTP client view.

Note that:

- This command applies to IPv6 network.
- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging onto the FTP server.
- If you specify the parameter, you will be asked to enter the username and password for accessing the FTP server.

**Examples** # Log onto the FTP server with IPv6 address 3000::200.

```
<Sysname> ftp ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
[ftp]
```

---

## get

**Syntax** **get** *remotefile* [ *localfile* ]

**View** FTP client view

**Parameters** *remotefile*: File name on the remote FTP server.

*localfile*: Local file name.

**Description** Use the **get** command to download a file from a remote FTP server and save it.

If no name is specified, the local file uses the name of the source file on the FTP server by default.

**Examples** # Download file testcfg.cfg and save it as **aa.cfg**.

```
[ftp]get testcfg.cfg aa.cfg
227 Entering Passive Mode (2,2,2,2,17,163).
```

```
125 ASCII mode data connection already open, transfer starting for testcfg.cfg.
....226 Transfer complete.
FTP: 5190 byte(s) received in 7.754 second(s), 669.00 byte(s)/sec.
[ftp]
```


---

## lcd

<b>Syntax</b>	<b>lcd</b>
<b>View</b>	FTP client view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>lcd</b> command to display the local directory of the FTP client.
<b>Examples</b>	# Display the local directory.  [ftp] lcd FTP: Local directory now flash:/temp

---

## ls

<b>Syntax</b>	<b>ls</b> [ <i>remotefile</i> ] [ <i>localfile</i> ] ]
<b>View</b>	FTP client view
<b>Parameters</b>	<i>remotefile</i> : Filename or directory on the remote FTP server.  <i>localfile</i> : Name of a local file used to save the displayed information.
<b>Description</b>	Use the <b>ls</b> command to view the information of all the files and subdirectories under the current directory of the remote FTP server. The file names and subdirectory names are displayed.  Use the <b>ls</b> <i>remotefile</i> command to view the information of a specified file or subdirectory.  Use the <b>ls</b> <i>remotefile localfile</i> command view the information of a specified file or subdirectory, and save the result to a local file specified by the <i>localfile</i> argument.
	<i>The <b>ls</b> command can only display the names of files and directories, whereas the <b>dir</b> command can display other related information of the files and directories, such as the size, the date they are created.</i>
<b>Examples</b>	# View the information of all files and subdirectories under the current directory of the FTP server.  [ftp] ls 227 Entering Passive Mode (192,168,1,50,17,165). 125 ASCII mode data connection already open, transfer starting for *. ar-router.cfg

```

logfile
mainar.bin
arbasicbtm.bin
ftp
test
bb.cfg
testcfg.cfg
226 Transfer complete.
FTP: 87 byte(s) received in 0.132 second(s) 659.00 byte(s)/sec.

View the information of directory logfile, and save the result to file aa.txt.

[ftp] ls logfile aa.txt
227 Entering Passive Mode (192,168,1,50,17,166).
125 ASCII mode data connection already open, transfer starting for logfile.
....226 Transfer complete.
FTP: 9 byte(s) received in 0.094 second(s) 95.00 byte(s)/sec.

View the content of file aa.txt.

[ftp] quit
<Sysname> more aa.txt
logfile

```

---

## mkdir

**Syntax** **mkdir** *directory*

**View** FTP client view

**Parameters** *directory*: Directory name.

**Description** Use the **mkdir** command to create a subdirectory under the specified directory on the remote FTP server.

To do this, you must be a user with the permission on the FTP server.

**Examples** # Create subdirectory **mytest** on the current directory of the remote FTP server.

```

[ftp] mkdir mytest
257 " flash:/mytest" new directory created.

```

---

## open

**Syntax** **open** *server-address* [ *service-port* ]

**View** FTP client view

**Parameters** *server-address*: IP address or host name of a remote FTP server.

*service-port*: Port number of the remote FTP server, in the range 0 to 65535, with the default value of 21.

**Description** Use the **open** command to log onto the IPv4 FTP server under FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

**Related commands:** **close**.

**Examples** # In FTP client view, log onto the FTP server with the IP address of 192.168.1.50.

```
<Sysname> ftp
[ftp] open 192.168.1.50
Trying 192.168.1.50 ...
Press CTRL+K to abort
Connected to 192.168.1.50.
220 FTP service ready.
User(192.168.1.50:(none)):aa
331 Password required for aa.
Password:
230 User logged in.

[ftp]
```

## open ipv6

**Syntax** **open ipv6** *server-address* [ *service-port* ] [ **-i** *interface-type interface-number* ]

**View** FTP client view

**Parameters** *server-address*: IP address or host name of the remote FTP server.

*service-port*: Port number of the remote FTP server, in the range 0 to 65535. The default value is 21.

**-i interface-type interface-number**: Specifies the egress interface by its type and number. This parameter can be used only in case that the FTP server address is the link local address and the specified egress interface must have a link local address (For the configuration of link local address, see *IPv6 Configuration*.).

**Description** Use the **open ipv6** command to log onto IPv6 FTP server in FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

**Related commands:** **close**.

**Examples** # Log onto the FTP server (with IPv6 address 3000::200) in FTP client view.

```
<Sysname> ftp
[ftp] open ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
```

```

220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.

```

---

## passive

**Syntax** **passive**  
**undo passive**

**View** FTP client view

**Parameters** None

**Description** Use the **passive** command to set the data transmission mode to **passive**.  
 Use the **undo passive** command to set the data transmission mode to **active**.  
 The default transmission mode is **passive**.

**Examples** # Set the data transmission mode to **passive**.  

```

[ftp] passive
FTP: passive is on

```

---

## put

**Syntax** **put** *localfile* [ *remotefile* ]

**View** FTP client view

**Parameters** *localfile*: Local file name.  
*remotefile*: Name of the file to be saved on the remote FTP server.

**Description** Use the **put** command to upload a file to the remote FTP server.  
 If no name is assigned to the file to be saved on the FTP server, the name of the source file is used by default.

**Examples** # Upload source file **cc.txt** to the remote FTP server and save it as **dd.txt**.  

```

[ftp] put cc.txt dd.txt
227 Entering Passive Mode (192,168,1,50,17,169).
125 ASCII mode data connection already open, transfer starting for dd.txt.
226 Transfer complete.
FTP: 9 byte(s) sent in 0.112 second(s), 80.00byte(s)/sec.

```

---

**pwd**

<b>Syntax</b>	<b>pwd</b>
<b>View</b>	FTP client view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>pwd</b> command to display the working directory on the remote FTP server.
<b>Examples</b>	<pre># Display the working directory on the remote FTP server. [ftp] pwd 257 "flash:/temp" is current directory.</pre>

---

**quit**

<b>Syntax</b>	<b>quit</b>
<b>View</b>	FTP client view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>quit</b> command to disconnect from the remote FTP server and exit to user view.
<b>Examples</b>	<pre># Disconnect from the remote FTP server and exit to user view. [ftp] quit 221 Server closing.  &lt;Sysname&gt;</pre>

---

**remotehelp**

<b>Syntax</b>	<b>remotehelp</b> [ <i>protocol-command</i> ]
<b>View</b>	FTP client view
<b>Parameters</b>	<i>protocol-command</i> : FTP command.
<b>Description</b>	Use the <b>remotehelp</b> command to display the help information of FTP-related commands supported by the remote FTP server.  If no parameter is specified, FTP-related commands supported by the remote FTP server are displayed.



**Examples** # Display FTP commands supported by the remote FTP server.

```
[ftp] remotehelp
214-Here is a list of available ftp commands
 Those with '*' are not yet implemented.
 USER PASS ACCT* CWD CDUP SMNT* QUIT REIN*
 PORT PASV TYPE STRU* MODE* RETR STOR STOU*
 APPE* ALLO* REST* RNFR* RNTO* ABOR* DELE RMD
 MKD PWD LIST NLST SITE* SYST STAT* HELP
 NOOP* XCUP XCWD XMKD XPWD XRMD
214 Direct comments to 3Com company.
```

# Display the help information for the **user** command.

```
[ftp] remotehelp user
214 Syntax: USER <sp> <username>.
```

```
[ftp]
```

**Table 266** Field descriptions of the remotehelp command

Field	Description
214-Here is a list of available ftp commands	The following is an available FTP command list.
Those with '*' are not yet implemented.	Those commands with "*" are not yet implemented.
USER	Username
PASS	Password
CWD	Change the current working directory
CDUP	Change to parent directory
SMNT*	File structure setting
QUIT	Quit
REIN*	Re-initialization
PORT	Port number
PASV	Passive mode
TYPE	Request type
STRU*	File structure
MODE*	Transmission mode
RETR	Download a file
STOR	Upload a file
STOU*	Store unique
APPE*	Appended file
ALLO*	Allocation space
REST*	Restart
RNFR*	Rename the source
RNTO*	Rename the destination
ABOR*	Abort the transmission
DELE	Delete a file
RMD	Delete a folder
MKD	Create a folder
PWD	Print working directory

**Table 266** Field descriptions of the remotehelp command

Field	Description
LIST	List files
NLST	List file description
SITE*	Orient a parameter
SYST	Display system parameters
STAT*	State
HELP	Help
NOOP*	No operation
XCUP	Extension command, the same meaning as CUP
XCWD	Extension command, the same meaning as CWD
XMKD	Extension command, the same meaning as MKD
XPWD	Extension command, the same meaning as PWD
XRMD	Extension command, the same meaning as RMD
Syntax: USER <sp> <username>.	Syntax of the <b>user</b> command: user (keyword) + space + <i>username</i>

---

## rmdir

**Syntax** `rmdir directory`

**View** FTP client view

**Parameters** *directory*: Directory name on the remote FTP server.

**Description** Use the **rmdir** command to remove a specified directory from the FTP server.

Note that only authorized users are allowed to use this command.

Note that:

- The directory to be deleted must be empty, meaning you should delete all files and the subdirectory under the directory before you delete a directory. For the deletion of files, refer to the **delete** on page 1084.
- After you execute the **rmdir** command, the files in the remote recycle bin under the directory will be automatically deleted.

**Examples** # Delete the flash:/temp1 directory from the FTP server.

```
[ftp] rmdir flash:/temp1
200 RMD command successful.
```

---

## user

**Syntax** `user username [ password ]`

<b>View</b>	FTP client view
<b>Parameters</b>	<p><i>username</i>: Other login username.</p> <p><i>password</i>: Login password.</p>
<b>Description</b>	<p>Use the <b>user</b> command to relog onto the currently accessing FTP server with other username after you have logged onto the FTP server.</p> <p>Before using this command, you must configure the corresponding username and password on the FTP server; otherwise, you login fails and the FTP connection is closed.</p>
<b>Examples</b>	<p># User <b>ftp1</b> has logged onto the FTP server and relogs onto the current FTP server with the username of <b>ftp2</b>. (Suppose username <b>ftp2</b> and password <b>123123123123</b> have been configured on the FTP server).</p> <pre>[ftp] user ftp2 331 Password required for ftp2. Password: 230 User logged in.  [ftp]</pre>

---

## verbose

<b>Syntax</b>	<p><b>verbose</b></p> <p><b>undo verbose</b></p>
<b>View</b>	FTP client view
<b>Parameters</b>	None
<b>Description</b>	<p>Use the <b>verbose</b> command to enable the verbose function to display detailed prompt information.</p> <p>Use the <b>undo verbose</b> command to disable the verbose function.</p> <p>By default, the verbose function is enabled.</p>
<b>Examples</b>	<p># Enable the verbose function.</p> <pre>[ftp] verbose FTP: verbose is on</pre>



# 82

## TFTP CLIENT CONFIGURATION COMMANDS

---

### display tftp client configuration

**Syntax** `display tftp client configuration`

**View** Any view

**Parameters** None

**Description** Use the **display tftp client configuration** command to display the configuration information of the TFTP client.

**Related commands:** **tftp client source.**

**Examples** # Display the current configuration information of the TFTP client.

```
<Sysname> display tftp client configuration
The source IP address is 192.168.0.123
```



*Currently this command displays the source address configuration information. If the currently valid source address is the source IP address, the configured source IP address is displayed; if the currently valid address is the source interface, the configured source interface is displayed.*

---

### tftp-server acl

**Syntax** `tftp-server [ ipv6 ] acl acl-number`

`undo tftp-server [ ipv6 ] acl`

**View** System view

**Parameters** **ipv6:** References an IPv6 ACL. If it is not specified, an IPv4 ACL is referenced.

*acl-number:* Number of basic ACL, in the range 2000 to 2999.

**Description** Use the **tftp-server acl** command to reference an ACL to control access to the TFTP server. Users can use the configured rules in ACL to allow or prevent the use of TFTP server in a network.

Use the **undo tftp-server acl** command to remove the access restriction.

For more information about ACL, refer to “Common ACL Configuration Commands” on page 943, “IPv4 ACL Configuration Commands” on page 947, and “IPv6 ACL Configuration Commands” on page 961.

**Examples** # Reference ACL 2000 to control access to the TFTP application in IPv4.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] tftp-server acl 2000
```

# Associate IPv6 ACL 2001 with TFTP application in Ipv6.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2030:5060::9050/64
[Sysname-acl6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

---

## tftp

**Syntax** **tftp** *server-address* { **get** | **put** | **sget** } *source-filename* [ *destination-filename* ] [ **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* } ]

**View** User view

**Parameters** *server-address*: IP address or host name of a TFTP server.

*source-filename*: Source file name.

*destination-filename*: Destination file name.

**get**: Downloads a file in normal mode.

**put**: Uploads a file.

**sget**: Downloads a file in secure mode.

**source**: Configures parameters for source address binding.

- **interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the transmission fails.
- **ip** *source-ip-address*: Specifies the source IP address for the current TFTP client to transmit packets. This source address must be the one that has been configured on the device.

**Description** Use the **tftp** command to upload files from the local device to a TFTP server or download files from the TFTP server to the local device.

- If no destination file name is specified, the saved file uses the source file name.

- The priority of the source address specified with this command is higher than that with the **tftp client source** command. If you use the **tftp client source** command to specify the source address first and then with the **tftp** command, the latter one is adopted.

This command applies to IPv4 network.

**Related commands:** **tftp client source**.

**Examples**

```
Download the config.cfg file from the TFTP server with the IP address of
192.168.0.98 and save it as config.bak. Specify the source IP address to be
192.168.0.92.

<Sysname> tftp 192.168.0.98 get config.cfg config.bak source ip 192.
168.0.92
.
File will be transferred in binary mode
Downloading file from remote tftp server, please wait...\
TFTP: 2143 bytes received in 0 second(s)
File downloaded successfully.

Upload the config.cfg file from the storage device to the default path of the TFTP
server with the IP address of 192.168.0.98 and save it as config.bak. Specify the
source IP interface to be Ethernet 1/0.

<Sysname> tftp 192.168.0.98 put config.cfg config.bak source interfa
ce Ethernet 1/0
.
File will be transferred in binary mode
Sending file to remote tftp server. Please wait... \
TFTP: 2143 bytes sent in 0 second(s).
File uploaded successfully.
```

---

## tftp client source

**Syntax** **tftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

**undo tftp client source**

**View** System view

**Parameters** **interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the transmission fails.

**ip** *source-ip-address*: The source IP address of the TFTP connection. It must be an IP address that has been configured on the device.

**Description** Use the **tftp client source** command to configure the source address of the TFTP packets from the TFTP client.

Use the **undo telnet client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the routing protocol as the source IP address to communicate with a TFTP server.

Note that:

- The source address includes the source interface and the source IP, if you use the **tftp client source** command to specify the source interface and the source IP, the newly specified source IP overwrites the original one and vice versa.
- If the source address is specified with the **tftp client source** command and then with the **tftp** command, use the latter one.
- The source address specified with the **tftp client source** command is valid for all **tftp** connections and the source address specified with the **tftp** command is valid for the current **tftp** command.

**Related commands:** **display tftp client configuration.**

**Examples**

```
Specify the source IP address of the TFTP client to 2.2.2.2.
<Sysname> system-view
[Sysname] tftp client source ip 2.2.2.2

Specify the source interface of the TFTP client to be Ethernet 1/0.

<Sysname> system-view
[Sysname] ftp client source interface ethernet 1/0
```

---

## tftp ipv6

**Syntax** **tftp ipv6** *tftp-ipv6-server* [ **-i** *interface-type interface-number* ] { **get** | **put** } *source-file* [ *destination-file* ]

**View** User view

**Parameters** *tftp-ipv6-server*: IPv6 address or host name (a string of 1 to 46 characters) of a TFTP server.

**-i** *interface-type interface-number*: Specifies the egress interface by its type and number. This parameter can be used only in case that the TFTP server address is a link local address and the specified egress interface must have a link local address (For the configuration of link local address, see *IPv6 Configuration*.).

**get**: Downloads a file.

**put**: Uploads a file.

*source-filename*: Source filename.

*destination-filename*: Destination filename. If not specified, this filename is the same as the source filename.



**Description** Use the **tftp ipv6** command to download a specified file from a TFTP server or upload a specified local file to a TFTP server.

This command applies to IPv6 network.

**Examples** # Download **filetoget.txt** from TFTP server.

```
<Sysname> tftp ipv6 fe80::250:daff:fe91:e058 -i ethernet 1/0 get filetoget.txt
```

```
File will be transferred in binary mode
```

```
Downloading file from remote tftp server, please wait...
```

```
TFTP: 32 bytes received in 5 second(s).
```

```
File downloaded successfully
```



# 83

## SFTP CONFIGURATION COMMANDS

---

### bye

**Syntax** `bye`

**View** SFTP client view

**Parameters** None

**Description** Use the **bye** command to terminate the connection with a remote SFTP server and return to system view.

This command functions as the **exit** and **quit** commands.

**Examples** # Terminate the connection with the remote SFTP server.

```
sftp-client> bye
Bye
<Sysname>
```

---

### cd

**Syntax** `cd [ remote-path ]`

**View** SFTP client view

**Parameters** *remote-path*: Name of a path on the server.

**Description** Use the **cd** command to change the working path on a remote SFTP server. With the argument not specified, the command displays the current working path.



- You can use the **cd ..** command to return to the upper-level directory.
- You can use the **cd /** command to return to the root directory of the system.

**Examples** # Change the working path to new1.

```
sftp-client> cd new1
Current Directory is:
/new1
```

---

**cdup**

<b>Syntax</b>	<b>cdup</b>
<b>View</b>	SFTP client view
<b>Parameters</b>	None
<b>Description</b>	Use the <b>cdup</b> command to return to the upper-level directory.
<b>Examples</b>	<pre># From the current working directory /new1, return to the upper-level directory. sftp-client&gt; cdup Current Directory is: /</pre>

---

**delete**

<b>Syntax</b>	<b>delete</b> <i>remote-file</i> &<1-10>
<b>View</b>	SFTP client view
<b>Parameters</b>	<i>remote-file</i> &<1-10>: Name of a file on the server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.
<b>Description</b>	Use the <b>delete</b> command to delete a specified file from a server.  This command functions as the <b>remove</b> command.
<b>Examples</b>	<pre># Delete file temp.c from the server. sftp-client&gt; delete temp.c The following files will be deleted: /temp.c Are you sure to delete it? [Y/N]:y This operation may take a long time.Please wait...  File successfully Removed</pre>

---

**dir**

<b>Syntax</b>	<b>dir</b> [ <b>-a</b>   <b>-l</b> ] [ <i>remote-path</i> ]
<b>View</b>	SFTP client view
<b>Parameters</b>	<b>-a</b> : Displays the filenames or the folder names of the specified directory.

**-l:** Displays in list form detailed information of the files and folder of the specified directory

*remote-path:* Name of the directory to be queried.

**Description** Use the **dir** command to display file and folder information under a specified directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folder under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **ls** command.

**Examples** # Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 config.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
-rwxrwxrwx 1 noone nogroup 225 Sep 28 08:28 pub1
drwxrwxrwx 1 noone nogroup 0 Sep 28 08:24 new1
drwxrwxrwx 1 noone nogroup 0 Sep 28 08:18 new2
-rwxrwxrwx 1 noone nogroup 225 Sep 28 08:30 pub2
```

## exit

**Syntax** **exit**

**View** SFTP client view

**Parameters** None

**Description** Use the **exit** command to terminate the connection with a remote SFTP server and return to system view.

This command functions as the **bye** and **quit** commands.

**Examples** # Terminate the connection with the remote SFTP server.

```
sftp-client> exit
Bye
<Sysname>
```

## get

**Syntax** **get** *remote-file* [ *local-file* ]

**View** SFTP client view

**Parameters** *remote-file*: Name of a file on the remote SFTP server.

*local-file*: Name for the local file.

**Description** Use the **get** command to download a file from a remote SFTP server and save it locally.

If you do not specify the *local-file* argument, the file will be saved locally with the same name as that on the remote SFTP server.

**Examples** # Download file temp1.c and save it as temp.c locally.

```
sftp-client> get temp1.c temp.c
Remote file:/temp1.c ---> Local file: temp.c
Downloading file successfully ended
```

## help

**Syntax** **help** [ **all** | *command-name* ]

**View** SFTP client view

**Parameters** **all**: Displays a list of all commands.

*command-name*: Name of a command.

**Description** Use the **help** command to display a list of all commands or the help information of an SFTP client command.

With neither the argument nor the keyword specified, the command displays a list of all commands.

**Examples** # Display the help information of the **get** command.

```
sftp-client> help get
get remote-path [local-path] Download file.Default local-path is the same
with remote-path
```

## ls

**Syntax** **ls** [ **-a** | **-l** ] [ *remote-path* ]

**View** SFTP client view

**Parameters** **-a**: Displays the filenames or the folder names of the specified directory.

**-l**: Displays in list form detailed information of the files and folder of the specified directory

*remote-path*: Name of the directory to be queried.

**Description** Use the **ls** command to display file and folder information under a specified directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folder under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **dir** command.

**Examples** # Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> ls
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 config.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
-rwxrwxrwx 1 noone nogroup 225 Sep 28 08:28 pub1
drwxrwxrwx 1 noone nogroup 0 Sep 28 08:24 new1
drwxrwxrwx 1 noone nogroup 0 Sep 28 08:18 new2
-rwxrwxrwx 1 noone nogroup 225 Sep 28 08:30 pub2
```

## mkdir

**Syntax** **mkdir** *remote-path*

**View** SFTP client view

**Parameters** *remote-path*: Name for the directory on a remote SFTP server.

**Description** Use the **mkdir** command to create a directory on a remote SFTP server.

**Examples** # Create a directory named **test** on the remote SFTP server.

```
sftp-client> mkdir test
New directory created
```

## put

**Syntax** **put** *local-file* [ *remote-file* ]

**View** SFTP client view

**Parameters** *local-file*: Name of a local file.

*remote-file*: Name for the file on a remote SFTP server.

**Description** Use the **put** command to upload a local file to a remote SFTP server.

If you do not specify the *remote-file* argument, the file will be saved remotely with the same name as the local one.

**Examples** # Upload local file temp.c to the remote SFTP server and save it as temp1.c.

```
sftp-client> put temp.c temp1.c
Local file:temp.c ---> Remote file: /temp1.c
Uploading file successfully ended
```

## pwd

**Syntax** **pwd**

**View** SFTP client view

**Parameters** None

**Description** Use the **pwd** command to display the current working directory of a remote SFTP server.

**Examples** # Display the current working directory of the remote SFTP server.

```
sftp-client> pwd
/
```

## quit

**Syntax** **quit**

**View** SFTP client view

**Parameters** None

**Description** Use the **quit** command to terminate the connection with a remote SFTP server and return to system view.

This command functions as the **bye** and **exit** commands.

**Examples** # Terminate the connection with the remote SFTP server.

```
sftp-client> quit
Bye
<Sysname>
```



---

**remove**

**Syntax** `remove remote-file<1-10>`

**View** SFTP client view

**Parameters** *remote-file<1-10>*: Name of a file on an SFTP server. <1-10> means that you can provide up to 10 filenames, which are separated by space.

**Description** Use the **remove** command to delete a specified file from a remote server.  
This command functions as the **delete** command.

**Examples** # Delete file temp.c from the server.  

```
sftp-client> remove temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

---

**rename**

**Syntax** `rename oldname newname`

**View** SFTP client view

**Parameters** *oldname*: Original file name or directory name.  
*newname*: New file name or directory name.

**Description** Use the **rename** command to change the name of a specified file or directory on an SFTP server.

**Examples** # Change the name of a file on the SFTP server from temp1.c to temp2.c.  

```
sftp-client> rename temp1.c temp2.c
File successfully renamed
```

---

**rmdir**

**Syntax** `rmdir remote-path<1-10>`

**View** SFTP client view

**Parameters** *remote-path*&<1-10>: Name of the directory on the remote SFTP server. &<1-10> means that you can provide up to 10 filenames that are separated by space.

**Description** Use the **rmdir** command to delete a specified directory from an SFTP server.

**Examples** # On the SFTP server, delete directory temp1 in the current directory.

```
sftp-client> rmdir temp1
Directory successfully removed
```

# 84

## INFORMATION CENTER CONFIGURATION COMMANDS

---

### display channel

**Syntax** `display channel [ channel-number | channel-name ]`

**View** Any view

**Parameters** *channel-number*: Displays information of the channel with a specified number, where *channel-number* represents the channel number, in the range 0 to 9.

*channel-name*: Displays information of the channel with a specified name, where *channel-name* represents the channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** on page 1142.

**Table 267** Information channels for different output destinations

Output destination	Information channel number	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP NMS	5	snmpagent
Log file	9	channel9

**Description** Use the **display channel** command to display channel information.

If no channel is specified, information for all channels is displayed.

**Examples** # Display information for channel 0.

```
<Sysname> display channel 0
channel number:0, channel name:console
MODU_ID NAME ENABLE LOG_LEVEL ENABLE TRAP_LEVEL ENABLE DEBUG_LEVEL
ffff0000 default Y warnings Y debugging Y debugging
```

**Table 268** Field descriptions of the display channel command

Field	Description
channel number	A specified channel number, in the range 0 to 9.

**Table 268** Field descriptions of the display channel command

Field	Description
channel name	A specified channel name, which varies with user's configuration. For more information, refer to the <b>info-center channel name</b> on page 1142.
MODU_ID	The ID of the module to which the information permitted to pass through the current channel belongs
NAME	The name of the module to which the information permitted to pass through the current channel belongs Default means all modules are allowed to output system information, but the module type varies with devices.
ENABLE	Indicates whether to enable or disable the output of log information, which could be Y or N.
LOG_LEVEL	The severity of log information, refer to Table 270 for details.
ENABLE	Indicates whether to enable or disable the output of trap information, which could be Y or N.
TRAP_LEVEL	The severity of trap information, refer to Table 270 for details.
ENABLE	Indicates whether to enable or disable the output of debugging information, which could be Y or N.
DEBUG_LEVEL	The severity of debugging information, refer to Table 270 for details.

The above information indicates to output log information with the severity from 0 to 4, trap information with the severity from 0 to 7 and debugging information with the severity from 0 to 7 to the console. The information source modules are all modules (default).

---

## display info-center

**Syntax** `display info-center`

**View** Any view

**Parameters** None

**Description** Use the **display info-center** command to display configurations on each output destination.

**Examples** # Display configurations on each output destination.

```
<Sysname> display info-center
Information Center:enabled
Log host:
 2.2.2.2, channel number : 8, channel name : channel8,
 host facility local7
Console:
 channel number : 0, channel name : console
Monitor:
 channel number : 1, channel name : monitor
SNMP Agent:
 channel number : 5, channel name : snmpagent
Log buffer:
 enabled,max buffer size 1024, current buffer size 512,
 current messages 512, dropped messages 0, overwritten messages 740
 channel number : 4, channel name : logbuffer
```

```

Trap buffer:
 enabled,max buffer size 1024, current buffer size 256,
 current messages 216, dropped messages 0, overwritten messages 0
 channel number : 3, channel name : trapbuffer
logfile:
 channel number:9, channel name:channel9
Information timestamp setting:
 log - date, trap - date, debug - date,
 loghost - date

```

**Table 269** Field descriptions of the display info-center command

Field	Description
Information Center	The current state of the information center, which could be enabled or disabled.
Log host: 2.2.2.2, channel number: 8, channel name: channel8, host facility local7	The information of the log host channel (It can be displayed only when the <b>info-center loghost</b> command is configured), including IP address of the log host, the channel number(s) and channel name(s) used, and logging facility used.)
Console: channel number: 0, channel name: console	The console channel information, including the channel number(s) and channel name(s) used
Monitor: channel number: 1, channel name: monitor	The monitor channel information, including the channel number(s) and channel name(s) used
SNMP Agent: channel number: 5, channel name: snmpagent	The SNMP agent channel information, including the channel number(s) and channel name(s) used
Log buffer: enabled,max buffer size 1024, current buffer size 512, current messages 512, dropped messages 0, overwritten messages 740 channel number: 4, channel name: logbuffer	The information of the log buffer channel, including whether it is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number(s) and channel name(s) used.
Trap buffer: enabled,max buffer size 1024, current buffer size 256, current messages 216, dropped messages 0, overwritten messages 0 channel number: 3, channel name: trapbuffer	The information of the trap buffer channel, including whether it is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number(s) and channel name(s) used.
logfile: channel number:9, channel name:channel9	The logfile configurations information, including the channel number(s), and channel name(s) used.
Information timestamp setting	The timestamp configurations, specifying the timestamp format for log, trap, debug, and log host information.



*Only devices that support the logfile feature display the related logfile information after the execution of the **display info-center** command.*

---

**display logbuffer**

**Syntax** **display logbuffer** [ **level** *severity* | **size** *buffersize* | **slot** *slotnum* ] \* [ | { **begin** | **exclude** | **include** } *text* ]

**View** Any view

**Parameters** **level** *severity*: Displays information of the log with specified level, where *severity* represents information level, in the range 0 to 7.

**Table 270** Severity description

Severity	Value	Description
emergencies	0	The system is unavailable
alerts	1	Information that requires prompt reaction
critical	2	Critical information
errors	3	Error information
warnings	4	Warnings
notifications	5	Normal errors with important information
informational	6	Informational information to be recorded
debugging	7	Debugging information

**size** *buffersize*: Displays specified number of the latest log messages in the log buffer, where *buffersize* represents the number of the latest log messages to be displayed in the log buffer, in the range 1 to 1,024.

**slot** *slotnum*: Slot number.

|: Uses a regular expression to filter the output information. For detailed information about regular expression, refer to "Parameters" on page 1165.

- **begin**: Displays the line that matches the regular expression and all the subsequent lines.
- **exclude**: Displays the lines that do not match the regular expression.
- **include**: Displays the lines that match the regular expression.

*text*: Regular expression, a string of 1 to 256 characters. Note that this argument is case-sensitive and can have spaces included.

**Table 271** Meanings of characters in text

Character	Meaning	Remarks
^	Starting sign, the string following it appears only at the beginning of a line.	Regular expression " <b>^</b> user" matches a string begins with "user", not "Auser".
\$	Ending sign, the string before it appears only at the end of a line.	Regular expression "user <b>\$</b> " matches a string ends with "user", not "userA".
.	Full stop, a wildcard used in place of any character, including blank	None

**Table 271** Meanings of characters in text

Character	Meaning	Remarks
*	Asterisk, used to match a sub expression before it zero or multiple times	zo* can map to "z" and "zoo".
+	Addition, used to match a sub expression before it one or multiple times	zo+ can map to "zo" and "zoo", but not "z".
-	Hyphen. It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, "1-9" means numbers from 1 to 9 (inclusive); "a-h" means from a to h (inclusive).
[ ]	Selects one character from the group.	For example, [1-36A] can match only one character among 1, 2, 3, 6, and A.
( )	A group of characters. It is usually used with "+" or "*".	For example, (123A) means a string "123A"; "408(12)+" can match 40812 or 408121212. But it cannot match 408. That is, "12" can appear continuously and it must at least appear once.

**Description** Use the **display logbuffer** command to display the state of the log buffer and the log information recorded. Absence of the **size buffersize** argument indicates that all log information recorded in the log buffer is displayed.

**Examples** # Display the state of the log buffer and the log information recorded on the device.

```
<Sysname> display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 6
```

```
%Apr 26 17:50:00:681 2007 3Com DEV/4/FAN ABSENT:
 Fan 1 is absent.
.....Omitted.....
```

**Table 272** Descriptions on the fields of the display logbuffer command

Field	Description
Logging buffer configuration and contents	Indicates the current state of the log buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size
Channel number	The channel number of the log buffer, defaults to 4
Channel name	The channel name of the log buffer, defaults to logbuffer
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages

---

**display logbuffer summary**

**Syntax** **display logbuffer summary** [ **level** *severity* | **slot** *slotnum* ] \*

**View** Any view

**Parameters** **level** *severity*: Displays the summary of the log buffer, where *severity* represents information level, in the range 0 to 7.

**slot** *slotnum*: Slot number.

**Description** Use the **display logbuffer summary** command to display the summary of the log buffer.

**Examples** # Display the summary of the log buffer on the device.

```
<Sysname> display logbuffer summary
 SLOT EMERG ALERT CRIT ERROR WARN NOTIF INFO DEBUG
 0 0 0 0 0 0 0 0 0
 1 0 0 0 0 0 0 0 0
 2 0 0 0 0 0 0 0 0
 3 0 0 0 0 16 0 1 0
```

**Table 273** Descriptions on the fields of the display logbuffer summary command

Field	Description
SLOT	Slot number
EMERG	Represents emergencies, refer to Table 270 for details
ALERT	Represents alerts, refer to Table 270 for details
CRIT	Represents critical, refer to Table 270 for details
ERROR	Represents errors, refer to Table 270 for details
WARN	Represents warnings, refer to Table 270 for details
NOTIF	Represents notifications, refer to Table 270 for details
INFO	Represents informational, refer to Table 270 for details
DEBUG	Represents debugging, refer to Table 270 for details

---

**display logfile buffer**

**Syntax** **display logfile buffer**

**View** Any view

**Parameters** None

**Description** Use the **display logfile buffer** command to display contents of the logfile buffer.

Note that all contents in the logfile buffer will be cleared after they are successfully saved into the log file automatically or manually.



**Examples** # Display the contents of the logfile buffer.

```
<Sysname> display logfile buffer
%@0%May 8 07:18:51 2007 3Com %%10IC/6/SYS_RESTART:
System restarted --
3Com Comware Software
.....Omitted.....
```

---

## display logfile summary

**Syntax** **display logfile summary**

**View** Any view

**Parameters** None

**Description** Use the **display logfile summary** command to display the configuration of the log file.

**Examples** # Display the configuration of the log file.

```
<Sysname> display logfile summary
Log file is enabled.
Channel number : 9
Log file size quota : 1 MB
Log file directory : cf:/logfile
Writing frequency : 24 hour 0 min 0 sec
```

**Table 274** Descriptions on the fields of the display logfile summary command

Field	Description
Log file is	The current state of a log file, which could be enabled or disabled.
Channel number	The channel number of a log file, defaults to 9.
Log file size quota	The maximum storage space reserved for a log file
Log file directory	Log file directory
Writing frequency	Log file writing frequency

---

## display trapbuffer

**Syntax** **display trapbuffer** [ *size buffersize* ]

**View** Any view

**Parameters** **size buffersize**: Displays specified number of the latest trap messages in a trap buffer, where *buffersize* represents the number of the latest trap messages in a trap buffer, in the range 1 to 1,024.

**Description** Use the **display trapbuffer** command to display the state and the trap information recorded.

Absence of the **size** *buffersize* argument indicates that all trap information is displayed.

**Examples** # Display the state of the trap buffer and the trap information recorded.

```
<Sysname> display trapbuffer
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 0
```

**Table 275** Descriptions on the fields of the display trapbuffer command

Field	Description
Trapping buffer configuration and contents	Indicates the current state of the trap buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size
Channel number	The channel number of the trap buffer, defaults to 3
Channel name	The channel name of the trap buffer, defaults to trapbuffer
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages

---

## info-center channel name

**Syntax** **info-center channel** *channel-number* **name** *channel-name*

**undo info-center channel** *channel-number*

**View** System view

**Parameters** *channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, a string of 1 to 30 characters, case insensitive. It must be an alphanumeric set starting with a letter.

**Description** Use the **info-center channel name** command to name a channel with a specified channel number.

Use the **undo info-center channel** command to restore the default name for a channel with a specified channel number.

Refer to Table 267 for details of default channel names and channel numbers.

**Examples** # Name channel 0 as **abc**.

```
<Sysname> system-view
[Sysname] info-center channel 0 name abc
```

---

## info-center console channel

**Syntax** **info-center console channel** { *channel-number* | *channel-name* }

**undo info-center console channel**

**View** System view

**Parameters** *channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to **info-center channel name** on page 1142.

**Description** Use the **info-center console channel** command to specify the channel to output system information to the console.

Use the **undo info-center console channel** command to restore the default output channel to the console.

By default, output of information to the console is enabled with channel 0 as the default channel (known as console).

Note that the **info-center console channel** command takes effect only after the information center is enabled first with the **info-center enable** command.

**Examples** # Set channel 0 to output system information to the console.

```
<Sysname> system-view
[Sysname] info-center console channel 0
```

---

## info-center enable

**Syntax** **info-center enable**

**undo info-center enable**

**View** System view

**Parameters** None

**Description** Use the **info-center enable** command to enable information center.

Use the **undo info-center enable** command to disable the information center.

The system outputs information to the log host or the console only after the information center is enabled first.

By default, the information center is enabled.

**Examples** # Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
% Information center is enabled
```

---

## info-center logbuffer

**Syntax** **info-center logbuffer** [ **channel** { *channel-number* | *channel-name* } | **size** *buffersize* ] \*

**undo info-center logbuffer** [ **channel** | **size** ]

**View** System view

**Parameters** *buffersize*: Specifies the maximum number of log messages in a log buffer, in the range 0 to 1,024 with 512 as the default value.

*channel-number*: A specified channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to **info-center channel name** on page 1142.

**Description** Use the **info-center logbuffer** command to enable information output to a log buffer and set the corresponding parameters.

Use the **undo info-center logbuffer** command to disable information output to a log buffer.

By default, information output to the log buffer is enabled with channel 4 (logbuffer) as the default channel and a maximum buffer size of 512.

Note that the **info-center logbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

**Examples** # Enable the system to output information to the log buffer using channel 4, with a default buffer size of 50.

```
<Sysname> system-view
[Sysname] info-center logbuffer size 50
```

---

## info-center logfile enable

**Syntax** **info-center logfile enable**

**undo info-center logfile enable****View** System view**Parameters** None**Description** Use the **info-center logfile enable** command to enable the output of system information to the log file.Use the **undo info-center logfile enable** command to disable the output of system information to the log file.

By default, the output of system information to the log file is enabled.

**Examples** # Enable the log file feature.

```
<Sysname> system-view
[Sysname] info-center logfile enable
```

**info-center logfile frequency****Syntax** **info-center logfile frequency** *freq-sec***undo info-center logfile frequency****View** System view**Parameters** *freq-sec*: Frequency with which the system saves the log file, in the range 1 to 86,400 seconds, defaults to 86400 seconds.**Description** Use the **info-center logfile frequency** command to configure the frequency with which the system saves the log file.Use the **undo info-center logfile frequency** command to restore the default frequency.

**Examples** # Configure the frequency with which the system saves the log file as 60,000 seconds.

```
<Sysname> system-view
[Sysname] info-center logfile frequency 60000
```

**info-center logfile size-quota****Syntax** **info-center logfile size-quota** *size***undo info-center logfile size-quota****View** System view

**Parameters** *size*: The maximum capacity of a disk, in MB, in the range 1 MB to 10 MB, defaults to 1 MB.

**Description** Use the **info-center logfile size-quota** command to set the maximum storage space reserved for a log file.

Use the **undo info-center logfile size-quota** command to restore the default maximum storage space reserved for a log file.

**Examples** # Set the maximum storage space reserved for a log file to 6 MB.

```
<Sysname> system-view
[Sysname] info-center logfile size-quota 6
```

## info-center logfile switch-directory

**Syntax** **info-center logfile switch-directory** *dir-name*

**View** System view

**Parameters** *dir-name*: The name of the directory where a log file is saved, a string of 1 to 64 characters.

**Description** Use the **info-center logfile switch-directory** command to configure the directory where a log file is saved. Ensure that the directory is created first before saving a log file into it.

By default, the directory to save a log file is the logfile directory under the root directory of the CF module, that is, *cf:/logfile*.

Note that this command can be used to configure the directory to which a log file can be saved. The configuration will lose after system restart or active/standby switchover of the main control modules.

**Examples** # Create a directory with the name **test** under flash root directory.

```
<Sysname> mkdir test
%Created dir flash:/test.
```

# Set the directory to save the log file to *flash:/test*.

```
<Sysname> system-view
[Sysname] info-center logfile switch-directory flash:/test
```

## info-center loghost

**Syntax** **info-center loghost** *host-ip* [ **channel** { *channel-number* | *channel-name* } | **facility** *local-number* ] \*

**undo info-center loghost** *host-ip*

**View** System view

**Parameters** *host-ip*: The IP address of the log host.

**channel**: Specifies the channel through which system information can be output to the log host.

*channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to **info-center channel name** on page 1142.

**facility local-number**: The logging facility of the log host. The *local-number* argument ranges from local0 to local7, with the corresponding value ranging from 16 to 23. The default logging facility is local7, with the value being 23. Logging facility is mainly used to mark the log sources on the log host, query and filter log information of the corresponding log source.

**Description** Use the **info-center loghost** command to specify a log host and to configure the related parameters.

Use the **undo info-center loghost** command to restore the default configurations on a log host.

By default, output of system information to the log host is disabled. When it is enabled, the default channel name will be loghost and the default channel number will be 2.

Note that:

- The **info-center loghost** command takes effect only after the information center is enabled with the **info-center enable** command.
- Ensure to input a correct IP address while using the **info-center loghost** command to configure the IP address for a log host. System will prompt an invalid address if the loopback address (127.0.0.1) is input.
- A maximum number of 4 hosts (different) can be designated as the log host.

**Examples** # Set to output log information to a Unix station with the IP address being 1.1.1.1/16.

```
<Sysname> system-view
[Sysname] info-center loghost 1.1.1.1
```

---

## info-center loghost source

**Syntax** **info-center loghost source** *interface-type interface-number*

**undo info-center loghost source**

<b>View</b>	System view
<b>Parameters</b>	<i>interface-type interface-number</i> : Specifies a source interface by its type and number.
<b>Description</b>	<p>Use the <b>info-center loghost source</b> command to configure the source interface to output log information to the log host.</p> <p>Use the <b>undo info-center loghost source</b> command to remove the source interface to output log information to the log host.</p> <p>By default, no source interface is configured to output log information to the log host, and the system selects an interface as the source interface.</p> <p>Note that the <b>info-center loghost source</b> command takes effect only after the information center is enabled with the <b>info-center enable</b> command.</p>
<b>Examples</b>	<p># Configure the interface VLAN-interface 1 as the source interface to output log information to the log host.</p> <pre>&lt;Sysname&gt; system-view [Sysname] info-center loghost source Vlan-interface 1</pre>

---

## info-center monitor channel

<b>Syntax</b>	<b>info-center monitor channel</b> { <i>channel-number</i>   <i>channel-name</i> }  <b>undo info-center monitor channel</b>
<b>View</b>	System view
<b>Parameters</b>	<p><i>channel-number</i>: Specifies a channel number, in the range 0 to 9.</p> <p><i>channel-name</i>: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to <b>info-center channel name</b> on page 1142.</p>
<b>Description</b>	<p>Use the <b>info-center monitor channel</b> command to configure the channel to output system information to the monitor.</p> <p>Use the <b>undo info-center monitor channel</b> command to restore the default channel to output system information to the monitor.</p> <p>By default, output of system information to the monitor is enabled with a default channel name of monitor and a default channel number of 1.</p> <p>Note that the <b>info-center monitor channel</b> command takes effect only after the information center is enabled with the <b>info-center enable</b> command.</p>
<b>Examples</b>	# Set to output system information to the monitor through channel 0.



```
<Sysname> system-view
[Sysname] info-center monitor channel 0
```

---

## info-center snmp channel

**Syntax** **info-center snmp channel** { *channel-number* | *channel-name* }

**undo info-center snmp channel**

**View** System view

**Parameters** *channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to **info-center channel name** on page 1142.

**Description** Use the **info-center snmp channel** command to configure the channel to output system information to the SNMP NMS.

Use the **undo info-center snmp channel** command to restore the default channel to output system information to the SNMP NMS.

By default, output of system information to the SNMP NMS is enabled with a default channel name of snmpagent and a default channel number of 5.

For more information, refer to the **display snmp-agent** commands in “SNMP Configuration Commands” on page 1023.

**Examples** # Set to output system information to the SNMP NMS through channel 6.

```
<Sysname> system-view
[Sysname] info-center snmp channel 6
```

---

## info-center source

**Syntax** **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [ **debug** { **level** *severity* | **state** *state* } \* | **log** { **level** *severity* | **state** *state* } \* | **trap** { **level** *severity* | **state** *state* } \* ] \*

**undo info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }

**View** System view

**Parameters** *module-name*: Specifies the output rules of the system information of the specified modules, which vary with devices. For instance, if information on ARP module is to be output, you can configure this argument as ARP.

**default:** Specifies the output rules of the system information of all the modules allowed to output the system information. This configuration varies with devices.

**debug:** Debugging information.

**log:** Log information.

**trap:** Trap information.

**level severity:** Specifies the severity of system information, refer to Table 270 for details.

**state state:** The state of system information output, which could be **on** (enabled) or **off** (disabled).

*channel-number:* Specifies a channel number, in the range 0 to 9.

*channel-name:* Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to **info-center channel name** on page 1142.

**Description** Use the **info-center source** command to specify the output rules of the system information.

Use the **undo info-center source** command to remove the specified output rules.

By default, the output rules for the system information are listed in Table 276.

This command can be used to configure the filter and redirection rules of log/trap/debugging information.

For example, the user can set to output log information with severity higher than warnings to the log host, and information with severity higher than informational to the log buffer. The user can also set to output trap information of the IP module to a specified output destination.

Note that:

- If you do not use the *module-name* argument to set output rules for a module, the module uses the default output rules or the output rules set by the **default** keyword; otherwise the module uses the output rules separately set for it.
- When you use the *module-name* argument to separately set the output rules for a module, the default output rules for the module are as follows: Log and trap information is enabled, with severity being informational; debugging information is disabled, with severity being debugging.
- After you separately set the output rules for a module, you must use the *module-name* argument to modify or remove the rules. The new configuration by using the **default** keyword is invalid on the module.

**Table 276** Default output rules for different output destinations

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/disabled	Severity	Enabled/disabled	Severity	Enabled/disabled	Severity
Console	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Monitor terminal	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Log host	default (all modules)	Enabled	informational	Enabled	debugging	Disabled	debugging
Trap buffer	default (all modules)	Disabled	informational	Enabled	warnings	Disabled	debugging
Log buffer	default (all modules)	Enabled	warnings	Disabled	debugging	Disabled	debugging
SNMP NMS	default (all modules)	Disabled	debugging	Enabled	warnings	Disabled	debugging
Log file	default (all modules)	Enabled	debugging	Enabled	debugging	Disabled	debugging

**Examples** # Set the output channel for the log information of VLAN module to snmpagent and to output information with severity being emergencies.

```
<Sysname> system-view
[Sysname] info-center source vlan channel snmpagent log level emergencies state on
```

## info-center synchronous

**Syntax** **info-center synchronous**

**undo info-center synchronous**

**View** System view

**Parameters** None

**Description** Use the **info-center synchronous** command to enable synchronous information output.

Use the **undo info-center synchronous** command to disable the synchronous information output.

By default, the synchronous information output is disabled.



- If system information, such as log information, is output before you input any information under the current command line prompt, the system will not display the command line prompt after the system information output.
- If system information is output when you are inputting some interactive information (non Y/N confirmation information), then after the system information output, the system will not display the command line prompt but your previous input in a new line.

**Examples** # Enable synchronous information output.

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
```

# The user receives log messages when he/she is about to display the configurations for an Ethernet interface by inputting the **display interface ethe** command. After the system has finished its output of log messages, it will display the user's original input, which is "display interface ethe" in this case.

```
<Sysname> system-view
[Sysname] display interface ethe
%Aug 14 17:10:33:438 2007 3Com SHELL/4/LOGOUT: VTY logout from 192.1
68.0.72
[Sysname]display interface ethe
```

---

## info-center timestamp

**Syntax** **info-center timestamp { debugging | log | trap } { boot | date | none }**

**undo info-center timestamp { debugging | log | trap }**

**View** System view

**Parameters** **debugging**: Sets the timestamp format of the debugging information.

**log**: Sets the timestamp output format of the log information.

**trap**: Sets the timestamp output format of the trap information.

**boot**: The time taken to boot up the system, in the format of xxxxxx.yyyyyy, in which xxxxxx represents the most significant 32 bits of the time taken to boot up the system (in milliseconds) whereas yyyyyy is the least significant 32 bits.

**date**: The current system date and time, in the format of "Mmm dd hh:mm:ss:sss yyyy".

- Mmm: The abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- dd: The date, starting with a space if less than 10, for example " 7".
- hh:mm:ss:sss: The local time, with hh ranging from 00 to 23, mm and ss ranging from 00 to 59, and sss ranging from 0 to 999.
- yyyy: Represents the year.

**none**: Indicates no time information is provided.

**Description** Use the **info-center timestamp** command to configure the timestamp format.

Use the **undo info-center timestamp** command to restore the default.

By default, the timestamp format of log, trap and debugging information is **date**.

**Examples** # Configure the timestamp format for debugging information as **boot**.

```
<Sysname> system-view
[Sysname] info-center timestamp debugging boot
```

---

## info-center timestamp loghost

**Syntax** **info-center timestamp loghost** { **date** | **no-year-date** | **none** }

**undo info-center timestamp loghost**

**View** System view

**Parameters** **date**: Indicates the current system date and time, the format of which depends on the log host.

**no-year-date**: Indicates the current system date and time (year exclusive).

**none**: Indicates that no timestamp information is provided.

**Description** Use the **info-center timestamp loghost** command to configure the timestamp format of the system information sent to the log host.

Use the **undo info-center timestamp loghost** command to restore the default.

By default, the timestamp format for system information sent to the log host is **date**.

**Examples** # Configure to exclude the year information in the time stamp of the system information output to the log host.

```
<Sysname> system-view
[Sysname] info-center timestamp loghost no-year-date
```

---

## info-center trapbuffer

**Syntax** **info-center trapbuffer** [ **channel** { *channel-number* | *channel-name* } | **size** *buffersize* ] \*

**undo info-center trapbuffer** [ **channel** | **size** ]

**View** System view

**Parameters** **size** *buffersize*: Specifies the maximum number of trap messages in a trap buffer, in the range 0 to 1,024 with 256 as the default value.

*channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it

as a self-defined channel name. For more information, refer to **info-center channel name** on page 1142.

**Description** Use the **info-center trapbuffer** command to enable information output to the trap buffer and set the corresponding parameters.

Use the **undo info-center trapbuffer** command to disable information output to the trap buffer.

By default, information output to the trap buffer is enabled with channel 3 (trapbuffer) as the default channel and a maximum buffer size of 256.

Note that the **info-center trapbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

**Examples** # Enable system to output information to the trap buffer using the default channel, with a default buffer size of 30.

```
<Sysname> system-view
[Sysname] info-center trapbuffer size 30
```

## logfile save

**Syntax** **logfile save**

**View** Any view

**Parameters** None

**Description** Use the **logfile save** command to manually save the log buffer contents into the log file.

By default, the system automatically saves the log file based on a frequency configured by the **info-center logfile frequency** command into a directory configured by the **info-center logfile switch-directory** command.

Note that all contents in the logfile buffer will be cleared after they are successfully saved into the log file automatically or manually.



*By default, the logfile is automatically saved under the logfile directory (cf://logfile) of the CF module. If there is no CF module on the device, you need to use the **info-center logfile switch-directory** command to specify the directory to save the file; otherwise, the system prompts error.*

**Examples** # Set to manually save the log buffer contents into the log file.

```
<Sysname> logfile save
```

---

## reset logbuffer

**Syntax** `reset logbuffer`

**View** User view

**Parameters** None

**Description** Use the **reset logbuffer** command to reset the log buffer contents.

**Examples** # Reset the log buffer contents.  
`<Sysname> reset logbuffer`

---

## reset trapbuffer

**Syntax** `reset trapbuffer`

**View** User view

**Parameters** None

**Description** Use the **reset trapbuffer** command to reset the trap buffer contents.

**Examples** # Reset the trap buffer contents.  
`<Sysname> reset trapbuffer`

---

## terminal debugging

**Syntax** `terminal debugging`  
`undo terminal debugging`

**View** User view

**Parameters** None

**Description** Use the **terminal debugging** command to enable the display of debugging information on the current terminal.

Use the **undo terminal debugging** command to disable the display of debugging information on the current terminal.

By default, the display of debugging information on the current terminal is disabled.

Note that the debugging information is displayed (using the **terminal debugging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

**Examples** # Enable the display of debugging information on the current terminal.

```
<Sysname> terminal debugging
% Current terminal debugging is on
```

---

## terminal logging

**Syntax** **terminal logging**

**undo terminal logging**

**View** User view

**Parameters** None

**Description** Use the **terminal logging** command to enable the display of log information on the current terminal.

Use the **undo terminal logging** command to disable the display of log information on the current terminal.

By default, the display of log information on the current terminal is disabled.

Note that the log information is displayed (using the **terminal logging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

**Examples** # Disable the display of log information on the current terminal.

```
<Sysname> undo terminal logging
% Current terminal logging is off
```

---

## terminal monitor

**Syntax** **terminal monitor**

**undo terminal monitor**

**View** User view

**Parameters** None

**Description** Use the **terminal monitor** command to enable the monitoring of system information on the current terminal.



Use the **undo terminal monitor** command to disable the monitoring of system information on the current terminal.

- You need to configure the **terminal monitor** command before you can display the log, trap, and debugging information.
- Configuration of the **undo terminal monitor** command automatically disables the monitoring of log, trap, and debugging information.

By default, the monitoring of the console is enabled and the monitoring of the terminal is disabled.

**Examples** # Enable the monitoring of system information on the current terminal.

```
<Sysname> terminal monitor
% Current terminal monitor is on
```

## terminal trapping

**Syntax** **terminal trapping**

**undo terminal trapping**

**View** User view

**Parameters** None

**Description** Use the **terminal trapping** command to enable the display of trap information on the current terminal.

Use the **undo terminal trapping** command to disable the display of trap information on the current terminal.

By default, the display of trap information on the current terminal is enabled.

Note that the trap information is displayed (using the **terminal trapping** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

**Examples** # Enable the display of trap information on the current terminal.

```
<Sysname> terminal trapping
% Current terminal trapping is on
```



# 85

## BASIC CONFIGURATION COMMANDS

---

### clock datetime

**Syntax** `clock datetime time date`

**View** User view

**Parameters** *time*: Current time in the format of *HH:MM:SS*, where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59. The zeros in the argument can be omitted except for indicating 0 hours.

*date*: Current date in the format of *MM/DD/YYYY* or *YYYY/MM/DD*. *MM* is the month of the year in the range 1 to 12, *DD* is the day of the month that varies with months, and *YYYY* is a year in the range 2000 to 2035.

**Description** Use the **clock datetime** command to set the current time and date of the device.

The current time and date of the device must be set in an environment that requires the acquisition of absolute time.

You may choose not to provide seconds when inputting the time parameters.

**Related commands:** **clock summer-time one-off**, **clock summer-time repeating**, **clock timezone**, **display clock**.

**Examples** # Set the current system time to 14:10:20 08/01/2005.  
`<Sysname> clock datetime 14:10:20 8/1/2005`  
# Set the current system time to 00:06:00 01/01/2007.  
`<Sysname> clock datetime 0:6 2007/1/1`

---

### clock summer-time one-off

**Syntax** `clock summer-time zone-name one-off start-time start-date end-time end-date add-time`

`undo clock summer-time`

**View** User view

**Parameters** *zone-name*: Name of the summer time, a string of 1 to 32 characters. It is case sensitive.

*start-time*: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

*start-date*: Start date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

*end-time*: End time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

*end-date*: End date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

*add-time*: Time added to the standard time of the device, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

**Description** Use the **clock summer-time one-off** command to adopt summer time from the *start-time* of the *start-date* to the *end-time* of the *end-date*. Summer time adds the *add-time* to the current time of the device.

Use the **undo clock summer-time** command to cancel the configuration of the summer time.

After the configuration takes effect, you can use the **display clock** command to view it. Besides, the time of the log or debug information is the local time of which the time zone and summer time have been adjusted.

Note that:

- The time range from *start-time* in *start-date* to *end-time* in *end-date* must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.
- If the current system time is in the time range specified with this command, the system time automatically adds "add-time" after the execution of this command.

**Related commands:** **clock datetime**, **clock summer-time repeating**, **clock timezone**, **display clock**.

**Examples** # For daylight saving time in **abc1** between 06:00:00 on 08/01/2006 and 06:00:00 on 09/01/2006, set the system clock ahead one hour.

```
<Sysname> clock summer-time abc1 one-off 6 08/01/2006 6 09/01/2006 1
```

---

## clock summer-time repeating

**Syntax** **clock summer-time** *zone-name* **repeating** *start-time* *start-date* *end-time* *end-date* *add-time*

## undo clock summer-time

**View** User view

**Parameters** *zone-name*: Name of the daylight saving time, a string of 1 to 32 characters.

*start-time*: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

*start-date*: Start date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January, February, March, April, May, June, July, August, September, October, November** or **December**; the start week can be the **first, second, third, fourth, fifth** or **last** week of the month; the start date is **Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday**.

*end-time*: End time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

*end-date*: End date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January, February, March, April, May, June, July, August, September, October, November** or **December**; the end week can be the **first, second, third, fourth, fifth** or **last** week of the month; the end date is **Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday**.

*add-time*: Time added to the current standard time of the device, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

**Description** Use the **clock summer-time repeating** command to adopt summer-time repeatedly.

Use the **undo clock summer-time** command to cancel the configuration of the daylight saving time.

For example, when *start-date* and *start-time* are set to 2007/6/6 and 00:00:00, *end-date* and *end-time* to 2007/10/01 and 00:00:00, and *add-time* to 01:00:00, it specifies to adopt daylight saving time from 00:00:00 of June 6 until 00:00:00 of October 1 each year from 2007 (2007 inclusive). The daylight saving time adds one hour to the current device time.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

Note that:

- The time range from “start-time” in “start-date” to “end-time” in “end-date” must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.
- If the current system time is in the time range specified with this command, the system time automatically adds “add-time” after the execution of this command.

**Related commands:** **clock datetime**, **clock summer-time one-off**, **clock timezone**, **display clock**.

**Examples** # For the summer time in **abc2** between 06:00:00 on 08/01/2007 and 06:00:00 on 09/01/2007 and from 06:00:00 08/01 to 06:00:00 on 09/01 each year after 2007, set the system clock ahead one hour.

```
<Sysname> clock summer-time abc2 repeating 06:00:00 08/01/2007 06:00:00 09/01/2007 01:00:00
```

## clock timezone

**Syntax** **clock timezone** *zone-name* { **add** | **minus** } *zone-offset*

**undo clock timezone**

**View** User view

**Parameters** *zone-name*: Time zone name, a string of 1 to 32 characters. It is case sensitive.

**add**: Positive offset to universal time coordinated (UTC) time.

**minus**: Negative offset to UTC time.

*zone-offset*: In the format of *HH/MM/SS* (hours/minutes/seconds), where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59. The zeros in the argument can be omitted except for indicating 0 hours.

**Description** Use the **clock timezone** command to set the local time zone.

Use the **undo clock timezone** command to restore the local time zone to the default UTC time zone.

By default, the local time zone is UTC zone.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

**Related commands:** **clock datetime, clock summer-time one-off, clock summer-time repeating, display clock.**

**Examples** # Set the name of the local time zone to **Z5**, five hours ahead of UTC time.  
 <Sysname> clock timezone z5 add 5

---

## command-privilege

**Syntax** **command-privilege level** *level* **view** *view* *command*  
**undo command-privilege view** *view* *command*

**View** System view

**Parameters** **level** *level*: Command level, in the range 0 to 3.

**view** *view*: Specifies a view.

*command*: Command to be set in the specified view.

**Description** Use the **command-privilege** command to assign a level for the commands in the specified view.

Use the **undo command-privilege view** command to restore the default.

By default, each command in each view has its specified level. Therefore, you are not recommended to modify the default command levels for fear of inconvenience brought to your operation and maintenance.

Command privilege falls into four levels: visit, monitor, system, and manage, which are identified by 0 through 3.

The administrator can assign a privilege level for a user according to his need. When the user logs on a device, the commands available depend on the user's privilege. For example, if a user's privilege is 3 and the command privilege of VTY 0 user interface is 1, and the user logs on the system from VTY 0, he can use all the commands with privilege smaller than three (inclusive).

The following table describes the default level of the commands.

**Table 277** Default level of the commands

Command level	Commands
Visit (0)	<b>ping, tracer, telnet</b>
Monitor (1)	<b>refresh, reset, send</b>
System (2)	Configuration commands
Manage (3)	FTP, Xmodem, TFTP, file system operation commands

**Examples** # Set the command level of the **interface** command to 0.

```
<Sysname> system-view
[Sysname] command-privilege level 0 view system interface
```

---

## display clipboard

**Syntax** **display clipboard**

**View** Any view

**Parameters** None

**Description** Use the **display clipboard** command to view the contents of the clipboard.

To copy the specified content to the clipboard:

Move the cursor to the starting position of the content and press the <Esc+Shift+,> combination ("," is an English comma).  
 Move the cursor to the ending position of the content and press the <Esc+Shift+.> combination (". " is an English dot) to copy the specified content to the clipboard.

**Examples** # View the content of the clipboard.

```
<Sysname> display clipboard
----- CLIPBOARD-----
 ip route 10.1.0.0 255.0.0.0 eth 0
```

---

## display clock

**Syntax** **display clock**

**View** Any view

**Parameters** None

**Description** Use the **display clock** command to view the current system time and date.

The current system time and date are decided by the **clock datetime**, **clock summer-time one-off** (or **clock summer-time repeating**), **clock timezone**. Refer to *Configuring the system clock* in the Configuration Guide for the detailed rules.

**Related commands:** **clock datetime**, **clock summer-time one-off**, **clock summer-time repeating**, **clock timezone**.

**Examples** # Display the current time and date.

```
<Sysname> display clock
09:41:23 UTC Thu 12/15/2005
```



---

## display current-configuration

**Syntax** **display current-configuration** [ [ **configuration** [ *configuration* ] | **interface** [ *interface-type* ] [ *interface-number* ] ] [ **by-linenum** ] [ [ { **begin** | **include** | **exclude** } *text* ] ]

**View** Any view

**Parameters** **configuration** [ *configuration* ]: Specifies to display non-interface configuration. If no parameter is used, all the non-interface configuration is displayed; if parameters are used, display the specified information. For example:

- **isis**: Displays the isis configuration.
- **isp**: Displays the ISP configuration.
- **post-system**: Displays the post-system configuration.
- **radius-template**: Displays the Radius template configuration.
- **system**: Displays the system configuration.
- **user-interface**: Displays the user interface configuration.

**interface** [ *interface-type* ] [ *interface-number* ]: Displays the interface configuration, where *interface-type* represents the interface type and *interface-number* represents the interface number.

**by-linenum**: Specifies to display the number of each line.

**]**: Specifies to use regular expression to filter the configuration of display device.

- **begin**: Displays the configuration beginning with the specified *text*.
- **include**: Displays the configuration including the specified *text*.
- **exclude**: Displays the configuration excluding the specified *text*.

*text*: Regular expression in a case-insensitive string with space allowed.

**Table 278** Special characters in regular expression

Character	Meaning	Note
^	Starting sign, the string following it appears only at the beginning of a line.	Regular expression " <b>^user</b> " matches a string begins with "user", not "Auser".
\$	Ending sign, the string following it appears only at the end of a line.	Regular expression " <b>user\$</b> " matches a string ends with "user", not "userA".
(	Left bracket, used as a stack symbol in a program	It is not recommended to use this character to establish a regular expression.
.	Full stop, a wildcard used in place of any character, including blank	None
*	Asterisk, used to match a sub expression zero or multiple times before it	zo* can map to "z" and "zoo".
+	Addition, used to match a sub expression one or multiple times before it	zo+ can map to "zo" and "zoo", but not "z".

**Table 278** Special characters in regular expression

Character	Meaning	Note
-	Hyphen. It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, "1-9" means numbers from 1 to 9 (inclusive); "a-h" means from a to h (inclusive).
[ ]	Selects one character from the group.	For example, [1-36A] can match only one character among 1, 2, 3, 6, and A.
( )	A group of characters. It is usually used with "+" or "*".	For example, (123A) means a string "123A"; "408(12)+" can match 40812 or 408121212. But it cannot match 408. That is, "12" can appear continuously and it must at least appear once.

**Description** Use the **display current-configuration** command to display the current validated configuration of a device.

You can use the **display current-configuration** command to view the currently validated configuration. A parameter is not displayed if it has the default configuration. If the validated parameter is changed, although you have configured it, the validated parameter is displayed. For example, ip address 11.11.11.11 24 has been configured on a Loopback interface. In this case, if you execute the **display current-configuration** command, ip address 11.11.11.11 255.255.255.255 is displayed, meaning the validated subnet mask is 32 bits.

**Related commands:** **save**, **reset saved-configuration**, **display saved-configuration**.

**Examples** # Display the configuration beginning with **user**.

```
<Sysname> display current-configuration | begin user
user-interface aux 0
user-interface vty 0 4
```

---

## display diagnostic-information

**Syntax** **display diagnostic-information**

**View** Any view

**Parameters** None

**Description** Use the **display diagnostic-information** command to display or save the statistics of each module's running status in the system.

When the system is out of order, you need to collect a lot of information to locate the problem. At this time you can use the **display diagnostic-information** command to collect prompt information of the commands **display clock**, **display version**, **display device**, **display current-configuration**.

**Examples** # Save the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)?[Y/N]y
Please input the file name(*.diag)[flash:/default.diag]:aa.diag
Diagnostic information is outputting to flash:/aa.diag.
Please wait...
Save succeeded.
```

You can view the content of the file aa.diag by executing the more.aa.diag command in user view, in combination of the <Page Up> and <Page Down> keys.

# Display the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)?[Y/N]n
.....Omitted.....
```

---

## display history-command

**Syntax** **display history-command**

**View** Any view

**Parameters** None

**Description** Use the **display history-command** command to display commands saved in the history buffer.

The system will save validated history commands performed last in current user view to the history buffer, which can save up to ten commands by default. You can use the **history-command max-size** command to set the size of the history buffer. Refer to the **history-command max-size** on page 67 for more information.

**Examples** # Display validated history commands in current user view (the display information varies with configuration).

```
<Sysname> display history-command
display history-command
system-view
vlan 2
quit
```

---

## display hotkey

**Syntax** **display hotkey**

**View** Any view

**Parameters** None

**Description** Use the **display hotkey** command to display hotkey information.

**Examples** # Display hotkey information.

```
<Sysname> display hotkey
----- HOTKEY -----

 =Defined hotkeys=
Hotkeys Command
CTRL_G display current-configuration
CTRL_L display ip routing-table
CTRL_O undo debug all

 =Undefined hotkeys=
Hotkeys Command
CTRL_T NULL
CTRL_U NULL

 =System hotkeys=
Hotkeys Function
CTRL_A Move the cursor to the beginning of the current line.
CTRL_B Move the cursor one character left.
CTRL_C Stop current command function.
CTRL_D Erase current character.
CTRL_E Move the cursor to the end of the current line.
CTRL_F Move the cursor one character right.
CTRL_H Erase the character left of the cursor.
CTRL_K Kill outgoing connection.
CTRL_N Display the next command from the history buffer.
CTRL_P Display the previous command from the history buffer.
CTRL_R Redisplay the current line.
CTRL_V Paste text from the clipboard.
CTRL_W Delete the word left of the cursor.
CTRL_X Delete all characters up to the cursor.
CTRL_Y Delete all characters after the cursor.
CTRL_Z Return to the User View.
CTRL_] Kill incoming connection or redirect connection.
ESC_B Move the cursor one word back.
ESC_D Delete remainder of word.
ESC_F Move the cursor forward one word.
ESC_N Move the cursor down a line.
ESC_P Move the cursor up a line.
ESC_< Specify the beginning of clipboard.
ESC_> Specify the end of clipboard.
```

---

## display this

**Syntax** **display this** [ **by-linenum** ]

**View** Any view

**Parameters** **by-linenum**: Specifies to display the number of each line.

**Description** Use the **display this** command to display the validated configuration information under the current view.

After finishing a set of configurations under a view, you can use the **display this** command to check whether the configuration takes effect.

Note that:

- A parameter is not displayed if it has the default configuration.
- A parameter is not displayed if the configuration has not taken effect.
- When you use the command under interface view, protocol view or protocol child view, the command displays the configuration corresponding to the current view.

**Examples** # Display configuration information of the current view (the display information varies with configuration).

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] display this
#
user-interface aux 0
user-interface vty 0
 history-command max-size 256
user-interface vty 1 4
#
return
```

---

## display version

**Syntax** **display version**

**View** Any view

**Parameters** None

**Description** Use the **display version** command to view system version information.

By viewing system version information, you can learn about the current software version, rack type and the information related to the main control module and interface modules.

**Examples** # Display system version information.

```
<Sysname> display version
3Com Comware Platform Software
Comware Software, Version 5.00, Release 0000
Copyright (c) 2004-2007 3Com Corporation All rights reserved.
S7902E uptime is 0 week, 0 day, 21 hours, 43 minutes
Slot 0 Without Board
SRPG(M) 1:
Uptime is 0 weeks,0 days,21 hours,43 minutes
```

```

S7902E SRPG(M) with 1 BCM1125H Processor
DRAM: 512M bytes
FLASH: 64M bytes
NVRAM: 512K bytes
Hardware Version: VER.A
Bootrom Version: 108
CPLD Version: 002
Release Version: S7902E-0000
I/O Module 2:
Uptime is 0 weeks,0 days,21 hours,42 minutes
S7902E I/O Module with 1 BCM1122H Processor
DRAM: 256M bytes
FLASH: 0M bytes
NVRAM: 0K bytes
Hardware Version: VER.C
Bootrom Version: 107
CPLD Version: 004
Release Version: S7902E-0000

Slot 3 Without Board

```

---

## header

**Syntax** `header { incoming | legal | login | motd | shell } text`  
`undo header { incoming | legal | login | motd | shell }`

**View** System view

**Parameters** **incoming**: Sets the banner displayed when a Modem login user enters user view. If authentication is needed, the incoming banner is displayed after the authentication is passed.

**legal**: Sets the authorization banner before a user logs onto the terminal interface. The legal banner is displayed before the user inputs the username and password.

**login**: Sets the login banner at authentication.

**motd**: Banner displayed before login. If authentication is required, the banner is displayed before authentication.

**shell**: Sets the banner displayed when a non Modem login user enters user view.

*text*: Banner message, which can be input in two formats. Refer to the *Basic System Configuration* part in the Configuration Guide for the detailed information.

**Description** Use the **header** command to create a banner.

Use the **undo header** command to clear a banner.

**Examples** # Configure banners.

```

<Sysname> system-view
[Sysname] header incoming %
Input banner text, and quit with the character '%'.
Welcome to incoming(header incoming)%
[Sysname] header legal %
Input banner text, and quit with the character '%'.
Welcome to legal (header legal)%
[Sysname] header login %
Input banner text, and quit with the character '%'.
Welcome to login(header login)%
[Sysname] header motd %
Input banner text, and quit with the character '%'.
Welcome to motd(header motd)%
[Sysname] header shell %
Input banner text, and quit with the character '%'.
Welcome to shell(header shell)%

```



- *The character % is the starting/ending character of text in this example. Entering % after the displayed text quits the header command.*
- *As the starting and ending character, % is not a part of a banner.*

# Test the configuration remotely using Telnet. (only when login authentication is configured can the login banner be displayed).

```

* Copyright (c) 2004-2007 3Com Corporation All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-switch fabricering shall be allowed. *

Welcome to legal (header legal)
 Press Y or ENTER to continue, N to exit.

Welcome to motd(header motd)

Welcome to shell(header shell)
<Sysname>

```

---

## hotkey

**Syntax** hotkey { CTRL\_G | CTRL\_L | CTRL\_O | CTRL\_T | CTRL\_U } *command*

**undo hotkey** { CTRL\_G | CTRL\_L | CTRL\_O | CTRL\_T | CTRL\_U }

**View** System view

**Parameters** CTRL\_G: Assigns the hot key <Ctrl+G> to a command.

CTRL\_L: Assigns the hot key <Ctrl+L> to a command.

CTRL\_O: Assigns the hot key <Ctrl+O> to a command.

CTRL\_T: Assigns the hot key <Ctrl+T> to a command.

CTRL\_U: Assigns the hot key <Ctrl+U> to a command.

*command*: The command line associated with the hot key.

**Description** Use the **hotkey** command to assign a hot key to a command line.

Use the **undo hotkey** command to restore the default.

By default, the system specifies corresponding commands for <Ctrl+G>, <Ctrl+L> and <Ctrl+O>, while the others are null.

- <Ctrl+G> corresponds to display current-configuration
- <Ctrl+L> corresponds to display ip routing-table
- <Ctrl+O> corresponds to undo debugging all

You can customize this scheme as needed however.

**Examples** # Assign the hot key <Ctrl+T> to the **display tcp status** command.

```
<Sysname> system-view
[Sysname] hotkey ctrl_t display tcp status
```

# Display the configuration of hotkeys.

```
[Sysname] display hotkey
----- HOTKEY -----

 =Defined hotkeys=
Hotkeys Command
CTRL_G display current-configuration
CTRL_L display ip routing-table
CTRL_O undo debug all
CTRL_T display tcp status
 =Undefined hotkeys=
Hotkeys Command
CTRL_U NULL

 =System hotkeys=
Hotkeys Function
CTRL_A Move the cursor to the beginning of the current line.
CTRL_B Move the cursor one character left.
CTRL_C Stop current command function.
CTRL_D Erase current character.
CTRL_E Move the cursor to the end of the current line.
CTRL_F Move the cursor one character right.
CTRL_H Erase the character left of the cursor.
CTRL_K Kill outgoing connection.
CTRL_N Display the next command from the history buffer.
CTRL_P Display the previous command from the history buffer.
CTRL_R Redisplay the current line.
CTRL_V Paste text from the clipboard.
CTRL_W Delete the word left of the cursor.
CTRL_X Delete all characters up to the cursor.
CTRL_Y Delete all characters after the cursor.
CTRL_Z Return to the user view.
CTRL_] Kill incoming connection or redirect connection.
ESC_B Move the cursor one word back.
ESC_D Delete remainder of word.
```



```
ESC_F Move the cursor forward one word.
ESC_N Move the cursor down a line.
ESC_P Move the cursor up a line.
ESC_< Specify the beginning of clipboard.
ESC_> Specify the end of clipboard.
```

---

## quit

**Syntax** `quit`

**View** Any view

**Parameters** None

**Description** Use the **quit** command to exit to a lower-level view. If the current view is user view, the **quit** command terminates the current connection and reconnects to the device.

**Examples** # Switch from Ethernet 2/0/1 port view to system view, and then to user view.

```
[Sysname-Ethernet2/0/1] quit
[Sysname] quit
<Sysname>
```

---

## return

**Syntax** `return`

**View** Any view except user view

**Parameters** None

**Description** Use the **return** command to return to user view from current view, as you do with the hot key <Ctrl+Z>.

**Related commands:** **quit**.

**Examples** # Return to user view from Ethernet port view.

```
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet 2/0/1] return
<Sysname>
```

---

## super

**Syntax** `super [ /level ]`

**View** User view

**Parameters** *level*: User level, in the range 0 to 3.

**Description** Use the **super** command to switch from the current user level to a specified user level.

There are four levels of commands:

- Visit: involves commands for network diagnosis (such as **ping** and **tracert**), commands for accessing an external device (such as Telnet client, SSH client, RLOGIN). Saving the configuration file is not allowed at this level.
- Monitor: includes the **display** and **debugging** commands for system maintenance, and service fault diagnosis. Saving the configuration file is not allowed at this level.
- System: provides service configuration commands, including routing and commands at each level of the network for providing services.
- Manage: influences the basic operation of the system and the system support modules for service support. Commands at this level involve file system, FTP, TFTP, Xmodem download and configuration file switch, power control, standby module control, user management, level setting, as well as parameter setting within a system (the last case involves those non-protocol or non RFC provisioned commands).

Login users are also classified into four levels that correspond to the four command levels. After users at different levels log in, they can only use commands at their own, or lower, levels.

Note that:

Users can switch to a lower user level unconditionally. To switch to a higher user level, however, they need to enter the password (The password can be set with the **super password** command.). If the entered password is incorrect or no password is configured, the switch fails. Therefore, before switching to a higher user level, users should configure the password needed.

**Related commands:** **super password**.

**Examples** # Set the user level to 2 (The current user level is 3.).

```
<Sysname> super 2
User privilege level is 2, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

# Switch the user level back to 3 (Suppose password **123** has been set; otherwise, the user level cannot be switched to 3.).

```
<Sysname> super 3
Password:
User privilege level is 3, and only those commands can be used
```

whose level is equal or less than this.

Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE

---

## super password

**Syntax** **super password** [ **level** *user-level* ] { **simple** | **cipher** } *password*  
**undo super password** [ **level** *user-level* ]

**View** System view

**Parameters** **level** *level*: User level in the range 1 to 3, with the default as 3.

**simple**: Plain text password.

**cipher**: Cipher text password.

*password*: Password, a string of characters. It is case-sensitive.

- For simple password, it is a string of 1 to 16 characters.
- For cipher password, it is a string of 1 to 16 characters in plain text or 24 characters in cipher text. For example, the simple text "1234567" corresponds to the cipher text "(TT8F)Y5SQ=^Q'MAF4<1!!".

**Description** Use the **super password** command to set the password needed to switch from a lower user level to a higher one.

Use the **undo super password** command to restore the default.

By default, no password is set to switch from a lower user level to a higher one.

Note that:

- If **simple** is specified, the configuration file saves a simple password.
- If **cipher** is specified, the configuration file saves a cipher password.
- The user must always enter a simple password, no matter **simple** or **cipher** is specified.
- Cipher passwords are recommended, as simple ones are easily getting cracked.

**Examples** # Set the password to **abc** in simple form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 simple abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
super password level 3 simple abc
```

# Set the password to abc in cipher form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 cipher abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
super password level 3 cipher =`*Y=F>*.%-a_SW8MYM2A!!
```

## sysname

**Syntax** `sysname sysname`

**undo sysname**

**View** System view

**Parameters** *sysname*: Name of the device, a string of 1 to 30 characters.

**Description** Use the **sysname** command to set the name of the device.

Use the **undo sysname** demand to restore the device name to the default.

The default name is 3Com.

Modifying device name affects the prompt of the CLI. For example, if the device name is **Sysname**, the prompt of user view is <Sysname>.

**Examples** # Set the name of the device to **R2000**.

```
<Sysname> system-view
[Sysname] sysname R2000
[R2000]
```

## system-view

**Syntax** `system-view`

**View** User view

**Parameters** None

**Description** Use the **system-view** command to enter system view from the current user view.

**Related commands:** `quit`, `return`.

**Examples** # Enter system view from the current user view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
```

---

**ping**

**Syntax** **ping** [ **ip** ] [ **-a** *source-ip* | **-c** *count* | **-f** | **-h** *tll* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v** ] \* *remote-system*

**View** Any view

**Parameters** **ip**: Supports IPv4 protocol.

**-a** *source-ip*: Specifies the source IP address of an ICMP echo request. It must be a legal IP address configured on the device.

**-c** *count*: Specifies the number of times that an ICMP echo request is sent, in the range 1 to 4294967295. The default value is 5.

**-f**: Discards packets larger than the MTU of a given interface, that is, the ICMP echo request is not allowed to be fragmented.

**-h** *tll*: Specifies the TTL value for an ICMP echo request, in the range 1 to 255. The default value is 255.

**-i** *interface-type interface-number*: Specifies the ICMP echo request sending interface by its type and number.

**-m** *interval*: Specifies the interval (in milliseconds) to send an ICMP echo response, in the range 1 to 65535. The default value is 200 ms.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval*.
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval*.

**-n**: Specifies that the Domain Name System (DNS) is disabled. DNS is enabled by default, that is, the *hostname* is translated into an address.

**-p** *pad*: Specifies the padded bytes in an ICMP echo request, in hexadecimal format. For example, if *pad* is configured as ff, then the packets will be padded with ff. By default, the padded bytes start from 0x01 up to 0x09, where another round starts again if necessary.

**-q**: Presence of this parameter indicates that only statistics are displayed. By default, all information is displayed.

**-r**: Records routes. By default, routes are not recorded.

**-s *packet-size***: Specifies length (in bytes) of an ICMP echo request, in the range 20 to 8100. The default value is 56.

**-t *timeout***: Specifies the timeout value (in milliseconds) of an ICMP echo request, in the range 0 to 65535. It defaults to 2000.

**-tos *tos***: Specifies type of service (ToS) of an echo request, in the range 0 to 255. The default value is 0.

**-v**: Displays non ICMP echo reply received. By default, the system does not display non ICMP echo reply.

*remote-system*: IP address or host name (a string of 1 to 20 characters) of the destination device.

**Description** Use the **ping** command to verify whether the destination device in an IP network is reachable, and to display the related statistics.

Note that:

- You must use the command in the form of **ping ip *ip*** instead of **ping *ip*** if the destination name is a key word, such as **ip**.
- Only the directly connected segment address can be pinged if the outgoing interface is specified with the **-i** argument.

**Examples** # Check whether the device with an IP address of 10.1.1.5 is reachable.

```
<Sysname> ping 10.1.1.5
PING 10.1.1.5 : 56 data bytes, press CTRL_C to break
Reply from 10.1.1.5 : bytes=56 Sequence=1 ttl=255 time = 1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 ttl=255 time = 2 ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 ttl=255 time = 1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 ttl=255 time = 3 ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 ttl=255 time = 2 ms

--- 10.1.1.5 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/2/3 ms
```

---

## ping ipv6

**Syntax** **ping ipv6** [ **-a** *source-ipv6* | **-c** *count* | **-m** *interval* | **-s** *packet-size* | **-t** *timeout* ] \* *remote-system* [ **-i** *interface-type interface-number* ]

**View** Any view

- Parameters**
- a *source-ipv6***: Specifies the source IPv6 address of an ICMP echo request. It must be a legal IPv6 address configured on the device.
  - c *count***: Specifies the number of times that an ICMPv6 echo request is sent, in the range 1 to 4294967295. The default value is 5.
  - m *interval***: Specifies the interval (in milliseconds) to send an ICMPv6 echo reply, in the range 1 to 65535. The default value is 200 ms.
    - If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval*.
    - If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval*.
  - s *packet-size***: Specifies length (in bytes) of an ICMPv6 echo request, in the range 20 to 8100. It defaults to 56.
  - t *timeout***: Specifies the timeout value (in milliseconds) of an ICMPv6 echo request, in the range 0 to 65535. It defaults to 2000.
- remote-system*: IPv6 address or host name (a string of 1 to 46 characters) of the destination device.
- i *interface-type interface-number***: Specifies an outgoing interface by its type and number. This parameter can be used only in case that the destination address is the link local address and the specified outgoing interface must have a link local address (For the configuration of link local address, see *IPv6 Configuration*).

**Description** Use the **ping ipv6** command to verify whether an IPv6 address is reachable, and display the corresponding statistics.

You must use the command in the form of **ping ipv6 ipv6** instead of **ping ipv6** if the destination name is an ipv6 name.

**Examples** # Verify whether the IPv6 address 2001::1 is reachable.

```
<Sysname> ping ipv6 2001::1
 PING 2001::1 : 56 data bytes, press CTRL_C to break
 Reply from 2001::1 bytes=56 Sequence=1 hop limit=64 time = 20 ms
 Reply from 2001::1 bytes=56 Sequence=2 hop limit=64 time = 0 ms
 Reply from 2001::1 bytes=56 Sequence=3 hop limit=64 time = 0 ms
 Reply from 2001::1 bytes=56 Sequence=4 hop limit=64 time = 0 ms
 Reply from 2001::1 bytes=56 Sequence=5 hop limit=64 time = 0 ms

 --- 2001::1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 0/4/20 ms
```

The "hop limit" field in this prompt information has the same meaning as the "ttl" field in the prompt information displayed by the IPv4 **ping** command, indicating the TTL value in the ICMPv6 echo request.

---

**tracert**

**Syntax** **tracert** [ **-a** source-ip | **-f** first-ttl | **-m** max-ttl | **-p** port | **-q** packet-number | **-w** timeout ] \* remote-system

**View** Any view

**Parameters** **-a** *source-ip*: Specifies the source IP address of a tracert packet. It must be a legal IP address configured on the device.

**-f** *first-ttl*: Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

**-m** *max-ttl*: Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30, and must be greater than the first TTL.

**-p** *port*: Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. You do not need to modify this parameter.

**-q** *packet-number*: Specifies the number of probe packets sent each time, in the range 1 to 65535. The default value is 3.

**-w** *timeout*: Specifies the packet timeout time, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

*remote-system*: IP address or host name (a string of 1 to 20 characters) of the destination device.

**Description** Use the **tracert** command to trace the routers the packets traverse from the source to the destination device.

After having identified network failure with the **ping** command, you can use the **tracert** command to determine the failed node(s).

Output information of the **tracert** command includes IP addresses of all the routers the packets traverse from the source to the destination device. If a router times out, “\* \* \*” will be displayed.

**Examples** # Display the routers the packets traverse from the current device, with an IP address of 8.26.0.115, to the destination device.

```
<Sysname> tracert 18.26.0.115
traceroute to 18.26.0.115(18.26.0.115) 30 hops max,40 bytes packet,
press CTRL_C to break
 1 128.3.112.1 10 ms 10 ms 10 ms
 2 128.32.210.1 19 ms 19 ms 19 ms
 3 128.32.216.1 39 ms 19 ms 19 ms
 4 128.32.136.23 19 ms 39 ms 39 ms
 5 128.32.168.22 20 ms 39 ms 39 ms
 6 128.32.197.4 59 ms 119 ms 39 ms
 7 131.119.2.5 59 ms 59 ms 39 ms
```



```

8 129.140.70.13 80 ms 79 ms 99 ms
9 129.140.71.6 139 ms 139 ms 159 ms
10 129.140.81.7 199 ms 180 ms 300 ms
11 129.140.72.17 300 ms 239 ms 239 ms
12 * * *
13 128.121.54.72 259 ms 499 ms 279 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 18.26.0.115 339 ms 279 ms 279 ms

```

---

## tracert ipv6

**Syntax** `tracert ipv6 [ -f first-ttl | -m max-ttl | -p port | -q packet-number | -w timeout ] *  
remote-system`

**View** Any view

**Parameters** **-f *first-ttl***: Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

**-m *max-ttl***: Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30 and must be greater than the first TTL.

**-p *port***: Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. It is unnecessary to modify this parameter.

**-q *packet-number***: Specifies the number of probe packets sent each time, in the range 1 to 65535, defaulting to 3.

**-w *timeout***: Specifies the timeout time of the probe packets, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

*remote-system*: IPv6 address or host name (a string of 1 to 46 characters) of the destination device.

**Description** Use the **tracert ipv6** command to view the routers the IPv6 packets traverse from the source to the destination device.

**Examples** # View the routes involved for packets to travel from the source to the destination with IPv6 address 3002::1.

```

<Sysname> tracert ipv6 3002::1
 traceroute to 3002::1 30 hops max,60 bytes packet
 1 3003::1 30 ms 10 ms 10 ms
 2 3002::1 10 ms 11 ms 9 ms

```



# 87

## SYSTEM DEBUGGING COMMANDS

---

### debugging

**Syntax** **debugging** { **all** [ **timeout** *time* ] | *module-name* [ *option* ] }

**undo debugging** { **all** | *module-name* [ *option* ] }

**View** User view

**Parameters** **all**: All debugging functions.

**timeout** *time*: Specifies the timeout time for the **debugging all** command. When all debugging is enabled, the system automatically executes the **undo debugging all** command after the *time*. The value ranges from 1 to 1440, in minutes.

*module-name*: Module name, such as ARP or ATM. You can use the **debugging ?** command to display the current module name.

*option*: Specifies the debugging option for a specific module. Different modules have different debugging options in terms of their number and content. You can use the **debugging module-name ?** command to display the currently supported options.

**Description** Use the **debugging** command to enable the debugging of a specific module.

Use the **undo debugging** command to disable the debugging of a specific module.

By default, debugging functions of all modules are disabled.

Note the following:

- This command is intended for network administrators to diagnose network failure.
- Output of the debugging information may degrade system efficiency, especially during the execution of the **debugging all** command. Therefore, use the command with caution.
- After finishing debugging, you can use the **undo debugging all** command to disable all the debugging functions.
- You must configure the **debugging**, **terminal debugging** and **terminal monitor** commands first to display detailed debugging information on the

terminal. For the detailed description refer to **terminal debugging** on page 1155 and **terminal monitor** on page 1156.

**Related commands:** **display debugging**.

**Examples** # Enable IP packet debugging.  
 <Sysname> debugging ip packet

---

## display debugging

**Syntax** **display debugging** [ **interface** *interface-type interface-number* ]  
 [ *module-name* ]

**View** Any view

**Parameters** **interface** *interface-type interface-number*: Displays the debugging settings of the specified interface, where *interface-type interface-number* represents the interface type and number.

*module-name*: Module name.

**Description** Use the **display debugging** command to display enabled debugging functions.

**Related commands:** **debugging**.

**Examples** # Display all enabled debugging functions.  
 <Sysname> display debugging  
 IP packet debugging is on



*File names in this document comply with the following rules*

- *Path + file name (namely, a full file name): File on a specified path. A full file name consists of 1 to 135 characters.*
- *File name" (namely, only a file name without a path): File on the current working path. The file name without a path consists of 1 to 91 characters.*

## boot-loader

**Syntax** `boot-loader file file-url slot slot-number { main | backup }`

**View** User view

**Parameters** `file file-url`: Specifies a file name, a string of 1 to 64 characters.

`slot slot-number`: Specifies the slot number of a module.

`main`: Specifies a file as a primary boot file.

`backup`: Specifies a file as a secondary boot file.

**Description** Use the **boot-loader** command to specify a boot file on a module.

A primary boot file is used to boot a device and a secondary boot file is used to boot a device only when a primary boot file is unavailable.

**Related commands:** `display boot-loader`.

**Examples** # Specify the primary boot file of the device as plat.app.

```
<Sysname> boot-loader file plat.app slot 1 main
```

```
This command will set the boot file of the specified board, Continue? [Y/N]:y
```

```
The specified file will be used as the main boot file at the next reboot!
```

## bootrom

**Syntax** `bootrom update file file-url } slot slot-number-list`

- View** User view
- Parameters** **update file** *file-url*: Upgrades Boot ROM, where *file-url* represents name of the file to be upgraded.
- slot** *slot-number-list*: Specifies a list of slot numbers of modules, in the format of { *slot-number* [ **to** *slot-number* ] }&<1-7>. The *slot-number* argument represents the slot number of a module and the value range varies with devices. &<1-7> indicates that you can specify up to seven lists of slot numbers.
- Description** Use the **bootrom** command to upgrade the Boot ROM program on a card(s).
- Examples** # Use the mpu108.app file to upgrade the Boot ROM file on subcard 1 of the device.
- ```
<Sysname> bootrom update file mpu108.app slot 1
  This command will update bootrom file on the specified board(s), C
  ontinue? [Y/N]:y
  Now updating bootrom, please wait...
  Start accessing bootflash chip...
  Bootrom update succeeded.
```

display cpu-usage

- Syntax** **display cpu-usage** [**task**] [*number* [*offset*]] [**verbose**] [**slave** | **slot** *slot-number*] [**from-device**] | **slave** | **slot** *slot-number*]
- View** Any view
- Parameters** **task**: Displays CPU usage of each task.
- number*: Number of CPU usage statistics records to be displayed.
- offset*: Offset between the serial number of the first CPU usage statistics record to be displayed and that of the last CPU usage record to be displayed.
- verbose**: Specifies to display detailed information of CPU usage statistics.
- slave**: Specifies to display the statistics of the CPU usage of a standby module.
- slot** *slot-number*: Specifies to display the statistics of the CPU usage of a module. *slot-number* specifies the slot number of a module. The value range varies with devices.
- from-device**: Displays external storage devices such as Flash and hard disk. The device currently does not support the **from-device** keyword.
- Description** Use the **display cpu-usage** command to display the CPU usage statistics.
- The system takes statistics of CPU usage at intervals (usually every 60 seconds) and saves the statistical results in the history record area. The maximum number of

records that can be saved depends on the device model. **display cpu-usage number** indicates the system displays *number* records from the newest (last) record. **display cpu-usage number offset** indicates the system displays *number* records from the last but *offset+1* record.

Equivalent to the **display cpu-usage 1 0 verbose** command, the **display cpu-usage** command displays detailed information of the last CPU usage statistics record.

Examples # Display information of the current CPU usage statistics.

```
<Sysname> display cpu-usage
Slot 4 CPU usage:
    14% in last 5 seconds
    12% in last 1 minute
    8% in last 5 minutes
```

Display detailed information of the last CPU usage statistics record of the current tasks.

```
<Sysname> display cpu-usage task
==== Current CPU usage info ====
CPU Usage Stat. Cycle: 41 (Second)
CPU Usage          : 3%
CPU Usage Stat. Time : 2006-07-10 11:02:20
CPU Usage Stat. Tick : 0x1da0(CPU Tick High) 0x62a5077f(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x3d5b5ad1(CPU Tick Low)

TaskName          CPU          Runtime(CPU Tick High/CPU Tick Low)
b2X0              0%           0/ ce77f
VIDL             97%           0/3bc6e650
TICK             0%           0/ 23ec62
STMR             0%           0/ ad24
DrTF             0%           0/ 28b6b
DrTm             0%           0/ 18a28
bCN0             0%           0/ d840e
...omitted...
```

Display the last fifth and sixth records of the CPU usage statistics history.

```
<Sysname> display cpu-usage 2 4
==== CPU usage info (no: 0 idx: 58) ====
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage          : 3%
CPU Usage Stat. Time : 2006-07-10 10:56:55
CPU Usage Stat. Tick : 0x1d9d(CPU Tick High) 0x3a659a70(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x95030517(CPU Tick Low)

==== CPU usage info (no: 1 idx: 57) ====
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage          : 3%
CPU Usage Stat. Time : 2006-07-10 10:55:55
CPU Usage Stat. Tick : 0x1d9c(CPU Tick High) 0xa50e5351(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x950906af(CPU Tick Low)
```

Table 279 Description on fields of the display cpu-usage command

| Field | Description |
|-------------------------------------|---|
| CPU usage info (no: idx:) | Information of CPU usage records (no: The (no+1)th record is currently displayed. no numbers from 0, a smaller number equals a newer record. idx: index of the current record in the history record table). If only the information of the current record is displayed, no and idx are not displayed. |
| CPU Usage Stat. Cycle | CPU usage measurement period in seconds |
| CPU Usage | CPU usage in percentage |
| CPU Usage Stat. Time | CPU usage statistics time in seconds |
| CPU Usage Stat. Tick | System runtime in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits. |
| Actual Stat. Cycle | Actual CPU usage measurement period in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits. Owing to the precision of less than one second, the actual measurement periods of different CPU usage records may differ slightly. |
| TaskName | Task name |
| CPU | CPU usage of the current task |
| Runtime(CPU Tick High/CPU Tick Low) | Running time of the current task |

display boot-loader

Syntax **display boot-loader slot** *slot-number*

View Any view

Parameters **slot** *slot-number*: Displays startup file information of the specified module, where *slot-number* represents the slot number of a module. The value range varies with devices.

Description Use the **display boot-loader** command to display information of the boot file.

Related commands: **boot-loader**.

Examples # Display the file adopted for the current and next boot of a centralized device.

```
<Sysname> display boot-loader
The primary app to boot of board 1 at this time is: flash:/ Switch.app
The primary app to boot of board 1 at next time is: flash:/ New.app
The slave app to boot of board 1 at next time is: flash:/Switch.app
```

display device

Syntax **display device** [**cf-card**] [[**shelf** *shelf-number*] [**frame** *frame-number*] [**slot** *slot-number*]] | **verbose**]

View Any view

Parameters **cf-card**: Displays information of a compact Flash (CF).

shelf *shelf-number*: Displays detailed information of the specified shelf or unit. The *shelf-number* argument represents a shelf number or unit number and the value range varies with devices.

frame *frame-number*: Displays detailed information of the specified frame. The *frame-number* argument represents a frame number and the value range varies with devices.

slot *slot-number*: Displays detailed information of the specified module. The *slot-number* argument represents the slot number of a module and the value range varies with devices.

verbose: Displays detailed information.

Description Use the **display device** command to display information about storage media such as module, subcard, and CF module.

Examples # Display brief information of modules on the device.

```
<Sysname> display device
Slot No.   Brd Type   Brd Status   Subslot Num   Sft Ver
0          NONE      Absent       0             NONE
1          0231A92Y  Master      0             V600R001B02D036
2          LSQ1FV48SA Normal      0             V600R001B02D036
3          NONE      Absent       0             NONE
```

Display detailed information of modules on the device.

```
<Sysname> display device verbose
Slot No.   Brd Type   Brd Status   Subslot Num   Sft Ver
0          NONE      Absent       0             NONE
1          0231A92Y  Master      0             V600R001B02D036
2          LSQ1FV48SA Normal      0             V600R001B02D036
3          NONE      Absent       0             NONE

Slot 1 info:
Status      : Master
Type        : 0231A92Y
PCB Ver     : VER.A
FPGA Ver    : 001
BootRom Ver : 108
CPLD Ver    : 002

Slot 2 info:
Status      : Normal
Type        : LSQ1FV48SA
PCB Ver     : VER.C
FPGA Ver    : 001
BootRom Ver : 107
CPLD Ver    : 004
Chip        : 0
  Learning Mode: IVL
Chip        : 1
  Learning Mode: IVL
```

Table 280 Field descriptions of the display device command

| Field | Description |
|---------------|---|
| Slot No. | Slot number of a card |
| Module Type | Hardware type of a card |
| Status | Module status |
| Maximum Ports | Maximum number of physical ports that a module supports |
| Type | Type of the current card |
| Hardware | Hardware version of the current card |
| Driver | Driver version of the current card |
| CPLD | CPLD version of the current card |

display device manuinfo

Syntax `display device manuinfo [slot slot-number [subslot subslot-number]]`

View Any view

Parameters `slot slot-number`: Displays detailed information of the specified module. The `slot-number` argument represents the slot number of a module and the value range varies with devices.

`subslot subslot-number`: Displays detailed information of the specified subcard. The `subslot-number` represents the subslot of a subcard and the value range varies with devices.

Description Use the **display device manuinfo** command to display manufacture information about the device.

Examples # Display manufacturing information of slot 2 on the device.

```
<Sysname> display device manuinfo slot 2
DEVICE_NAME           : LSQ1FV48SA0
DEVICE_SERIAL_NUMBER  : 03A27N1234567890
MAC_ADDRESS           : No
MANUFACTURING_DATE    : 2007-4-18
VENDOR_NAME           : 3Com
```

Table 281 Field descriptions of the display device manuinfo command

| Field | Description |
|----------------------|----------------------------------|
| DEVICE_NAME | Device name |
| DEVICE_SERIAL_NUMBER | Device serial number |
| MAC_ADDRESS | MAC address of the device |
| MANUFACTURING_DATE | Manufacturing date of the device |
| VENDOR_NAME | Manufacturer name |

display environment

Syntax **display environment**

View Any view

Parameters None

Description Use the **display environment** command to display the temperature information, including the current temperature and temperature thresholds of modules.

Examples # Display the temperature information of modules.

```
<Sysname> display environment
System temperature information (degree centigrade):
-----
Board      Temperature      Lower limit      Upper limit
0          28                0                80
3          35                0                80
```

Table 282 Description on fields on the display environment command

| Field | Description |
|--|--|
| System Temperature information (degree centigrade) | Temperature information of system modules (degree centigrade) |
| CPU Temperature information (degree centigrade) | Temperature information of modules of the system (degree centigrade) |
| Board | Module number |
| Temperature | Current temperature |
| Lower limit | Lower limit of temperature |
| Upper limit | Upper limit of temperature |

display fan

Syntax **display fan** [*fan-id*]

View Any view

Parameters *fan-id*: Built-in fan number.

Description Use the **display fan** command to display the operating state of built-in fans.

Examples # Display the operating state of all fans in a device.

```
<Sysname> display fan
Fan 1 State: Normal
```

The above information indicates that fan 1 works normally.

display memory

Syntax `display memory [slave | slot slot-number]`

View Any view

Parameters **slave**: Displays the memory usage of the standby module.

slot *slot-number*: Specifies the slot number of a module. The value range varies with devices.

Description Use the **display memory** command to display the usage of the memory of all or specified modules of a device.

Examples # Display the usage of the memory of a device.

```
<Sysname> display memory
System Total Memory(bytes): 431869088
Total Used Memory(bytes): 71963156
Used Rate: 16%
```

Table 283 Description on fields on the display memory command

| Field | Description |
|----------------------------|---|
| System Total Memory(bytes) | Total size of the system memory (in bytes) |
| Total Used Memory(bytes) | Size of the memory used (in bytes) |
| Used Rate | Percentage of the memory used to the total memory |

display power

Syntax `display power [power-id]`

View Any view

Parameters *power-id*: Power supply number.

Description Use the **display power** to display the status of the power supply of a device.

Examples # Display the status of the power supply of a device.

```
<Sysname> display power
Power 1 State: Normal
Power 2 State: Absent
```

The above information indicates that power supply 1 works normally, and power supply 2 is absent.

display schedule reboot

Syntax `display schedule reboot`

View Any view

Parameters None

Description Use the **display schedule reboot** command to display the device reboot time set by the user.

Related commands: **schedule reboot at** and **schedule reboot delay**.

Examples # Display the reboot time of a device.

```
<Sysname> display schedule reboot
System will reboot at 16:00:00 2006/03/10 (in 2 hours and 5 minutes)
.
```

The above information indicates the system will reboot at 16:00:00 on March 10, 2006 (in two hours and five minutes).

display switch-mode status

Syntax `display switch-mode status`

View Any view

Parameters None

Description Use the **display switch-mode status** command to view the current traffic forwarding mode or working mode of all modules on the switch.

Examples # View the current traffic forwarding mode or working mode of all modules on the switch.

```
<Sysname> display switch-mode status
Slot No.      Switch-Mode
  0           STANDARD-ROUTING
  2           ROUTING
  3           NONE
```

Table 284 Field descriptions of the display switch-mode status command

| Field | Description |
|------------------|--|
| Slot No. | Module slot number |
| Switch-Mode | Traffic forwarding mode or working mode of a card |
| STANDARD-ROUTING | Standard forwarding mode with the route extension function |
| ROUTING | Route extension mode |

Table 284 Field descriptions of the display switch-mode status command

| Field | Description |
|-------|--------------------------------------|
| NONE | This module is not an EA I/O Module. |

display transceiver alarm interface

Syntax **display transceiver alarm interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Interface type and interface number.

Description Use the **display transceiver alarm interface** command to display the current alarm information of a single or all transceivers.

If no error occurs, **None** is displayed.

Table 285 shows the alarm information that may occur for the four types of transceivers.

Table 285 Field descriptions of display transceiver alarm interface

| Field | Remarks |
|--|---|
| GBIC/SFP | |
| RX loss of signal | RX signal is lost. |
| RX power high | RX power is high. |
| RX power low | RX power is low. |
| TX fault | TX fault |
| TX bias high | TX bias current is high. |
| TX bias low | TX bias current is low. |
| TX power high | TX power is high. |
| TX power low | TX power is low. |
| Temp high | Temperature is high. |
| Temp low | Temperature is low. |
| Voltage high | Voltage is high. |
| Voltage low | Voltage is low. |
| Transceiver info I/O error | Transceiver information read and write error |
| Transceiver info checksum error | Transceiver information checksum error |
| Transceiver type and port configuration mismatch | Transceiver type does not match port configuration. |
| Transceiver type not supported by port hardware | Transceiver type is not supported on the port. |
| XFP | |
| RX loss of signal | RX signal is lost. |
| RX not ready | RX is not ready |
| RX CDR loss of lock | RX clock cannot be recovered. |

Table 285 Field descriptions of display transceiver alarm interface

| Field | Remarks |
|--|---|
| RX power high | RX power is high. |
| RX power low | RX power is low. |
| TX not ready | TX is not ready. |
| TX fault | TX fault |
| TX CDR loss of lock | TX clock cannot be recovered. |
| TX bias high | TX bias current is high. |
| TX bias low | TX bias current is low. |
| TX power high | TX power is high. |
| TX power low | TX power is low. |
| Module not ready | Module is not ready. |
| APD supply fault | APD (Avalanche Photo Diode) supply fault |
| TEC fault | TEC (Thermoelectric Cooler) fault |
| Wavelength unlocked | Wavelength of optical signal exceeds the manufacturer's tolerance. |
| Temp high | Temperature is high. |
| Temp low | Temperature is low. |
| Voltage high | Voltage is high. |
| Voltage low | Voltage is low. |
| Transceiver info I/O error | Transceiver information read and write error |
| Transceiver info checksum error | Transceiver information checksum error |
| Transceiver type and port configuration mismatch | Transceiver type does not match port configuration. |
| Transceiver type not supported by port hardware | Transceiver type is not supported on the port. |
| XENPAK | |
| WIS local fault | WIS (WAN Interface Sublayer) local fault |
| Receive optical power fault | Receive optical power fault |
| PMA/PMD receiver local fault | PMA/PMD (Physical Medium Attachment/Physical Medium Dependent) receiver local fault |
| PCS receive local fault | PCS (Physical Coding Sublayer) receiver local fault |
| PHY XS receive local fault | PHY XS (PHY Extended Sublayer) receive local fault |
| RX power high | RX power is high. |
| RX power low | RX power is low. |
| Laser bias current fault | Laser bias current fault |
| Laser temperature fault | Laser temperature fault |
| Laser output power fault | Laser output power fault |
| TX fault | TX fault |
| PMA/PMD receiver local fault | PMA/PMD receiver local fault |
| PCS receive local fault | PCS receive local fault |
| PHY XS receive local fault | PHY XS receive local fault |
| TX bias high | TX bias current is high. |
| TX bias low | TX bias current is low. |
| TX power high | TX power is high. |

Table 285 Field descriptions of display transceiver alarm interface

| Field | Remarks |
|--|---|
| TX power low | TX power is low. |
| Temp high | Temperature is high. |
| Temp low | Temperature is low. |
| Transceiver info I/O error | Transceiver information read and write error |
| Transceiver info checksum error | Transceiver information checksum error |
| Transceiver type and port configuration mismatch | Transceiver type does not match port configuration. |
| Transceiver type not supported by port hardware | Transceiver type is not supported on the port. |



For pluggable transceivers supported by S7900E Ethernet switches, refer to 3Com S7900E Family Installation Manual.

Examples # Display the alarm information of the transceiver on interface GigabitEthernet 2/0/1.

```
<Sysname> display transceiver alarm interface gigabitethernet 2/0/1
GigabitEthernet2/0/1 transceiver current alarm information:
  TX fault
```

Table 286 Field descriptions of display transceiver alarm interface

| Field | Description |
|---------------------------------------|--|
| transceiver current alarm information | Current alarm information of the transceiver |
| TX fault | TX fault |

display transceiver diagnosis interface

Syntax **display transceiver diagnosis interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Interface type and interface number.

Description Use the **display transceiver diagnosis interface** command to display the currently measured value of digital diagnosis parameters of a single or all anti-spoofing transceivers customized by 3Com.

Examples # Display the currently measured value of digital diagnosis parameters of the anti-spoofing pluggable optical transceiver customized by 3Com on interface GigabitEthernet 2/0/2.

```
<Sysname> display transceiver diagnosis interface gigabitethernet 2/0/2
GigabitEthernet2/0/2 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    36         3.31         6.13     -35.64         -5.19
```


Table 287 Field descriptions of display transceiver diagnosis interface

| Field | Description |
|------------------------------------|---|
| transceiver diagnostic information | Digital diagnosis information of the transceiver carried by an interface |
| Current diagnostic parameters | Current diagnostic parameters |
| Temp(°C) | Digital diagnosis parameter-temperature, in °C, with the precision to 1°C. |
| Voltage(V) | Digital diagnosis parameter-voltage, in V, with the precision to 0.01 V. |
| Bias(mA) | Digital diagnosis parameter-bias current, in mA, with the precision to 0.01 mA. |
| RX power(dBM) | Digital diagnosis parameter-RX power, in dBm, with the precision to 0.01 dBm. |
| TX power(dBM) | Digital diagnosis parameter-TX power, in dBm, with the precision to 0.01 dBm. |

display transceiver interface

Syntax `display transceiver interface [interface-type interface-number]`

View Any view

Parameters `interface-type interface-number`: Interface type and interface number.

Description Use the **display transceiver interface** command to display main parameters of a single or all transceivers.

Examples # Display main parameters of the pluggable transceiver on interface GigabitEthernet 2/0/3.

```
<Sysname> display transceiver interface gigabitethernet 2/0/3
GigabitEthernet2/0/3 transceiver information:
  Transceiver Type           : 1000_BASE_LX_SFP
  Connector Type             : LC
  Wavelength(nm)            : 1310
  Transfer Distance(km)      : 10(9um)
  Digital Diagnostic Monitoring : YES
  Vendor Name                 : 3Com
  Ordering Name               : SFP-GE-LX10-SM1310
```

Table 288 Field descriptions of the display transceiver interface command

| Field | Description |
|-------------------------|---|
| transceiver information | Transceiver information of the interface |
| Transceiver Type | Transceiver type |
| Connector Type | Type of the connectors of the transceiver: <ul style="list-style-type: none"> ■ Optical connectors, including SC (SC connector, developed by NTT) and LC (LC connector, 1.25 mm/RJ45 optical connector developed by Lucent). ■ Other connectors, including RJ-45 and CX4. |

Table 288 Field descriptions of the display transceiver interface command

| Field | Description |
|-------------------------------|---|
| Wavelength(nm) | <ul style="list-style-type: none"> Optical transceiver: central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, every two wavelength values are separated by a comma. Electrical transceiver: displayed as N/A. |
| Transfer distance(xx) | <p>Transfer distance, with xx representing km for single-mode transceivers and m for other transceivers. If the transceiver supports multiple transfer medium, every two values of the transfer distance are separated by a comma. The corresponding transfer medium is included in the bracket following the transfer distance value. The following are the transfer media:</p> <ul style="list-style-type: none"> 9 um: 9/125 um single-mode fiber 50 um: 50/125 um multi-mode fiber 62.5 um: 62.5/125 um multi-mode fiber TP: Twisted pair CX4: CX4 cable |
| Digital Diagnostic Monitoring | <p>Whether the digital diagnosis function is supported, where:</p> <ul style="list-style-type: none"> YES: supported NO: not supported |
| Vendor Name | <p>Vendor name or vendor name specified of the transceiver:</p> <ul style="list-style-type: none"> The anti-spoofing transceiver customized by 3Com: 3Com is displayed. Other transceivers: The original vendor name is displayed. |
| Ordering Name | Ordering name of the transceiver |

display transceiver manuinfo interface

Syntax **display transceiver manuinfo interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Interface type and interface number.

Description Use the **display transceiver manuinfo interface** command to display part of the electrical label information of a single or all anti-spoofing pluggable transceivers customized by 3Com.

Examples # Display part of the electrical label information of the anti-spoofing pluggable transceiver customized by 3Com on interface GigabitEthernet 2/0/4.

```
<Sysname> display transceiver manuinfo interface gigabitethernet 2/0/4
GigabitEthernet2/0/4 transceiver manufacture information:
  Manu. Serial Number   : 213410A0000054000251
  Manufacturing Date    : 2007-07-28
  Vendor Name           : 3Com
```

Table 289 Field descriptions of display transceiver manuinfo interface

| Field | Description |
|---------------------|---|
| Manu. Serial Number | Serial number generated during debugging and testing |
| Manufacturing Date | Debugging and testing date. The date takes the value of the system clock of the computer that performs debugging and testing. |
| Vendor Name | Vendor name specified, that is, 3Com. |

reboot

Syntax `reboot`

View User view

Parameters None

Description Use the **reboot** command to reboot the device.



CAUTION:

- *This command reboots the device, thus resulting in service interruption. Please use it with caution.*
- *If a primary boot file fails or does not exist, the device cannot be rebooted with this command. In this case, you can re-specify a primary boot file to reboot the device, or you can power off the device then power it on and the system automatically uses the secondary boot file to restart the device.*
- *If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.*

Examples # Reboot the device.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait
.....
This command will reboot the device. Current configuration will be
lost in next startup if you continue. Continue? [Y/N]:y
This will reboot device. Continue? [Y/N]:y
Now rebooting, please wait...
```

reset unused porttag

Syntax `reset unused porttag`

View User view

Parameters None

Description Use the **reset unused porttag** command to clear the 16-bit index saved but not used in the current system.

A confirmation is required when you carry out this command. If you fail to make a confirmation within 30 seconds or enter "N" to cancel the operation, the command will not be carried out.

Examples # Clear the 16-bit index saved but not used in the current system.

```
<Sysname> reset unused porttag
Current operation will delete all unused port tag(s). Continue? [Y/N]
]:y
<Sysname>
```

schedule reboot at

Syntax schedule reboot at *hh:mm* [*date*]

undo schedule reboot

View User view

Parameters *hh:mm*: Reboot time of a device, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges of is 0 to 23, and the value of the *mm* argument ranges from 0 to 59.

date: Reboot date of a device, in the format mm/dd/yyyy (Month/day/year) or in the format yyyy/mm/dd (year/month/day) The yyyy value ranges from 2000 to 2035, the mm value ranges from 1 to 12, and the dd value depends on a specific month.

Description Use the **schedule reboot at** command to enable the scheduled reboot function and specify a specific reboot time and date.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

There are two cases if no specific reboot date is specified:

- When the specified reboot time is later than the current time, the device will be rebooted at the reboot time of the current day.
- When the specified reboot time is earlier than the current time, the device will be rebooted at the reboot time the next day.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

Note that:

- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt "REBOOT IN ONE MINUTE" and will be rebooted in one minute.
- The difference between the reboot date and the current date cannot exceed 30 x 24 hours (namely, 30 days).
- After you execute the above command, the device will prompt you to confirm the configuration. You must enter <Y> or <y> to make the configuration take effect. The original configuration will be overwritten at the same time.
- If a date (month/day/year or year/month/day) later than the current date is specified for the **schedule reboot at** command, the device will be rebooted at the reboot time.
- If you use the **clock** command after the **schedule reboot at** command to adjust the system time, the reboot time set by the **schedule reboot at** command will become invalid.



CAUTION: This command reboots the device in a future time, thus resulting in service interruption. Please use it with caution.

Examples # Configure the device to reboot at 12:00 AM (supposing that the current time is 11:43).

```
<Sysname> schedule reboot at 12:00
Reboot system at 12:00 2006/06/06(in 0 hour(s) and 16 minute(s))
confirm? [Y/N]:
```

If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter <y>. By default, the log display function is enabled.

```
<Sysname>
%Jun 6 11:43:11:629 2006 Sysname CMD/5/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:43:11 2006/
06/06, and system will reboot at 12:00 2006/06/06.
```

schedule reboot delay

Syntax schedule reboot delay { *hh:mm* | *mm* }

undo schedule reboot

View User view

Parameters *hh:mm*: Device reboot wait time, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges of is 0 to 720, and the value of the *mm* argument ranges from 0 to 59, and the value of the *hh:mm* argument cannot exceed 720:00.

mm: Device reboot wait time in minutes, in the range of 0 to 43,200.

Description Use the **schedule reboot delay** command to enable the scheduled reboot function and set a reboot wait time.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

Note that:

- The reboot wait time can be in the format of hh:mm (hours:minutes) or mm (absolute minutes). The absolute minutes cannot exceed 30 x 24 x 60 minutes, namely, 30 days.
- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt "REBOOT IN ONE MINUTE" and will be rebooted in one minute.
- After you execute the above command, the device will prompt you to confirm the configuration. You must enter <Y> or <y> to make the configuration take effect. The original configuration will be overwritten at the same time.
- If you use the **clock** command after the **schedule reboot delay** command to adjust the system time, the reboot wait time set by the **schedule reboot delay** command will become invalid.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.



CAUTION: This command reboots the device after the specified delay time, thus resulting in service interruption. Please use it with caution.

Examples # Configure the device to reboot in 88 minutes (supposing the current time is 11:48).

```
<Sysname> schedule reboot delay 88
Reboot system at 13:16 2006/06/06(in 1 hour(s) and 28 minute(s))
confirm? [Y/N]:
```

If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter <y>. By default, the log display function is enabled on the terminal.

```
<Sysname>
%Jun 6 11:48:44:860 2006 Sysname CMD/5/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:48:44 2006/
06/06, and system will reboot at 13:16 2006/06/06.
```

shutdown-interval

Syntax **shutdown-interval** *time*

undo shutdown-interval

View System view

Parameters *time*: Detection interval in seconds, in the range of 1 to 300.

Description Use the **shutdown-interval** command to set a detection interval.

Use the **undo shutdown-interval** command to restore the default.

By default, the detection interval is 30 seconds.

Note that:

- If a protocol module such as the operation, administration and maintenance (OAM) module detects an exception on a port (for example, signal loss of the link on the peer end), the port will be closed automatically, without execution of the **shutdown** command. You can set the automatic recovery time of the port by using the **shutdown-interval** command.
- The **shutdown-interval** command helps you to dynamically set a detection interval to cooperate with the OAM module.
- If you change the detection interval to T1 during interface detection, the interval from when you change the interval to the time when detection starts is T. If T<T1, the interface which is down will be brought up after T1-T time; if T>=T1, the interface which is down will be brought up immediately.

Examples # Set the detection interval to 100 seconds.

```
<Sysname> system-view
[Sysname] shutdown-interval 100
```

switch-mode (for Fabric)

Syntax When the Fabric is 0231A935:

switch-mode { **I2-enhanced** | **standard-bridging** | **standard-routing** }

undo switch-mode

When the Fabric is 0231A933, 0231A934, or 0231A92Y:

switch-mode { **I2-enhanced** | **standard** }

undo switch-mode

View System view

Parameters **I2-enhanced**: Indicates the enhanced Layer 2 forwarding mode with the MAC extension function when the Fabric is 0231A935, and the enhanced Layer 2 forwarding mode when the Fabric is 0231A933, 0231A934, or 0231A92Y.

standard: Indicates the standard forwarding mode.

standard-bridging: Indicates the standard forwarding mode with the MAC extension function.

standard-routing: Indicates the standard forwarding mode with the route extension function.

Description Use the **switch-mode** command to configure the traffic forwarding mode of an Fabric.

Use the **undo switch-mode** command to restore the default traffic forwarding mode of the Fabric.

- The default traffic forwarding mode of 0231A935 is **standard-routing**.
- The default traffic forwarding mode of 0231A933, 0231A934, or 0231A92Y is **standard**.



To make the configured forwarding mode take effect, you need to save the configuration and restart the switch.

Examples # Configure the traffic forwarding mode of the Fabric (0231A92Y) as the enhanced Layer 2 forwarding mode.

```
<Sysname> system-view
[Sysname] switch-mode 12-enhanced
```

Restore the default traffic forwarding mode of the Fabric.

```
<Sysname> system-view
[Sysname] undo switch-mode
```

switch-mode (for I/O Module)

Syntax **switch-mode** { **bridging** | **routing** } **slot** *slot-num*

undo switch-mode **slot** *slot-num*

View System view

Parameters **bridging:** Indicates the MAC extension mode.

routing: Indicates the route extension mode.

slot-num: Number of the slot where the I/O Module resides.

Description Use the **switch-mode** command to configure the working mode of an EA I/O Module.

Use the **undo switch-mode** command to restore the default working mode of the EA I/O Module.

By default, the working mode of an EA I/O Module is determined by the Fabric model and the current traffic forwarding mode of the Fabric. Refer to Table 290 for details.

Table 290 Default working mode of EA I/O Modules

Fabric model	Current traffic forwarding mode of the Fabric	Default working mode of EA I/O Modules
0231A933, 0231A934, 0231A92Y	I2-enhanced or standard	routing
0231A935	I2-enhanced or standard-bridging	bridging
	standard-routing	routing



- When the Fabric of the S7900E is 0231A935, it is recommended not to modify the default working mode the EA I/O Modules.
- When the Fabric of the S7900E is 0231A933, 0231A934, or 0231A92Y, if an EA I/O Module is connected to a Layer 2 forwarding network with a large number of MAC addresses, you can configure the EA I/O Module to work in the MAC extension mode.
- To make the configured working mode take effect, you need to save the configuration and restart the switch.

Examples # Configure the working mode of the EA I/O Module on slot 2 of the S7902E switch as the MAC extension mode.

```
<Sysname> system-view
[Sysname] switch-mode bridging slot 2
```

Restore the default working mode of the EA I/O Module on slot 2 of the S7902E switch.

```
<Sysname> system-view
[Sysname] undo switch-mode slot 2
```

temperature-limit

Syntax **temperature-limit** *slot-number lower-value upper-value*

undo temperature-limit *slot-number*

View System view

Parameters *slot-number*: Slot number.

lower-value: Lower temperature limit in Celsius degrees, in the range 0°C to 70°C.

upper-value: Upper temperature limit in Celsius degrees, in the range 20°C to 90°C.

Description Use the **temperature-limit** command to set the temperature alarm threshold on a module.

Use the **undo temperature-limit** command to restore the temperature alarm threshold to the default.

By default, the upper value and lower value for the temperature alarm threshold are 80°C and 0°C respectively.

Examples # Set the lower temperature limit on module 0 to 10°C and the upper temperature limit to 75°C.

```
<Sysname> system-view  
[Sysname] temperature-limit 0 10 75  
Setting temperature limit succeeded.
```



The upper-value argument must be bigger than the lower-level argument.

89

POE CONFIGURATION COMMANDS

apply poe-profile

Syntax **apply poe-profile** { **index** *index* | **name** *profile-name* }
undo apply poe-profile { **index** *index* | **name** *profile-name* }

View PoE interface view

Parameters **index** *index*: Index number of the PoE configuration file, in the range 1 to 100.
name *profile-name*: Name of the PoE configuration file, a string of 1 to 15 characters.

Description Use the **apply poe-profile** command to apply the PoE configuration file to the current PoE interface.

Use the **undo apply poe-profile** command to remove the application of the PoE configuration file to the current PoE interface.

Note that the index number, instead of the name, of the PoE configuration file is displayed when you execute the **display this** command.

Related commands: **display poe-profile, apply poe-profile interface.**

Examples # Apply the PoE configuration file named **A20** to the PoE interface Ethernet 2/0/2.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] apply poe-profile name A20
[Sysname-Ethernet2/0/2] display this
#
interface Ethernet2/0/2
apply poe-profile index 1
#
```

apply poe-profile interface

Syntax **apply poe-profile** { **index** *index* | **name** *profile-name* } **interface** *interface-range*
undo apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

View System view

Parameters **index** *index*: Index number of the PoE configuration file, in the range 1 to 100.

name *profile-name*: Name of the PoE configuration file, a string of 1 to 15 characters.

interface-range: Range of Ethernet interface numbers, indicating multiple Ethernet interfaces. The expression is *interface-range* = *interface-type interface-number* [**to** *interface-type interface-number*], where *interface-type interface-number* represents the interface type and interface number. The start interface number should be smaller than the end interface number. Ethernet interface numbers can be in any range. If any interface in the specified range does not support PoE, it is ignored when the PoE configuration file is applied.

Description Use the **apply poe-profile interface** command to apply the PoE configuration file to one or more PoE interfaces.

Use the **undo apply poe-profile interface** command to remove the application of the PoE configuration file to the specified PoE interface(s).

Related commands: **display poe-profile interface, apply poe-profile.**

Examples # Apply the PoE configuration file named ABC to the PoE interface Ethernet 2/0/2.

```
<Sysname> system-view
[Sysname] apply poe-profile name ABC interface Ethernet 2/0/2
```

Apply the PoE configuration file with the index of 5 to PoE interfaces Ethernet 2/0/2 through Ethernet 2/0/8.

```
<Sysname> system-view
[Sysname] apply poe-profile index 5 interface ethernet 2/0/2 to ethernet 2/0/8
```

display poe device

Syntax **display poe device**

View Any view

Parameters None

Description Use the **display poe device** command to display the mapping between ID, module, and slot of all the power sourcing equipment (PSEs).

Examples # Display the mapping between ID, module, and slot of each PSE.

```
<Sysname> display poe device
PSE ID  SlotNo  SubSNo  PortNum  MaxPower(W)  State  Model
10      3         0       48       100           on     0231A930
```

Table 291 Field descriptions of the display poe device command

Field	Description
PSE ID	ID of the PSE
SlotNo	Slot number of the PSE
SubSNo	Subslot number of the PSE
PortNum	Number of PoE interfaces on the PSE
MaxPower(W)	Maximum power of the PSE (W)
State	PSE state: on: The PSE is supplying power. off: The PSE stops supplying power. faulty: The PSE fails.
Model	PSE model

display poe interface

Syntax **display poe interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display poe interface** command to display the power information of the specified interface.

If no interface is specified, the power information of all PoE interfaces is displayed.

Examples # Display the power state of Ethernet 2/0/2.

```
<Sysname> display poe interface Ethernet 2/0/2
Port Power Enabled           : enable
Port Power Priority          : critical
Port Operating Status        : on
Port IEEE Class              : 0
Port Detection Status        : delivering-power
Port Power Mode              : signal
Port Current Power           : 5400      mW
Port Average Power           : 5490      mW
Port Peak Power              : 6500      mW
Port Max Power               : 15400     mW
Port Current                 : 108       mA
Port Voltage                 : 50.8      V
Port PD Description          : IP Phone For Room 101
```

Table 292 Field descriptions of the display poe interface ethernet command

Field	Description
Port Power Enabled	PoE state: enabled/disabled <ul style="list-style-type: none"> ■ enable: PoE is enabled. ■ disable: PoE is disabled.

Table 292 Field descriptions of the display poe interface ethernet command

Field	Description
Port Power Priority	Power priority of the PoE interface: <ul style="list-style-type: none"> critical (highest) high low
Port Operating Status	Operating state of a PoE interface: <ul style="list-style-type: none"> off: PoE is disabled. on: Power is supplied for a PoE interface normally. power lack: The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. power-itself: The external equipment is supplying power for itself. power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.
Port IEEE class	PD power class: 0, 1, 2, 3, 4
Port Detection Status	Power detection state of a PoE interface: <ul style="list-style-type: none"> disabled: The PoE function is disabled. searching: The PoE interface is searching for the PD. delivering-power: The PoE interface is supplying power for the PD. fault: There is a fault defined in 802.3af. test: The PoE interface is under test. other-fault: There is a fault other than defined in 802.3af. pd-disconnect: The PD is disconnected. Port detection status varies with devices.
Port Power Mode	Power mode of a PoE interface: <ul style="list-style-type: none"> signal: Power is supplied over signal cables. spare: Power is supplied over spare cables.
Port Current Power	Current power of a PoE interface, including PD consumption power and transmission loss The transmission loss usually does not exceed one watt.
Port Average Power	Average power of a PoE interface
Port Peak Power	Peak power of a PoE interface
Port Max Power	Maximum power of a PoE interface
Port Current	Current of a PoE interface
Port Voltage	Voltage of a PoE interface
Port PD Description	Description of the PD connected to the PoE interface, which is used to identify the type and location of the PD.

Display the state of all PoE interfaces.

```
<Sysname> display poe interface
Interface  Enable  Priority  CurPower  Operating  IEEE  Detection
           Enable  (W)      Status    class     Status
Eth2/0/1   disable low      0.0       off       0      disabled
Eth2/0/2   disable low      0.0       off       0      disabled
Eth2/0/3   disable low      0.0       off       0      disabled
```

```

Eth2/0/4   disable low      0.0    off    0    disabled
Eth2/0/5   disable low      0.0    off    0    disabled
Eth2/0/6   disable low      0.0    off    0    disabled
Eth2/0/7   disable low      0.0    off    0    disabled
Eth2/0/8   disable low      0.0    off    0    disabled
Eth2/0/9   disable low      0.0    off    0    disabled
Eth2/0/10  disable low      0.0    off    0    disabled
Eth2/0/11  disable low      0.0    off    0    disabled
Eth2/0/12  disable low      0.0    off    0    disabled
Eth2/0/13  disable low      0.0    off    0    disabled
Eth2/0/14  disable low      0.0    off    0    disabled
Eth2/0/15  enable  high     3.8    on     0    delivering-power
Eth2/0/16  enable  low      5.4    on     0    delivering-power
Eth2/0/17  disable low      0.0    off    0    disabled
Eth2/0/18  disable low      0.0    off    0    disabled
Eth2/0/19  disable low      0.0    off    0    disabled
Eth2/0/20  disable low      0.0    off    0    disabled
Eth2/0/21  disable low      0.0    off    0    disabled
Eth2/0/22  disable low      0.0    off    0    disabled
Eth2/0/23  disable low      0.0    off    0    disabled
Eth2/0/24  disable low      0.0    off    0    disabled
Eth2/0/25  disable low      0.0    off    0    disabled
Eth2/0/26  disable low      0.0    off    0    disabled
Eth2/0/27  disable low      0.0    off    0    disabled
Eth2/0/28  disable low      0.0    off    0    disabled
Eth2/0/29  disable low      0.0    off    0    disabled
Eth2/0/30  disable low      0.0    off    0    disabled
Eth2/0/31  disable low      0.0    off    0    disabled
Eth2/0/32  disable low      0.0    off    0    disabled
Eth2/0/33  disable low      0.0    off    0    disabled
Eth2/0/34  disable low      0.0    off    0    disabled
Eth2/0/35  disable low      0.0    off    0    disabled
Eth2/0/36  disable low      0.0    off    0    disabled
Eth2/0/37  disable low      0.0    off    0    disabled
Eth2/0/38  disable low      0.0    off    0    disabled
Eth2/0/39  disable low      0.0    off    0    disabled
Eth2/0/40  disable low      0.0    off    0    disabled
Eth2/0/41  disable low      0.0    off    0    disabled
Eth2/0/42  disable low      0.0    off    0    disabled
Eth2/0/43  disable low      0.0    off    0    disabled
Eth2/0/44  disable low      0.0    off    0    disabled
Eth2/0/45  disable low      0.0    off    0    disabled
Eth2/0/46  disable low      0.0    off    0    disabled
Eth2/0/47  disable low      0.0    off    0    disabled
Eth2/0/48  disable low      0.0    off    0    disabled
--- 2 port(s) on, 9.2 (W) consumed, 90.8 (W) remaining ---

```

Table 293 Field descriptions of the display poe interface command

Field	Description
Interface	Shortened form of a PoE interface
Enable	PoE state: enabled/disabled <ul style="list-style-type: none"> ■ enable: PoE is enabled. ■ disable: PoE is disabled.
Priority	Power priority of a PoE interface: <ul style="list-style-type: none"> ■ critical (highest) ■ high ■ low
CurPower	Current power of a PoE interface

Table 293 Field descriptions of the display poe interface command

Field	Description
Operating Status	<p>Operating state of a PoE interface</p> <ul style="list-style-type: none"> ■ off: PoE is disabled. ■ on: Power is supplied for a PoE interface normally. ■ power lack: The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. ■ power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. ■ power-itself: The external equipment is supplying power for itself. <p>power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.</p>
IEEE class	PD power class defined by IEEE
Detection Status	<p>Power detection state of a PoE interface:</p> <ul style="list-style-type: none"> ■ disabled: The PoE function is disabled. ■ searching: The PoE interface is searching for the PD. ■ delivering-power: The PoE interface is supplying power for the PD. ■ fault: There is a fault defined in 802.3af. ■ test: The PoE interface is under test. ■ There is a fault other than defined in 802.3af. <p>pd-disconnect: The PD is disconnected.</p>
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power consumed by the current PoE interface
Remaining	Total remaining power of the system

display poe interface power

Syntax `display poe interface power [interface-type interface-number]`

View Any view

Parameters `interface-type interface-number`: Specifies an interface by its type and number.

Description Use the **display poe interface power** command to display the power information of a PoE interface(s).

If no interface is specified, the power information of all PoE interfaces will be displayed.

Examples # Display the power information of Ethernet 2/0/2.

```
<Sysname> display poe interface power Ethernet 2/0/2
Interface  CurPower PeakPower MaxPower PD Description
           (W)       (W)       (W)
Eth2/0/2  15.0       15.3       15.4       Access Point on Room 509 for Peter
```

Display the power information of all PoE interfaces.


```

<Sysname> display poe interface power
Interface      CurPower      PeakPower      MaxPower      PD Description
              (W)           (W)           (W)
Eth2/0/1       0.0           0.0           15.4
Eth2/0/2       0.0           0.0           15.4
Eth2/0/3       0.0           0.0           15.4
Eth2/0/4       0.0           0.0           15.4
Eth2/0/5       0.0           0.0           15.4
Eth2/0/6       0.0           0.0           15.4
Eth2/0/7       0.0           0.0           15.4
Eth2/0/8       0.0           0.0           15.4
Eth2/0/9       0.0           0.0           15.4
Eth2/0/10      0.0           0.0           15.4
Eth2/0/11      0.0           0.0           15.4
Eth2/0/12      0.0           0.0           15.4
Eth2/0/13      0.0           0.0           15.4
Eth2/0/14      0.0           0.0           15.4
Eth2/0/15      3.8           3.9           10.0
Eth2/0/16      5.4           6.5           15.4
Eth2/0/17      0.0           0.0           15.4
Eth2/0/18      0.0           0.0           15.4
Eth2/0/19      0.0           0.0           15.4
Eth2/0/20      0.0           0.0           15.4
Eth2/0/21      0.0           0.0           15.4
Eth2/0/22      0.0           0.0           15.4
Eth2/0/23      0.0           0.0           15.4
Eth2/0/24      0.0           0.0           15.4
Eth2/0/25      0.0           0.0           15.4
Eth2/0/26      0.0           0.0           15.4
Eth2/0/27      0.0           0.0           15.4
Eth2/0/28      0.0           0.0           15.4
Eth2/0/29      0.0           0.0           15.4
Eth2/0/30      0.0           0.0           15.4
Eth2/0/31      0.0           0.0           15.4
Eth2/0/32      0.0           0.0           15.4
Eth2/0/33      0.0           0.0           15.4
Eth2/0/34      0.0           0.0           15.4
Eth2/0/35      0.0           0.0           15.4
Eth2/0/36      0.0           0.0           15.4
Eth2/0/37      0.0           0.0           15.4
Eth2/0/38      0.0           0.0           15.4
Eth2/0/39      0.0           0.0           15.4
Eth2/0/40      0.0           0.0           15.4
Eth2/0/41      0.0           0.0           15.4
Eth2/0/42      0.0           0.0           15.4
Eth2/0/43      0.0           0.0           15.4
Eth2/0/44      0.0           0.0           15.4
Eth2/0/45      0.0           0.0           15.4
Eth2/0/46      0.0           0.0           15.4
Eth2/0/47      0.0           0.0           15.4
Eth2/0/48      0.0           0.0           15.4
--- 2 port(s) on,    9.1 (W) consumed,    90.9 (W) remaining ---

```

Table 294 Field descriptions of the display poe interface power command

Field	Description
Interface	Shortened form of a PoE interface
CurPower	Current power of a PoE interface

Table 294 Field descriptions of the display poe interface power command

Field	Description
PeakPower	Peak power of a PoE interface
MaxPower	Maximum power of a PoE interface
PD Description	Description of the PD connected with a PoE interface When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power currently consumed by all PoE interfaces
Remaining	Total remaining power of the system

display poe power-usage

Syntax `display poe power-usage`

View Any view

Parameters None

Description Use the **display poe power-usage** command to display the power information of the PoE power and all PSEs

Examples # Display the power information of the PoE power and all PSEs.

```
<Sysname> display poe power-usage
PoE Current Power           : 2      W
PoE Max Power               : -
PoE Max Guaranteed Power   : 2250  W
PoE Remaining Allocated Power : 2213  W
PoE Remaining Guaranteed Power : 2250  W
PoE Total Powered Port Number : 1
Detailed power usage of PSE(s):
PSE ID  Max      Current  Peak      Average  Remaining  Powered
        (W)      (W)      (W)      (W)      Guaranteed(W) PortNum
10      37       2        3        2        37         1
```

Table 295 Field descriptions of the display poe power-usage command

Field	Description
PoE Current Power	Total consumption power of the PSE
PoE Max Power	Maximum PoE power
PoE Max Guaranteed Power	Guaranteed maximum PoE power, namely, the maximum power supplied to critical PSEs
PoE Remaining Allocate Power	Remaining allocable PoE power = Maximum PoE power - the sum of the maximum power of all PoE-enabled PSEs
PoE Remaining Guaranteed Power	Guaranteed remaining PoE power = Guaranteed maximum PoE power - the sum of the maximum power of critical PSEs
PoE Total Powered Port Number	Number of PoE interfaces that are currently supplying power
PSE ID	ID of the PSE

Table 295 Field descriptions of the display poe power-usage command

Field	Description
Max	Maximum power of the PSE
Current	Current power of the PSE
Peak	Peak power of the PSE
Average	Average power of the PSE
Remaining Guaranteed	Guaranteed remaining power of the PSE = Guaranteed maximum power of the PSE - the sum of the maximum power of critical PoE interfaces of the PSE
Powered PortNum	Number of PoE interfaces for which the PSE is supplying power

display poe pse

Syntax `display poe pse [pse-id]`

View Any view

Parameters *pse-id*: PSE ID. You can use the **display poe device** command to view the mapping between PSE ID and slot. If you enter a PSE ID, the information of the PSE is displayed. Otherwise, the information of all PSEs on the device is displayed.

Description Use the **display poe pse** command to display the information of the specified PSE.

Examples # Display the information of PSE 7.

```
<Sysname> display poe pse 7
PSE ID                : 7
PSE Slot No           : 0
PSE SubSlot No        : 0
PSE Model              : LSQ1FV48SA
PSE Power Enabled      : enable
PSE Power Preempted   : no
PSE Power Priority     : low
PSE Current Power     : 9      W
PSE Average Power     : 8      W
PSE Peak Power        : 11     W
PSE Max Power         : 100    W
PSE Remaining Guaranteed : 100    W
PSE CPLD Version      : -
PSE Software Version  : 503
PSE Hardware Version  : 1
PSE Legacy Detection  : enable
PSE Utilization-threshold : 80
PSE Pse-policy Mode   : priority
PSE Pd-policy Mode    : priority
PSE PD Disconnect Detect Mode : AC
```

Table 296 Field descriptions of the display poe pse command

Field	Description
PSE ID	ID of the PSE
PSE Slot No	Slot number of the PSE
PSE Model	Model of the PSE module
PSE Power Enabled	PoE is enabled for the PSE
PSE Power Preempted	PSE power preempted state <ul style="list-style-type: none"> ■ no: The power of the PSE is not preempted. ■ yes: The power of the PSE is preempted so that it cannot supply power, although PoE is enabled for the PSE
PSE Power Priority	Power priority of the PSE
PSE Current Power	Current power of the PSE
PSE Average Power	Average power of the PSE
PSE Peak Power	Peak power of the PSE
PSE Max Power	Maximum power of the PSE
PSE Remaining Guaranteed	Guaranteed remaining power of the PSE = Maximum power of the PSE- the sum of the maximum power of the critical PoE interfaces of the PSE
PSE CPLD Version	PSE CPLD version
PSE Software Version	PSE software version number
PSE Hardware Version	PSE hardware version number
PSE Legacy Detection	Nonstandard PD detection by the PSE: <ul style="list-style-type: none"> ■ enable: Enabled ■ disable: Disabled
PSE Utilization-threshold	PSE power alarm threshold
PSE Pse-policy Mode	PSE power management policy mode
PSE Pd-policy Mode	PD power management policy mode
PSE PD Disconnect Detect Mode	PD disconnection detection mode

display poe-power

Syntax **display poe-power**

View Any view

Parameters None

Description Use the **display poe-power** command to display the information of the PoE power.

Examples # Display information of the PoE power.

```
<Sysname> display poe-power
PoE Current Power      : 1870      W
PoE Average Power     : 2100      W
```

```

PoE Peak Power           : 2350    W
PoE Max Power           : 2000    W
PoE Nominal Power       : 2500    W
PoE Current Current     : 3.00    A
PoE Current Voltage     : 55.00   V
PoE Input-threshold Lower : 111.22  V
PoE Input-threshold Upper : 131.00  V
PoE Output-threshold Lower : 45.00   V
PoE Output-threshold Upper : 57.00   V
PoE Hardware Version    : 0002
PoE Software Version    : 0001
PoE Power Number       : 2
PoE Power 1:
  Manufacturer          : Tyco Electronics Com
  Type                  : PSE2500-A
  Status                : Normal
PoE Power 2:
  Manufacturer          : Tyco Electronics Com
  Type                  : PSE2500-B
  Status                : Normal

```

Table 297 Field descriptions of the display poe-power command

Field	Description
PoE Current Power	Current PoE power
PoE Average Power	Average PoE power
PoE Peak Power	Peak PoE power
PoE Max Power	Maximum PoE power
PoE Nominal Power	Nominal PoE power
PoE Current Current	Current PoE current
PoE Current Voltage	Current PoE voltage
PoE Input-threshold Lower	AC input under-voltage threshold
PoE Input-threshold Upper	AC input over-voltage threshold
PoE Output-threshold Lower	DC output under-voltage threshold
PoE Output-threshold Upper	DC output over-voltage threshold
PoE Hardware Version	PoE hardware version number
PoE Software Version	PoE software version number
PoE Power Number	Number of PoE power supply units
PoE Power Manufacturer	Manufacturer of the PoE power
PoE Power Type	Type of the PoE power
PoE Power Status	PoE power state: <ul style="list-style-type: none"> ■ Normal ■ Absent ■ Off ■ Master ■ Slave ■ Balance ■ Redundant ■ Alarm ■ Faulty

display poe-power ac-input state

- Syntax** `display poe-power ac-input state`
- View** Any view
- Parameters** None
- Description** Use the **display poe-power ac-input state** command to display the state information of the AC input power.
- Examples** # Display the state information of the AC input power.

```
<Sysname> display poe-power ac-input state
Module Number           : 2
Output AC Current A Alarm : Normal
Output AC Current B Alarm : Under Limit
Output AC Current C Alarm : Lack Phase
Module 1:
    Volt Phase AB Alarm   : Above Limit
    Volt Phase BC Alarm   : Fuse Broken
    Volt Phase CA Alarm   : Switch Off
Module 2:
    Volt Phase AB Alarm   : Above Limit
    Volt Phase BC Alarm   : Fuse Broken
    Volt Phase CA Alarm   : Switch Off
```

Table 298 Field descriptions of display poe-power ac-input state

Field	Description
Module Number	Number of modules that a power supply unit (PSU) contains
Output AC Current A/B/C Alarm	Output three-phase AC voltage state: <ul style="list-style-type: none"> ■ Normal: The voltage is normal. ■ Under Limit: The voltage is below the lower limit. ■ Above Limit: The voltage is above the upper limit. ■ Lack Phase: A phase is lost. ■ Fuse Broken: The fuse is broken. ■ Switch Off: The switch is turned off. ■ Other Error: Other faults
Volt Phase AB/BC/CA Alarm	AC voltage input state: Same as those of the output three-phase AC current

display poe-power alarm

- Syntax** `display poe-power alarm`
- View** Any view
- Parameters** None

Description Use the **display poe-power alarm** command to display the alarm information of the PoE power.

Examples # Display the alarm information of the PoE power.

```
<Sysname> display poe-power alarm
PSU Number           : 3
PSU 1 State          : Normal
PSU 2 State          : Disconnect
PSU 3 State          : Over Voltage
                     Over Temperature
```

Table 299 Field descriptions of the display poe-power alarm command

Field	Description
PSU Number	Number of PSUs
PSU x State	PSU state: <ul style="list-style-type: none"> ■ Normal: The PSU is normal. ■ Disconnect: The PSU is disconnected. ■ Input Error: An input error occurs to the PSU. ■ Output Error: An output error occurs to the PSU. ■ Over Voltage: An over-voltage occurs to the PSU. ■ Over Temperature: An over-temperature occurs to the PSU. ■ Fan Error: A fault occurs to the fan of the PSU. ■ Shut Down: The PSU is shut down. ■ Current Restricted: The current of the PSU is restricted.

display poe-power dc-output state

Syntax **display poe-power dc-output state**

View Any view

Parameters None

Description Use the **display poe-power dc-output state** command to display the state information of the DC output power

Examples # Display the state information of the DC output power.

```
<Sysname> display poe-power dc-output state
DC Output State      : Normal
```

Table 300 Field descriptions of display poe-power dc-output state

Field	Description
DC Output State	DC output state. See Table 298.

display poe-power dc-output value

- Syntax** `display poe-power dc-output value`
- View** Any view
- Parameters** None
- Description** Use the **display poe-power dc-output value** command to display the parameter values of the DC output power.
- Examples** # Display the parameter values of the DC output power.

```
<Sysname> display poe-power dc-output value
DC Output Voltage      : 54.05 V
DC Output Current      : 0.35 A
```

Table 301 Field descriptions of display poe-power dc-output value

Field	Description
DC Output Voltage	DC output voltage
DC Output Current	DC output current

display poe-power status

- Syntax** `display poe-power status`
- View** Any view
- Parameters** None
- Description** Use the **display poe-power status** command to display the status information of the PoE power.
- Examples** # Display the status information of the PoE power.

```
<Sysname>display poe-power status
Switch Number          : 1
Switch 1 State         : AC Switch High Voltage
DC Output State        : Under Limit
DC Output Voltage      : 56.00 V
DC Output Current      : 15.00 A
Module Number          : 2
Output AC Current A Alarm : Normal
Output AC Current B Alarm : Under Limit
Output AC Current C Alarm : Lack Phase
Module 1:
    Volt Phrase AB Alarm  : Above Limit
    Volt Phrase BC Alarm  : Fuse Broken
    Volt Phrase CA Alarm  : Switch Off
Module 2:
```



```

Volt Phrase AB Alarm      : Above Limit
Volt Phrase BC Alarm      : Fuse Broken
Volt Phrase CA Alarm      : Switch Off

```

Table 302 Field descriptions of the display poe-power status command

Field	Description
Switch Number	Number of power switches
Switch x State	State of a power switch
DC Output State	DC output state
DC Output Voltage	DC output voltage
DC Output Current	DC output current
Module Number	Number of modules that a PSU contains
Output AC Current A/B/C Alarm	Output three-phase AC current state. See Table 298.
Volt Phrase AB/BC/CA Alarm	AC voltage input state. See Table 298.

display poe-power supervision-module

Syntax `display poe-power supervision-module`

View Any view

Parameters None

Description Use the **display poe-power supervision-module** command to display the information of the monitoring module of the PoE power.

Examples # Display the information of the monitoring module of the PoE power.

```

<Sysname> display poe-power supervision-module
Supervision Version      : 2.6
Supervision Name         : Summer Pms
PoE Power Type           : PSE2500-A
PoE Current Power        : 600 W
PoE Average Power        : 630 W
PoE Peak Power           : 650 W
PoE Nominal Power        : 2400 W
PSU Available Number     : 1
PSU 1:
  Nominal Output Power   : 2500(W) (220V)/1250(W) (110V)
  Hardware Version Info   : NP Series

```

Table 303 Field descriptions of display poe-power supervision-module

Field	Description
Supervision Version	Software version number of the monitoring module of the PoE power
Supervision Name	Name of the monitoring module of the PoE power
PoE Power Type	Type of the PoE power
PoE Current Power	Current consumption power
PoE Average Power	Average power

Table 303 Field descriptions of display poe-power supervision-module

Field	Description
PoE Peak Power	Peak power
PoE Nominal Power	Nominal power
PSU Available Number	Number of available PSUs
Nominal Output Power	Nominal output power of a PSU
Hardware Version Info	Hardware version information of the PSU

display poe-power switch state

Syntax `display poe-power switch state`

View Any view

Parameters None

Description Use the **display poe-power switch state** command to display the switch information of the PoE power.

Examples # Display the switch information of the PoE power.

```
<Sysname> display poe-power switch state
Switch Number          : 1
Switch 1 State         : AC Switch High Voltage
```

Table 304 Field descriptions of display poe-power switch state

Field	Description
Switch Number	Number of power switches
Switch x State	Switch state: <ul style="list-style-type: none"> ■ AC Switch On: The AC switch is turned on. ■ AC Switch Off: The switch is turned off. ■ AC Switch High Voltage: The voltage of the AC switch is high. ■ AC Switch Low Voltage: The voltage of the AC switch is low.

display poe-profile

Syntax `display poe-profile [index index | name profile-name]`

View Any view

Parameters **index** *index*: Index number of the PoE configuration file, in the range 1 to 100.

name *profile-name*: Name of the PoE configuration file, a string of 1 to 15 characters.

Description Use the **display poe-profile** command to display all information of the configurations and applications of the PoE configuration file.

If no argument is specified, all information of the configurations and applications of existing PoE configuration files is displayed.

Examples # Display all information of the configurations and applications of the current PoE configuration file.

```
<Sysname> display poe-profile
Poe-profile      Index  ApplyNum  Interface  Configuration
AA3456789012345  1      3          GE3/0/1    poe enable
                  GE3/0/2    poe priority critical
                  GE3/0/3

poe-profileAA    2      1          GE3/0/4    poe enable
poe max-power 12300

poe-profileBB    3      0          poe enable
poe priority critical
poe max-power 15400

--- 3 poe-profile(s) created, 4 port(s) applied ---
```

Table 305 Field descriptions of the display poe-profile command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
poe-profile(s) created	Number of PoE configuration files
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

Display all information of the configurations and applications of the PoE configuration file whose index number is 1.

```
<Sysname> display poe-profile index 1
Poe-profile      Index  ApplyNum  Interface  Configuration
AA3456789012345  1      2          GE3/0/2    poe enable
                  GE3/0/4    poe priority critical
poe max-power 12300

--- 2 port(s) applied ---
```

Table 306 Field descriptions of the display poe-profile index command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file

Table 306 Field descriptions of the display poe-profile index command

Field	Description
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

Display all information of the configurations and applications of the PoE configuration file named **AA**.

```
<Sysname> display poe-profile name AA
Poe-profile      Index  ApplyNum  Interface  Configuration
AA              1      2         GE3/0/1    poe enable
                GE3/0/2    poe priority critical
                poe max-power 12300

--- 2 port(s) applied ---
```

Table 307 Field descriptions of the display poe-profile name command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

display poe-profile interface

Syntax **display poe-profile interface** *interface-type interface-number*

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display poe-profile interface** command to display all information of the configurations and applications of the PoE configuration file that currently takes effect on the specified PoE interface.

Examples # Display all information of the configurations and applications of the current PoE configuration file applied to Ethernet 2/0/2.

```
<Sysname> display poe-profile interface Ethernet 2/0/2
Poe-profile      Index  ApplyNum  Interface  Current Configuration
AA3456789012345 1      2         Eth2/0/2    poe enable
                poe priority critical
```

Table 308 Field descriptions of the display poe-profile interface command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which the PoE configuration file is applied

Table 308 Field descriptions of the display poe-profile interface command

Field	Description
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Current Configuration	Configurations of the PoE configuration file that currently take effect on a PoE interface



Because not all the configurations of a PoE configuration file can be applied successfully, only the configurations that currently take effect on the interface are displayed.

poe enable

Syntax **poe enable**

undo poe enable

View PoE interface view, PoE-profile file view

Parameters None

Description Use the **poe enable** command to enable PoE on a PoE interface.

Use the **undo poe enable** command to disable PoE on a PoE interface.

By default, PoE is disabled on a PoE interface.



CAUTION:

- *If a PoE configuration file is already applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.*
- *If a PoE configuration file is applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE interface view.*

Examples # Enable PoE on a PoE interface.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] poe enable
```

Enable PoE on a PoE interface through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe enable
[Sysname-poe-profile-abc-1] quit
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] apply poe-profile name abc
```

poe enable pse

Syntax **poe enable pse** *pse-id*
undo poe enable pse *pse-id*

View System view

Parameters *pse-id*: PSE ID.

Description Use the **poe enable pse** command to enable PoE for the PSE.
Use the **undo poe enable pse** command to disable PoE for the PSE.
By default, PoE is disabled for the PSE.

Examples # Enable PoE for PSE 7.

```
<Sysname> system-view  
[Sysname] poe enable pse 7
```

poe legacy enable

Syntax **poe legacy enable** [**pse** *pse-id*]
undo poe legacy enable [**pse** *pse-id*]

View System view

Parameters **pse** *pse-id*: Specifies a PSE ID.

Description Use the **poe legacy enable** command to enable the PSE to detect nonstandard PDs.
Use the **undo poe legacy enable** command to disable the PSE from detecting nonstandard PDs.
By default, the PSE is disabled from detecting nonstandard PDs.

Examples # Enable PSE 7 to detect nonstandard PDs.

```
<Sysname> system-view  
[Sysname] poe legacy enable pse 7
```

poe max-power

Syntax **poe max-power** *max-power*
undo poe max-power

View	PoE interface view, PoE-profile file view
Parameters	<i>max-power</i> : Maximum power in milliwatts allocated to a PoE interface, in the range 1000 to 15400.
Description	Use the poe max-power command to configure the maximum power for a PoE interface. Use the undo poe max-power command to restore the default. By default, the maximum power of the PoE interface is 15,400 milliwatts.
Examples	<pre># Set the maximum power of Ethernet 2/0/2 to 12,000 milliwatts. <Sysname> system-view [Sysname] interface Ethernet 2/0/2 [Sysname-Ethernet2/0/2] poe max-power 12000 # Set the maximum power of Ethernet 2/0/2 to 12,000 milliwatts through a PoE configuration file. <Sysname> system-view [Sysname] poe-profile abc [Sysname-poe-profile-abc-1] poe max-power 12000 [Sysname-poe-profile-abc-1] quit [Sysname] interface Ethernet 2/0/2 [Sysname-Ethernet2/0/2] apply poe-profile name abc</pre>

poe max-power

Syntax	poe max-power <i>max-power</i> [pse <i>pse-id</i>] undo poe max-power [pse <i>pse-id</i>]
View	System view
Parameters	<i>max-power</i> : Maximum power in watts of the PSE, in the range 37 to 806. pse <i>pse-id</i> : Specifies a PSE ID.
Description	Use the poe max-power command to configure the maximum power for the PSE. Use the undo poe max-power command to restore the default maximum power of the PSE. The default maximum power of the PSE is 37 watts. Note that: <ul style="list-style-type: none"> ■ The maximum power of the PSE must be greater than or equal to the sum of the maximum power of all critical PoE interfaces on the PSE so as to guarantee

the power supply to these PoE interfaces. When the consumption power of all PDs connected to the PSE is greater than the maximum power of the PSE, some PDs will be powered off.

- The sum of the maximum power of all PSEs cannot exceed the maximum PoE power.

Related commands: **poe priority.**

Examples # Set the maximum power of PSE 7 to 150 watts.

```
<Sysname> system-view
[Sysname] poe max-power 150 pse 7
```

poe mode

Syntax **poe mode signal**

undo poe mode

View PoE interface view, PoE-profile file view

Parameters **signal**: Specifies the PoE mode as **signal** (power over signal cables).

Description Use the **poe mode** command to configure a PoE mode.

Use the **undo poe mode** command to restore the default.

By default, the PoE mode is **signal** (power over signal cables).

The PSE supplies power for a PoE interface in the following two modes: **signal** and **spare**.

- In the signal mode, lines in Category 3 and 5 twisted pair cables used for transmitting data are also used for supplying DC power.
- In the spare mode, lines in Category 3 and 5 twisted pair cables not in use are used for supplying DC power.

Currently, the S7900Es do not support the spare mode.

Examples # Set the PoE mode to **signal** (power over signal cables).

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] poe mode signal
```

Set the PoE mode to **signal** (power over signal cables) through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe mode signal
[Sysname-poe-profile-abc-1] quit
```



```
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] apply poe-profile name abc
```

poe pd-description

Syntax **poe pd-description** *string*

undo poe pd-description

View PoE interface view

Parameters *string*: Description of the PD connected to a PoE interface, a string of 1 to 80 characters.

Description Use the **poe pd-description** command to configure a description for the PD connected to a PoE interface.

Use the **undo poe pd-description** command to restore the default.

By default, no description is available for the PD connected to a PoE interface.

Examples # Configure the description for the PD connected to Ethernet 2/0/2 as IP Phone for Room 101.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] poe pd-description IP Phone For Room 101
```

poe pd-policy priority

Syntax **poe pd-policy priority**

undo poe pd-policy priority

View System view

Parameters None

Description Use the **poe pd-policy priority** command to configure a PD power management priority policy.

Use the **undo poe pd-policy priority** command to remove the PD power management priority policy.

By default, no PD power management priority policy is configured.

Examples # Configure a PD power management priority policy

```
<Sysname> system-view
[Sysname] poe pd-policy priority
```

poe power max-value

Syntax `poe power max-value max-power`

`undo poe power max-value`

View System view

Parameters *max-power*: Maximum PoE power, namely, maximum power that the device can provide for all PSEs. In consideration of the transient peak power effect, the maximum power available is 5% higher than the configured maximum power. The range, default value, granularity, and limit vary with devices.

Description Use the **poe power max-value** command to configure the maximum PoE power.

Use the **undo poe power max-value** command to restore the default.

Note that the configured maximum PoE power cannot exceed the rated PoE power.

Examples # Set the maximum PoE power to 1,000 watts for the device.

```
<Sysname> system-view  
[Sysname] poe power max-value 1000
```

poe priority

Syntax `poe priority { critical | high | low }`

`undo poe priority`

View PoE interface view, PoE-profile file view

Parameters **critical**: Sets the power priority of a PoE interface to **critical**. The PoE interface whose power priority level is **critical** works in guaranteed mode, that is, power is first supplied to the PD connected to this critical PoE interface.

high: Sets the power priority of a PoE interface to **high**.

low: Sets the power priority of a PoE interface to **low**.

Description Use the **poe priority** command to configure a power priority level for a PoE interface.

Use the **undo poe priority** command to restore the default.

By default, the power priority of a PoE interface is **low**.

Note that:

- When the PoE power is insufficient, power is first supplied to PoE interfaces with a higher priority level.
- If a PoE configuration file is already applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.
- If a PoE configuration file is applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE interface view.
- If two PoE interfaces have the same priority level, the PoE interface with a smaller ID has the higher priority level.

Examples # Set the power priority of Ethernet 2/0/2 to **critical**.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] poe priority critical
```

Set the power priority of Ethernet 2/0/2 to **critical** through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe priority critical
[Sysname-poe-profile-abc-1] quit
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] apply poe-profile name abc
```

poe priority

Syntax **poe priority** { **critical** | **high** | **low** } [**pse** *pse-id*]

undo poe priority [**pse** *pse-id*]

View System view

Parameters **critical**: Sets the power priority level of the PSE to **critical**. The PSE whose power priority level is **critical** works in guaranteed mode, that is, power is first supplied to the PSE.

high: Sets the power priority of the PSE to **high**.

low: Sets the power priority of the PSE to **low**.

pse *pse-id*: Specifies a PSE ID.

Description Use the **poe priority** command to configure a power priority level for the PSE.

Use the **undo poe priority** command to restore the default.

By default, the power priority level of the PSE is **low**.

When the PoE power is insufficient, power is first supplied to PSE with a higher power priority level.

Examples # Set the power priority of PSE 7 to **critical**.

```
<Sysname> system-view
[Sysname] poe priority critical pse 7
```

poe pse-policy priority

Syntax **poe pse-policy priority**
undo poe pse-policy priority

View System view

Parameters None

Description Use the **poe pse-policy priority** command to configure a PSE power management priority policy.

Use the **undo poe pse-policy priority** command to remove the PSE power management priority policy.

By default, no PSE power management priority policy is configured.

Examples # Configure a PSE power management priority policy.

```
<Sysname> system-view
[Sysname] poe pse-policy priority
```

poe update

Syntax **poe update { full | refresh } filename [pse pse-id]**

View System view

Parameters **full**: Specifies to upgrade the PSE processing software in full mode when the software is unavailable.

refresh: Specifies to upgrade the PSE processing software in refresh mode when the software is available.

filename: Name of the upgrade file, a string of 1 to 64 characters. This file must be under the root directory of the file system of the device. The extension of the upgrade file is .s19.

pse pse-id: Specifies a PSE ID.

Description Use the **poe update** command to upgrade the PSE processing software online.

Examples # Upgrade the processing software of PSE 7 online.

```
<Sysname> system-view
[Sysname] poe update refresh 0400_001.S19 pse 7
```

poe utilization-threshold

Syntax **poe utilization-threshold** *utilization-threshold-value* [**pse** *pse-id*]
undo poe utilization-threshold [**pse** *pse-id*]

View System view

Parameters *utilization-threshold-value*: Power alarm threshold in percentage, in the range 1 to 99.

pse *pse-id*: Specifies a PSE ID.

Description Use the **poe utilization-threshold** command to configure a power alarm threshold for the PSE.

Use the **undo poe utilization-threshold** command to restore the default power alarm threshold of the PSE.

By default, the power alarm threshold for the PSE is 80%.

The system sends a Trap message when the percentage of power utilization exceeds the alarm threshold. If the percentage of the power utilization always keeps above the alarm threshold, the system does not send any Trap message. Instead, when the percentage of the power utilization drops below the alarm threshold, the system sends a Trap message again.

Examples # Set the power alarm threshold of PSE 7 to 90%.

```
<Sysname> system-view
[Sysname] poe utilization-threshold 90 pse 7
```

poe-power input-threshold

Syntax **poe-power input-threshold** { **lower** | **upper** } *value*
undo poe-power input-threshold { **lower** | **upper** }

View System view

Parameters **lower** *value*: Specifies an under-voltage threshold in volts, in the range 90 to 264, with the default value being 90.

upper *value*: Specifies an over-voltage threshold in volts, in the range 90 to 264, with the default value being 264.

Description Use the **poe-power input-threshold** command to configure an AC input under-voltage/over-voltage threshold.

Use the **undo poe-power input-threshold** command to restore the default.

Examples # Set the AC input under-voltage threshold to 181 V.

```
<Sysname> system-view
[Sysname] poe-power input-threshold lower 181
```

Set the AC input over-voltage threshold to 264 V.

```
<Sysname> system-view
[Sysname] poe-power input-threshold upper 264
```

poe-power output-threshold

Syntax **poe-power output-threshold** { **lower** | **upper** } *value*
undo poe-power output-threshold { **lower** | **upper** }

View System view

Parameters **lower** *value*: Specifies an under-voltage threshold in volts, in the range 45 to 47, with the default value being 45.

upper *value*: Specifies an over-voltage threshold in volts, in the range 55 to 57, with the default value being 57.

Description Use the **poe-power output-threshold** command to configure a DC output under-voltage/over-voltage threshold.

Use the **undo poe-power output-threshold** command to restore the default.

Examples # Set a DC output under-voltage threshold to 45 V.

```
<Sysname> system-view
[Sysname] poe-power output-threshold lower 45
```

Set a DC output over-voltage threshold to 57 V.

```
<Sysname> system-view
[Sysname] poe-power output-threshold upper 57
```

poe-profile

Syntax **poe-profile** *profile-name* [*index*]
undo poe-profile { **index** *index* | **name** *profile-name* }

View System view

Parameters *profile-name*: Name of a PoE configuration file, a string of 1 to 15 characters. A PoE configuration file name begins with a letter (a through z or A through Z) and must not contain reserved keywords such as **undo**, **all**, **name**, **interface**, **user**, **poe**, **disable**, **max-power**, **mode**, **priority** and **enable**.

index: Index number of a PoE configuration file, in the range 1 to 100.

Description Use the **poe-profile** *profile-name* command to create a PoE configuration file and enter PoE-profile view.

Use the **undo poe-profile** command to delete the specified PoE configuration file.

If no index is specified, the system automatically assigns an index to the PoE configuration file, starting from 1.

Note that if a PoE configuration file is already applied to a PoE interface, you cannot delete it. To delete the file, you must first execute the **undo apply poe-profile** command to remove the application of the PoE configuration file to the PoE interface.

Examples # Create a PoE configuration file, name it **abc**, and specify the index number as **3**.

```
<Sysname> system-view  
[Sysname] poe-profile abc 3
```


90

IPv4 VRRP CONFIGURATION COMMANDS



At present, the interfaces that VRRP involves can only be VLAN interfaces unless otherwise specified.

display vrrp

Syntax **display vrrp** [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameters **verbose**: Displays detailed state information of VRRP.

interface *interface-type interface-number*: Displays VRRP state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays state information of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

Description Use the **display vrrp** command to display the state information of VRRP.

If you do not specify **verbose**, only the brief state information of VRRP is displayed.

If you specify both interface and standby group, only the state information of the specified standby group is displayed; if you only specify an interface, the state information of all the standby groups on the interface is displayed; if you specify neither, the state information of all the standby groups on the device is displayed.

Examples # Display brief information about all standby groups on the device.

```
<Sysname> display vrrp
IPv4 Standby Information:
Run Method      : VIRTUAL-MAC
Virtual IP Ping : Enable
The total number of the virtual routers: 1
Interface      VRID  State      Run   Adver.  Auth   Virtual
                Pri   Time      Pri   Time   Type   IP
-----
Vlan100        1    Master     100   1       NONE   10.10.10.2
```

Display detailed information about all standby groups on the device.

```

<Sysname> display vrrp verbose
IPv4 Standby Information:
Run Method      : VIRTUAL-MAC
Virtual IP Ping : Enable
Interface       : Vlan-interface100
VRID            : 1                      Adver. Timer   : 1
Admin Status    : UP                      State          : Master
Config Pri     : 100                     Run Pri       : 100
Preempt Mode    : YES                     Delay Time    : 0
Auth Type       : NONE
Track IF        : Vlan-interface200      Pri Reduced    : 10
Virtual IP      : 10.10.10.2
Virtual MAC     : 0000-5e00-0101
Master IP       : 10.10.10.1

```

Table 309 Field descriptions of the display vrrp command

Field	Description
Run Method	Current VRRP running mode, real MAC or virtual MAC
Virtual IP Ping	Whether you can ping the virtual IP address of the standby group
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
Adver. Timer	VRRP advertisement interval
Admin Status	Administrative state: UP or DOWN
State	Status of the switch in the standby group, master, backup, or initialize
Config Pri	Configured priority
Run Pri	Running priority
Preempt Mode	Preemption mode
Delay Time	Preemption delay, not displayed when the device works in non-preemption mode.
Auth Type	Authentication type
Track IF	The interface to be tracked. It is displayed only after the execution of the vrrp vrid track command.
Pri Reduced	The priority value that is reduced when the interface being tracked is down. It is displayed only after the execution of the vrrp vrid track command.
Virtual IP	Virtual IP addresses of the standby group
Virtual MAC	Virtual MAC address corresponding to the virtual IP address of the standby group. It is displayed only when the switch is in the state of master.
Master IP	Primary IP address of the interface to which the switch in the state of master belongs

display vrrp statistics

Syntax **display vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameters **interface** *interface-type interface-number*: Displays VRRP statistics of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays statistics of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

Description Use the **display vrrp statistics** command to display statistics about VRRP.

If you specify both interface and standby group, only the statistics about the specified standby group are displayed; if you only specify an interface, the statistics about all the standby groups on the interface are displayed; if you specify neither, the statistics about all the standby groups on the device are displayed.

Examples # Display the statistics about all standby groups.

```
<Sysname> display vrrp statistics
Interface          : Vlan-interface100
VRID               : 1
Checksum Errors   : 16          Version Errors           : 0
Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors : 0
IP TTL Errors     : 0          Auth Failures            : 0
Invalid Auth Type : 0          Auth Type Mismatch       : 0
Packet Length Errors : 0          Address List Errors      : 0
Become Master     : 1          Priority Zero Pkts Rcvd   : 0
Advertise Rcvd    : 16         Priority Zero Pkts Sent   : 0
Advertise Sent    : 40

Interface          : Vlan-interface200
VRID               : 105
Checksum Errors    : 0          Version Errors           : 0
Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors : 0
IP TTL Errors     : 0          Auth Failures            : 0
Invalid Auth Type : 0          Auth Type Mismatch       : 0
Packet Length Errors : 0          Address List Errors      : 0
Become Master     : 0          Priority Zero Pkts Rcvd   : 0
Advertise Rcvd    : 0          Priority Zero Pkts Sent   : 0
Advertise Sent    : 30

Global statistics
Checksum Errors    : 16
Version Errors     : 0
VRID Errors        : 20
```

Table 310 Field descriptions of the display vrrp statistics command

Field	Description
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
Checksum Errors	Number of packets with checksum errors
Version Errors	Number of packets with version errors
Invalid Type Pkts Rcvd	Number of packets with incorrect packet type
Advertisement Interval Errors	Number of packets with advertisement interval errors
IP TTL Errors	Number of packets with TTL errors
Auth Failures	Number of packets with authentication failures
Invalid Auth Type	Number of packets with authentication failures due to invalid authentication types
Auth Type Mismatch	Number of packets with authentication failures due to mismatching authentication types
Packet Length Errors	Number of packets with VRRP packet length errors

Table 310 Field descriptions of the display vrrp statistics command

Field	Description
Address List Errors	Number of packets with virtual IP address list errors
Become Master	Number of times that the switch worked as the master
Priority Zero Pkts Rcvd	Number of received advertisements with the priority of 0
Advertise Rcvd	Number of received advertisements
Advertise Sent	Number of advertisements sent
Global statistics	Statistics about all standby groups
Checksum Errors	Total number of packets with checksum errors
Version Errors	Total number of packets with version errors
VRID Errors	Total number of packets with VRID errors

reset vrrp statistics

Syntax `reset vrrp statistics [interface interface-type interface-number [vrid virtual-router-id]]`

View User view

Parameters `interface interface-type interface-number`: Clears VRRP statistics of a specified interface. `interface-type interface-number` specifies an interface by its type and number.

`vrid virtual-router-id`: Clears VRRP statistics of the specified standby group. `virtual-router-id` specifies a standby group by its group number, in the range 1 to 255.

Description Use the `reset vrrp statistics` command to clear VRRP statistics.

If you specify both the interface and standby group, the statistics about the specified standby group on the specified interface are cleared; if you specify only the interface, the statistics about all the standby groups on the interface are cleared; if you specify neither, the statistics about all the standby groups on the device are cleared.

Examples # Clear the statistics about all the standby groups on the device.

```
<Sysname> reset vrrp statistics
```

vrrp vrid authentication-mode

Syntax `vrrp vrid virtual-router-id authentication-mode { md5 | simple } key`

`undo vrrp vrid virtual-router-id authentication-mode`

View Interface view

- Parameters** *virtual-router-id*: VRRP standby group number, in the range 1 to 255.
- simple**: Plain text authentication mode.
- md5**: Authentication header (AH) authentication using the MD5 algorithm.
- key*: Authentication key, case sensitive.
- When **simple** authentication applies, the authentication key is in plain text with a length of 1 to 8 characters.
 - When **md5** authentication applies, the authentication key is in MD5 cipher text or in plain text and the length of the key depends on its input format. If the key is input in plain text, its length is 1 to 8 characters, such as 1234567; if the key is input in cipher text, its length must be 24 characters, such as `_(TT8F]Y5SQ=^Q'MAF4<1!!`.
- Description** Use the **vrrp vrid authentication-mode** command to configure authentication mode and authentication key for the VRRP standby groups to send and receive VRRP packets.
- Use the **undo vrrp vrid authentication-mode** command to restore the default.
- By default, authentication is disabled.
- Note that:
- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
 - You may configure different authentication types and authentication keys for the standby groups on an interface. However, the members of the same standby group must use the same authentication mode and authentication key.
- Examples** # Set the authentication mode and authentication key for VRRP standby group 1 on interface VLAN-interface 2 to send and receive VRRP packets.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 authentication-mode simple Sysname
```

---

## vrrp method

**Syntax** **vrrp method { real-mac | virtual-mac }**  
**undo vrrp method**

**View** System view

**Parameters** **real-mac**: Associates the real MAC address of the interface with the virtual IP address of the standby group.

**virtual-mac:** Associates the virtual MAC address of the switch with the virtual IP address of the standby group.

**Description** Use the **vrrp method** command to set the mappings between the virtual IP addresses and the MAC addresses of the standby groups.

Use the **undo vrrp method** command to restore the default mapping.

By default, the virtual MAC address of the standby group is associated with the virtual IP address.

You must configure the mapping between the virtual IP address and the MAC address before configuring a standby group. Otherwise, your configuration will fail.

**Examples** # Associate the virtual IP address of the standby group with the real MAC address of the routing interface.

```
<Sysname> system-view
[Sysname] vrrp method real-mac
```

## vrrp ping-enable

**Syntax** **vrrp ping-enable**

**undo vrrp ping-enable**

**View** System view

**Parameters** None

**Description** Use the **vrrp ping-enable** command to enable users to ping the virtual IP addresses of standby groups.

Use the **undo vrrp ping-enable** command to disable the virtual IP addresses of standby groups from being pinged.

By default, the virtual IP addresses of standby groups can be pinged.

Perform this configuration before configuring a standby group.

**Examples** # Enable users to ping the virtual IP addresses of standby groups.

```
<Sysname> system-view
[Sysname] vrrp ping-enable
```

## vrrp un-check ttl

**Syntax** **vrrp un-check ttl**

**undo vrrp un-check ttl**

|                    |                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View</b>        | Interface view                                                                                                                                                                                                                           |
| <b>Parameters</b>  | None                                                                                                                                                                                                                                     |
| <b>Description</b> | <p>Use the <b>vrrp un-check ttl</b> command to disable TTL check on VRRP packets.</p> <p>Use the <b>undo vrrp un-check ttl</b> command to enable TTL check on VRRP packets.</p> <p>By default, TTL check on VRRP packets is enabled.</p> |
| <b>Examples</b>    | <pre># Disable TTL check on VRRP packets. &lt;Sysname&gt; system-view [Sysname] interface vlan-interface 2 [Sysname-Vlan-interface2] vrrp un-check ttl</pre>                                                                             |

---

## vrrp vrid preempt-mode

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <p><b>vrrp vrid</b> <i>virtual-router-id</i> <b>preempt-mode</b> [ <b>timer delay</b> <i>delay-value</i> ]</p> <p><b>undo vrrp vrid</b> <i>virtual-router-id</i> <b>preempt-mode</b> [ <b>timer delay</b> ]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>View</b>        | Interface view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Parameters</b>  | <p><i>virtual-router-id</i>: Virtual router ID or VRRP standby group number, in the range 1 to 255.</p> <p><b>timer delay</b> <i>delay-value</i>: Sets preemption delay. The <i>delay-value</i> argument is in the range of 0 to 255 seconds and defaults to 0 seconds.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <p>Use the <b>vrrp vrid preempt-mode</b> command to enable preemption on the switch and configure its preemption delay in the specified standby group.</p> <p>Use the <b>undo vrrp vrid preempt-mode</b> command to disable preemption on the switch in the specified standby group.</p> <p>Use the <b>undo vrrp vrid preempt-mode timer delay</b> command to restore the default preemption delay, that is, zero seconds.</p> <p>The default mode is immediate preemption without delay.</p> <p>On an instable network, the standby group member in the backup state may not normally receive the packets from the master due to network congestion, resulting in frequent master/backup state transition of the standby group members. Preemption delay is introduced to solve this problem. With a preemption delay set, if the backup does not receive the packet from the master duly, it waits for a period to see whether it can receive any packet from the master. If the specified period elapses but it still receives no packet from the master, it becomes the master.</p> |

Note that before executing the command, you need to create a standby group on an interface and configure the virtual IP address of the standby group.

**Examples** # Enable preemption on the router in VRRP standby group 1, and set the preemption delay to five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

---

## vrrp vrid priority

**Syntax** **vrrp vrid** *virtual-router-id* **priority** *priority-value*

**undo vrrp vrid** *virtual-router-id* **priority**

**View** Interface view

**Parameters** *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

*priority-value*: Priority value of the router in the specified standby group, in the range 1 to 254, with a higher number indicating a higher priority.

**Description** Use the **vrrp vrid priority** command to configure the priority of the switch in the specified standby group.

Use the **undo vrrp vrid priority** command to restore the default.

By default, the priority of a switch in a standby group is 100.

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- In VRRP, the role that a switch plays in a standby group depends on its priority. A higher priority means that the switch is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.
- If the switch is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

**Examples** # Set the priority of standby group 1 on interface VLAN-interface 2 to 150.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 priority 150
```

---

## vrrp vrid timer advertise

**Syntax** **vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval*

**undo vrrp vrid** *virtual-router-id* **timer advertise**



- View** Interface view
- Parameters** *virtual-router-id*: VRRP standby group number, in the range 1 to 255.
- adver-interval*: Interval at which the master in the specified standby group sends VRRP advertisements. It ranges from 1 to 255 seconds.
- Description** Use the **vrrp vrid timer advertise** command to configure the Adver\_Timer of the specified standby group.
- Use the **undo vrrp vrid timer advertise** command to restore the default.
- By default the Adver\_Timer is 1 second.
- The Adver\_Timer controls the interval at which the master sends VRRP packets.
- Note that:
- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
  - Routers in the same VRRP standby group must use the same Adver\_Timer setting.
- Examples** # Set the master in standby group 1 to send VRRP advertisements at intervals of five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

---

## vrrp vrid track

- Syntax** **vrrp vrid** *virtual-router-id* **track interface** *interface-type interface-number* [ **reduced** *priority-reduced* ]
- undo vrrp vrid** *virtual-router-id* **track** [ **interface** *interface-type interface-number* ]
- View** Interface view
- Parameters** *virtual-router-id*: VRRP standby group number, in the range 1 to 255.
- interface** *interface-type interface-number*: Specifies an interface to be tracked by its type and number.
- reduced** *priority-reduced*: Value by which the priority decrements. *priority-reduced* ranges from 1 to 254 and defaults to 10.
- Description** Use the **vrrp vrid track** command to configure to track the specified interface.

Use the **undo vrrp vrid track** command to disable tracking the specified interface.

By default, no interface is being tracked.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- When the switch is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding switch restores its priority automatically.

**Examples** # On interface VLAN-interface 2, set the interface to be tracked as VLAN-interface 1, making the priority of standby group 1 on interface VLAN-interface 2 decrement by 50 when VLAN-interface 1 goes down.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 1 reduced 50
```

---

## vrrp vrid virtual-ip

**Syntax** **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*  
**undo vrrp vrid** *virtual-router-id* [ **virtual-ip** *virtual-address* ]

**View** Interface view

**Parameters** *virtual-router-id*: VRRP standby group number, in the range 1 to 255.  
*virtual-address*: Virtual IP address.

**Description** Use the **vrrp vrid virtual-ip** command to create a standby group the first time that you add a virtual IP address or add a virtual IP address to it after that.

Use the **undo vrrp vrid** *virtual-router-id* command to remove a standby group.

Use the **undo vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address* command to remove a virtual IP address from a standby group.

By default, no standby group is created.

Note that:

- The system removes a standby group after you delete all the virtual IP addresses in it.
- The virtual IP address of the standby group cannot be 0.0.0.0, 255.255.255.255, loopback address, non A/B/C address and other illegal IP addresses such as 0.0.0.1.

- Only when the configured virtual IP address and the interface IP address belong to the same segment and are legal host addresses can the standby group operate normally. If they are not in the same network segment, or the configured IP address is the network address or network broadcast address of the network segment that the interface IP address belongs to, though you can perform the configuration successfully, the state of the standby group is always **Initialize**, that is, VRRP does not take effect in this case.

**Examples** # Create standby group 1 and set its virtual IP address to 10.10.10.10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
```

# Add virtual IP address 10.10.10.11 to standby group 1.

```
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11
```



# 91

## IPv6 VRRP CONFIGURATION COMMANDS

---

### display vrrp ipv6

**Syntax** `display vrrp ipv6 [ verbose ] [ interface interface-type interface-number [ vrid virtual-router-id ] ]`

**View** Any view

**Parameters** **verbose**: Displays detailed state information of VRRP.

**interface interface-type interface-number**: Displays VRRP state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

**vrid virtual-router-id**: Displays state information of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

**Description** Use the **display vrrp ipv6** command to display the state information of VRRP for IPv6.

If you do not specify **verbose**, only the brief state information of VRRP is displayed.

If you specify both interface and standby group, only the state information of the specified standby group is displayed; if you only specify an interface, the state information of all the standby groups on the interface is displayed; if you specify neither, the state information of all the standby groups on the device is displayed.

**Examples** # Display brief information about all VRRP standby groups on the device for IPv6.

```
<Sysname> display vrrp ipv6
IPv6 Standby Information:
Run Method : VIRTUAL-MAC
Virtual IP Ping : Enable
The total number of the virtual routers: 1
Interface VRID State Run Adver. Auth Virtual
 Pri Time Type Type IP

Vlan100 1 Master 100 100 NONE FE80::1
```

# Display detailed information about all standby groups on the device.

```
<Sysname>display vrrp ipv6 verbose
IPv6 Standby Information:
Run Method : VIRTUAL-MAC
```

```

Virtual IP Ping : Enable
Interface : Vlan-interface100
VRID : 1 Adver. Timer : 100
Admin Status : UP State : Master
Config Pri : 100 Run Pri : 100
Preempt Mode : YES Delay Time : 0
Auth Type : NONE
Track IF : Vlan-interface200 Pri Reduced : 10
Virtual IP : FE80::1
Virtual MAC : 0000-5e00-0201
Master IP : FE80::20F:E2FF:FE49:8060

```

**Table 311** Field descriptions of the display vrrp ipv6 command

| Field           | Description                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Run Method      | Current VRRP running mode, real MAC or virtual MAC                                                                                                                |
| Virtual IP Ping | Whether you can ping the virtual IPv6 address                                                                                                                     |
| Interface       | Interface to which the standby group belongs                                                                                                                      |
| VRID            | Number of the standby group                                                                                                                                       |
| Adver. Timer    | VRRP advertisement interval in centiseconds                                                                                                                       |
| Admin Status    | Administrative state: UP or DOWN                                                                                                                                  |
| State           | Status of the switch in the standby group, master, backup, or initialize                                                                                          |
| Config Pri      | Configured priority                                                                                                                                               |
| Run Pri         | Running priority                                                                                                                                                  |
| Preempt Mode    | Preemption mode                                                                                                                                                   |
| Delay Time      | Preemption delay, not displayed when the device works in non-preemption mode.                                                                                     |
| Auth Type       | Authentication type                                                                                                                                               |
| Track IF        | The interface to be tracked. It is displayed only after the execution of the <b>vrrp ipv6 vrid track</b> command.                                                 |
| Pri Reduced     | The priority value that is reduced when the interface being tracked is down. It is displayed only after the execution of the <b>vrrp ipv6 vrid track</b> command. |
| Virtual IP      | Virtual IPv6 addresses of the standby group                                                                                                                       |
| Virtual MAC     | Virtual MAC address corresponding to the virtual IPv6 address of the standby group. It is displayed only when the switch is in the state of master.               |
| Master IP       | Primary IPv6 address of the interface to which the switch in the state of master belongs                                                                          |

## display vrrp ipv6 statistics

**Syntax** **display vrrp ipv6 statistics** [ **interface** *interface-type interface-number* [ **vrid** *virtual-router-id* ] ]

**View** Any view

**Parameters** **interface** *interface-type interface-number*: Displays VRRP statistics information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

**vrid** *virtual-router-id*: Displays statistics information of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

**Description** Use the **display vrrp ipv6 statistics** command to display statistics about VRRP for IPv6.

If you specify both interface and standby group, only the statistics about the specified standby group are displayed; if you only specify an interface, the statistics about all the standby groups on the interface are displayed; if you specify neither, the statistics about all the standby groups on the device are displayed.

**Examples** # Display the statistics about all standby groups for IPv6.

```
<Sysname> display vrrp ipv6 statistics
Interface : Vlan-interface100
VRID : 80
Checksum Errors : 0 Version Errors : 0
Invalid Type Pkts Rcvd : 0 Advertisement Interval Errors : 0
Hop Limit Errors : 0 Auth Failures : 0
Invalid Auth Type : 0 Auth Type Mismatch : 0
Packet Length Errors : 0 Address List Errors : 0
Become Master : 1 Priority Zero Pkts Rcvd : 0
Advertise Rcvd : 0 Priority Zero Pkts Sent : 0
Advertise Sent : 20

Interface : Vlan-interface200
VRID : 10
Checksum Errors : 0 Version Errors : 0
Invalid Type Pkts Rcvd : 0 Advertisement Interval Errors : 0
Hop Limit Errors : 0 Auth Failures : 0
Invalid Auth Type : 0 Auth Type Mismatch : 0
Packet Length Errors : 0 Address List Errors : 0
Become Master : 1 Priority Zero Pkts Rcvd : 0
Advertise Rcvd : 0 Priority Zero Pkts Sent : 0
Advertise Sent : 30

Global statistics
Checksum Errors : 0
Version Errors : 0
VRID Errors : 1439
```

**Table 312** Field descriptions of the display vrrp ipv6 statistics command

| Field                         | Description                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------|
| Interface                     | Interface to which the standby group belongs                                           |
| VRID                          | Number of the standby group                                                            |
| Checksum Errors               | Number of packets with checksum errors                                                 |
| Version Errors                | Number of packets with version errors                                                  |
| Invalid Type Pkts Rcvd        | Number of packets with incorrect packet type                                           |
| Advertisement Interval Errors | Number of packets with advertisement interval errors                                   |
| Hop Limit Errors              | Number of packets with hop limit errors                                                |
| Auth Failures                 | Number of packets with authentication failures                                         |
| Invalid Auth Type             | Number of packets with authentication failures due to invalid authentication types     |
| Auth Type Mismatch            | Number of packets with authentication failures due to mismatching authentication types |
| Packet Length Errors          | Number of packets with VRRP packet length errors                                       |

**Table 312** Field descriptions of the display vrrp ipv6 statistics command

| Field                   | Description                                              |
|-------------------------|----------------------------------------------------------|
| Address List Errors     | Number of packets with virtual IPv6 address list errors  |
| Become Master           | Number of times that the switch worked as the master     |
| Priority Zero Pkts Rcvd | Number of received advertisements with the priority of 0 |
| Advertise Rcvd          | Number of received advertisements                        |
| Advertise Sent          | Number of advertisements sent                            |
| Global statistics       | Statistics about all standby groups                      |
| Checksum Errors         | Total number of packets with checksum errors             |
| Version Errors          | Total number of packets with version errors              |
| VRID Errors             | Total number of packets with VRID errors                 |

---

## reset vrrp ipv6 statistics

**Syntax** **reset vrrp ipv6 statistics** [ **interface** *interface-type interface-number* [ **vrid** *virtual-router-id* ] ]

**View** User view

**Parameters** **interface** *interface-type interface-number*: Clears VRRP statistics of a specific interface. *interface-type interface-number* specifies an interface by its type and number.

**vrid** *virtual-router-id*: Clears VRRP statistics of the specified standby group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

**Description** Use the **reset vrrp ipv6 statistics** command to clear VRRP statistics.

If you specify both the interface and standby group, the statistics about the specified standby group on the specified interface are cleared; if you specify only the interface, the statistics about all the standby groups on the interface are cleared; if you specify neither, the statistics about all the standby groups on the device are cleared.

**Examples** # Clear the statistics about all the standby groups on the device.

```
<Sysname> reset vrrp ipv6 statistics
```

---

## vrrp ipv6 vrid authentication-mode

**Syntax** **vrrp ipv6 vrid** *virtual-router-id* **authentication-mode simple** *key*

**undo vrrp ipv6 vrid** *virtual-router-id* **authentication-mode**

**View** Interface view



- Parameters** *virtual-router-id*: VRRP standby group number, in the range 1 to 255.
- simple**: Sets the authentication mode to plain text authentication.
- key*: Authentication key of 1 to 8 case-sensitive characters in plain text.
- Description** Use the **vrrp ipv6 vrid** *virtual-router-id* **authentication-mode simple** *key* command to configure authentication mode and authentication key for the VRRP standby groups to send and receive VRRP packets.
- Use the **undo vrrp ipv6 vrid** *virtual-router-id* **authentication-mode** command to restore the default.
- By default, authentication is disabled.
- Note that:
- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
  - You may configure different authentication types and authentication keys for the standby groups on an interface. However, the members of the same standby group must use the same authentication mode and authentication key.
- Examples** # Set the authentication mode and authentication key for VRRP standby group 10 on interface VLAN-interface 2 to send and receive VRRP packets.
- ```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 10 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2]vrrp ipv6 vrid 10 authentication-mode simple test
```

vrrp ipv6 method

- Syntax** **vrrp ipv6 method** { **real-mac** | **virtual-mac** }
- undo vrrp ipv6 method**
- View** System view
- Parameters** **real-mac**: Associates the real MAC address of the interface with the virtual IPv6 address of the standby group.
- virtual-mac**: Associates the virtual MAC address of the router with the virtual IPv6 address of the standby group.
- Description** Use the **vrrp ipv6 method** command to set the mappings between the virtual IPv6 addresses and the MAC addresses of the standby groups.
- Use the **undo vrrp ipv6 method** command to restore the default mapping.
- By default, the virtual MAC address of the standby group is associated with the virtual IP address.

Configure the mapping between the virtual IPv6 address and the MAC address before configuring a standby group. Otherwise, your configuration will fail.

Examples # Associate the virtual IP address of the standby group with the real MAC address of the routing interface.

```
<Sysname> system-view
[Sysname] vrrp ipv6 method real-mac
```

vrrp ipv6 ping-enable

Syntax **vrrp ipv6 ping-enable**
undo vrrp ipv6 ping-enable

View System view

Parameters None

Description Use the **vrrp ipv6 ping-enable** command to enable users to ping the virtual IPv6 addresses of standby groups.

Use the **undo vrrp ipv6 ping-enable** command to disable the virtual IPv6 addresses of standby groups from being pinged.

By default, the virtual IP addresses of standby groups can be pinged.

Perform this configuration before configuring a standby group.

Examples # Enable users to ping the virtual IPv6 addresses of standby groups.

```
<Sysname> system-view
[Sysname] vrrp ipv6 ping-enable
```

vrrp ipv6 vrid preempt-mode

Syntax **vrrp ipv6 vrid** *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]
undo vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**timer delay**]

View Interface view

Parameters *virtual-router-id*: Virtual router ID or VRRP standby group number, in the range 1 to 255.

timer delay *delay-value*: Sets preemption delay. The *delay-value* argument is in the range of 0 to 255 seconds and defaults to 0 seconds.

Description Use the **vrrp ipv6 vrid preempt-mode** command to configure preemption on the switch and configure its preemption delay in the specified standby group.

Use the **undo vrrp ipv6 vrid preempt-mode** command to disable preemption on the switch in the specified standby group.

Use the **undo vrrp ipv6 vrid preempt-mode timer delay** command to restore the default preemption delay, that is, zero seconds.

The default mode is immediate preemption without delay.

If you set the router in the standby group to work in non-preemption mode, the delay period changes to zero seconds automatically.

On an instable network, the standby group member in the backup state may not normally receive the packets from the master due to network congestion, resulting in frequent master/backup state transition of the standby group members. Preemption delay is introduced to solve this problem. With a preemption delay set, if the backup does not receive the packet from the master duly, it waits for a period to see whether it can receive any packet from the master. If the specified period elapses but it still receives no packet from the master, it becomes the master.

Note that before executing the command, you need to create a standby group on an interface and configure the virtual IPv6 address of the standby group.

Examples # Enable preemption on the router in VRRP standby group 80 and set the preemption delay to five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 80 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 80 preempt-mode timer delay 5
```

vrrp ipv6 vrid priority

Syntax **vrrp ipv6 vrid** *virtual-router-id* **priority** *priority-value*

undo vrrp ipv6 vrid *virtual-router-id* **priority**

View Interface view

Parameters *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

priority-value: Priority value of the router in the specified standby group, in the range 1 to 254, with a higher number indicating a higher priority.

Description Use the **vrrp ipv6 vrid priority** command to configure the priority of the switch in the specified standby group.

Use the **undo vrrp ipv6 vrid priority** command to restore the default.

By default, the priority of a switch in a standby group is 100.

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- In VRRP, the role that a switch plays in a standby group depends on its priority. A higher priority means that the switch is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.
- If the switch is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

Examples # Set the priority of standby group 1 on interface VLAN-interface 2 to 150.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 priority 150
```

vrrp ipv6 vrid timer advertise

Syntax **vrrp ipv6 vrid** *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp ipv6 vrid *virtual-router-id* **timer advertise**

View Interface view

Parameters *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

adver-interval: Interval at which the master in the specified standby group sends VRRP advertisements. It ranges from 100 to 4095 centiseconds.

Description Use the **vrrp ipv6 vrid timer advertise** command to configure the Adver_Timer of the specified standby group.

Use the **undo vrrp ipv6 vrid timer advertise** command to restore the default.

By default the Adver_Timer is 100 centiseconds.

The Adver_Timer controls the interval at which the master sends VRRP packets.

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- Routers in the same VRRP standby group must use the same Adver_Timer setting.

Examples # Set the master in standby group 1 to send VRRP advertisements at intervals of 500 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500
```

vrrp ipv6 vrid track

Syntax **vrrp ipv6 vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]

undo vrrp ipv6 vrid *virtual-router-id* **track** [**interface** *interface-type interface-number*]

View Interface view

Parameters *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

interface *interface-type interface-number*: Specifies an interface by its type and number.

reduced *priority-reduced*: Value by which the priority decrements. *priority-reduced* ranges from 1 to 254 and defaults to 10.

Description Use the **vrrp ipv6 vrid track** command to configure to track the specified interface.

Use the **undo vrrp ipv6 vrid track** command to disable tracking the specified interface.

By default, no interface is being tracked.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- When the switch is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding switch restores its priority automatically.

Examples # On interface VLAN-interface 2, set the interface to be tracked as VLAN-interface 1, making the priority of standby group 1 on interface VLAN-interface 2 decrement by 50 when VLAN-interface 1 goes down.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-interface 1 reduced 50
```

vrrp ipv6 vrid virtual-ip

Syntax **vrrp ipv6 vrid** *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**]

undo vrrp ipv6 vrid *virtual-router-id* [**virtual-ip** *virtual-address* [**link-local**]]

View Interface view

Parameters *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

virtual-address: Virtual IPv6 address.

link-local: Indicates that the virtual IPv6 address of the standby group is a link local address.

Description Use the **vrrp ipv6 vrid virtual-ip link-local** command to create a standby group and assign the first virtual IPv6 address to the specified standby group. The first virtual IPv6 address assigned to a standby group must be a link local address and only one such address is allowed in a standby group.

Use the **vrrp ipv6 vrid virtual-ip** command to add a virtual IPv6 address to a standby group.

Use the **undo vrrp ipv6 vrid** command to remove a standby group.

Use the **undo vrrp ipv6 vrid virtual-router-id virtual-ip virtual-address [link-local]** command to remove a virtual IPv6 address from a standby group.

After you remove all virtual IPv6 addresses, the standby group is automatically removed. Note that the first address assigned to the group must be removed the last.

By default, no standby group is created.

Examples # Create standby group 1, and configure its virtual IPv6 address as fe80::10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10
```

Configure the virtual IPv6 address of standby group 1 as 1::10.

```
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

92

REDUNDANCY CONFIGURATION COMMANDS

display switchover state

Syntax `display switchover state [slot-id]`

View Any view

Parameters *slot-id*: Slot ID of the active main module (AMB) or standby main module (SMB).

Description Use the **display switchover state** command to display the switchover state. The switchover state of the corresponding module will be displayed if slot number is specified. The switchover state of the AMB will be displayed if no slot number is specified.

Examples # Display the switchover state on the AMB.

```
<Sysname> display switchover state  
HA FSM State(master): Slave is absent.
```

Table 313 Field descriptions of the display switchover state command

Field	Description
Slave is absent	The SMB is not in the slot.
Waiting batch backup request from slave	Waiting for the backup requests from the SMB
Batch backup	Backup state
Realtime and routine backup to slave	Real-time or routine backup state

ha slave-ignore-version-check

Syntax `ha slave-ignore-version-check`
`undo ha slave-ignore-version-check`

View System view

Parameters None

Description Use the **ha slave-ignore-version-check** command to ignore version check of the AMB and SMB, meaning not to check the version of the AMB and SMB.

Use the **undo ha slave-ignore-version-check** command to enable version check of the AMB and SMB.

By default, version check of the AMB and SMB is enabled.

Note that inconsistency of the software version of the AMB and SMB may result in system failure when the system is running.

Examples # Ignore version check of the AMB and SMB.

```
<Sysname> system-view
[Sysname] ha slave-ignore-version-check
```

slave auto-update config

Syntax **slave auto-update config**

undo slave auto-update config

View System view

Parameters None

Description Use the **slave auto-update config** command to enable automatic synchronization of the configuration file on the AMB and SMB.

Use the **undo slave auto-update config** command to disable automatic synchronization of the configuration file on the AMB and SMB.

By default, automatic synchronization of the configuration file on the AMB and SMB is enabled.

Examples # Enable automatic synchronization of the configuration file on the AMB and SMB.

```
<Sysname> system-view
[Sysname] slave auto-update config
```

slave restart

Syntax **slave restart**

View System view

Parameters None

Description Use the **slave restart** command to manually configure the SMB to restart.

When the backup system program operates abnormally and needs to be reloaded, you can manually restart the SMB.

Examples # Restart the SMB.

```
<Sysname> system-view
[Sysname] slave restart
The slave will reset! Continue?[Y/N]:y
```

slave switchover

Syntax **slave switchover**

View System view

Parameters None

Description Use the **slave switchover** command to manually configure the switchover between the AMB and SMB.

Related commands: **slave switchover { enable | disable }.**

Examples # Manually configure the switchover between the AMB and the SMB.

```
<Sysname> system-view
[Sysname] slave switchover
Caution!!! Confirm switch slave to master?[Y/N] y
Starting.....
RAM Line...OK
```

slave switchover { enable | disable }

Syntax **slave switchover { enable | disable }**

View System view

Parameters **enable:** Enables manual configuration of the switchover between AMB and SMB.
disable: Disables manual configuration of the switchover between AMB and SMB.

Description Use the **slave switchover { enable | disable }** command to configure manual switchover function between AMB and SMB.

By default, manual configuration of the switchover between AMB and SMB is enabled.

Related commands: **slave switchover.**

Examples # Enable manual configuration of the switchover between AMB and SMB.

```
<Sysname> system-view
[Sysname] slave switchover enable
```


93

RRPP CONFIGURATION COMMANDS

control-vlan

Syntax `control-vlan vlan-id`

View RRPP domain view

Parameters *vlan-id*: Control VLAN ID, in the range 2 to 4093.

Description Use the **control-vlan** command to specify a control VLAN for an RRPP domain.

Note that:

- The control VLAN must be a new one.
- You can configure a control VLAN for the primary ring. However, the control VLAN of a subring is assigned automatically by the system and its VLAN ID is the control VLAN ID of the primary ring plus 1. So, you should select two consecutive new VLANs. Otherwise, the configuration fails.
- Each RRPP domain has its own control VLAN which is deleted while you delete the RRPP domain. You cannot use the **undo vlan all** command to delete a control VLAN.
- You cannot specify a control VLAN as a remotely mirrored VLAN or isolate-user-vlan.
- Do not enable QinQ or VLAN mapping on the control VLAN. Otherwise, RRPPDU protocol packets cannot be forwarded properly.

Related commands: **rrpp domain**.

Examples # Configure the control VLAN of RRPP domain 1 as VLAN 100.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
```

display rrpp brief

Syntax `display rrpp brief`

View Any view

Parameters None

Description Use the **display rrpp brief** command to display the brief information of RRPP configuration.

Examples # Display the brief information of RRPP configuration.

```
<Sysname> display rrpp brief
Flags for Node Mode :
M -- Master , T -- Transit , E -- Edge , A -- Assistant-Edge

RRPP Protocol Status: Enable
Number of RRPP Domains: 2

Domain ID      : 1
Control VLAN   : Major 5      Sub 6
Hello Timer    : 1 sec  Fail Timer : 3 sec
Ring ID        : 1          Ring Level : 1
Node Mode      : M          Primary/Common Port : GigabitEthernet3/0/1
Secondary/Edge Port : GigabitEthernet3/0/2
Enable Status  : Yes

Domain ID      : 2
Control VLAN   : Major 10     Sub 11
Hello Timer    : 1 sec  Fail Timer : 3 sec
Ring ID        : 1          Ring Level : 0
Node Mode      : M          Primary/Common Port : GigabitEthernet3/0/3
Secondary/Edge Port : GigabitEthernet3/0/4
Enable Status  : Yes
```

Table 314 Field descriptions of the display rrpp brief command

Field	Description
Flags for Node Mode	RRPP node mode: M represents master node, T represents transit node, E represents edge node and A represents assistant edge node
RRPP Protocol Status	RRPP protocol status: Enable (globally enabled)/Disable (globally disabled)
Number of RRPP Domains	Number of RRPP domains configured
Domain ID	RRPP domain ID
Control VLAN	Control VLANs of an RRPP domain: Major and Sub
Hello Timer	Hello Timer value configured in seconds
Fail Timer	Fail Timer value configured in seconds
Ring ID	RRPP ring ID
Ring Level	RRPP ring level, with 0 representing primary ring and 1 representing subring
Node Mode	Node mode
Primary/Common Port	Primary port when the node mode is master node or transit node; common port when the node mode is edge node or assistant edge node; "-" appears when the port is not configured on the ring or the module to which the port belongs does not start.
Secondary/Edge Port	Secondary port when the node mode is master node or transit node; edge port when the node mode is edge node or assistant edge node; "-" appears when the port is not configured on the ring or the module to which the port belongs does not start.
Enable Status	RRPP ring status: Yes indicates enabled and No indicates disabled.

display rrpp statistics

Syntax **display rrpp statistics domain** *domain-id* [**ring** *ring-id*]

View Any view

Parameters *domain-id*: RRPP domain ID, in the range 1 to 8.

ring-id: RRPP ring ID, in the range 1 to 64.

Description Use the **display rrpp statistics** command to display RRPP message statistics.

Note that:

- If you have specified an RRPP ring ID in the command, RRPP message statistics of the specified RRPP ring in the specified RRPP domain on the current device appears. Otherwise, RRPP message statistics of all RRPP rings in the specified RRPP domain appears.
- If some port belongs to more than one ring, its packets are taken statistics based on the rings. You will view the statistics of the port under the current ring.
- When a ring transits from inactive status into active status, its packets will be taken statistics again.

Related commands: **reset rrpp statistics.**

Examples # Display RRPP message statistics of ring 1 in RRPP domain 1.

```
<Sysname> display rrpp statistics domain 1 ring 1
Ring ID      : 1
Ring Level   : 1
Node Mode    : Master
Active Status : Yes
Primary port  : GigabitEthernet3/0/1
Packet      Link      Common      Complete      Packet
Direct Health Down      Flush FDB    Flush FDB     Total
-----
Send 16424    0          0            1             16425
Rcv  0         0          0            0             0
Secondary port: GigabitEthernet3/0/2
Packet      Link      Common      Complete      Packet
Direct Health Down      Flush FDB    Flush FDB     Total
-----
Send 0        0          0            0             0
Rcv  16378    0          0            1             16379
```

Display RRPP message statistics of RRPP domain 2.

```
<Sysname> display rrpp statistics domain 2
Ring ID      : 1
Ring Level   : 0
Node Mode    : Master
Active Status : Yes
Primary port  : GigabitEthernet3/0/3
Packet      Link      Common      Complete      Packet
Direct Health Down      Flush FDB    Flush FDB     Total
```

```

-----
Send  16924    0    0    1    16925
Rcv   0        0    0    0    0
Secondary port: GigabitEthernet3/0/4
Packet      Link      Common      Complete      Packet
Direct Health  Down      Flush FDB  Flush FDB  Total
-----
Send  0        0    0    0    0
Rcv   16878    0    0    1    16879

Ring ID      : 2
Ring Level   : 1
Node Mode    : Edge
Active Status : No
Common port  : GigabitEthernet3/0/3
Packet      Link      Common      Complete      Packet
Direct Health  Down      Flush FDB  Flush FDB  Total
-----
Send  0        0    0    0    0
Rcv   0        0    0    0    0
Edge port    : GigabitEthernet3/0/5
Packet      Link      Common      Complete      Packet
Direct Health  Down      Flush FDB  Flush FDB  Total
-----
Send  0        0    0    0    0
Rcv   0        0    0    0    0

```

Table 315 Field descriptions of the display rrpp statistics command

Field	Description
Ring ID	RRPP ring ID
Ring Level	RRPP ring level: 0 for primary ring and 1 for subring
Node Mode	Node mode: master node, transit node, edge node and assistant edge node
Active Status	RRPP ring activation status: Yes indicates active and No indicates inactive (An RRPP is active only if the RRPP ring is enabled and the RRPP protocol is globally enabled)
Primary Port	The primary port field means the node mode is master node or transit node. "-" appears when the port is not configured on the ring, and in this case, no corresponding statistics appears.
Secondary Port	The secondary port field means the node mode is master node or transit node. "-" appears when the port is not configured on the ring, and in this case, no corresponding statistics appears.
Common Port	The common port field means the node mode is edge node or assistant edge node. "-" appears when the port is not configured on the ring, and in this case, no corresponding statistics appears.
Edge Port	The edge port field means the node mode is edge node or assistant edge node. "-" appears when the port is not configured on the ring, and in this case, no corresponding statistics appears.
Packet Direct	Packet transmission direction on the port: Send or Rcv
Health	Health packet statistics received/sent on the port
Link-Down	Link-Down packet statistics received/sent on the port
Common Flush FDB	Common-Flush-FDB packet statistics received/sent on the port
Complete Flush FDB	Complete-Flush-FDB packet statistics received/sent on the port
Packet Total	Total number of packets received/sent on the port. Here only Health, Link-Down, Common-Flush-FDB and Complete-Flush-FDB packets of RRPP are taken statistics.

display rrpp verbose

Syntax **display rrpp verbose domain** *domain-id* [**ring** *ring-id*]

View Any view

Parameters *domain-id*: RRPP domain ID, in the range 1 to 8.
ring-id: RRPP ring ID, in the range 1 to 64.

Description Use the **display rrpp verbose** command to display detailed information about RRPP configuration.

If you have specified an RRPP ring ID in the command, the detailed information of the specified ring in the specified RRPP domain appears. Otherwise, the detailed information of all the rings in the specified RRPP domain appears.

Examples # Display the detailed information of ring 1 in RRPP domain 1.

```
<Sysname> display rrpp verbose domain 1 ring 1
Domain ID      : 1
Control VLAN   : Major 5      Sub 6
Hello Timer    : 1 sec  Fail Timer : 3 sec

Ring ID        : 1
Ring Level     : 1
Node Mode      : Master
Ring State     : Complete
Enable Status  : Yes      Active Status: Yes
Primary port   : GigabitEthernet3/0/1      Port status: UP
Secondary port : GigabitEthernet3/0/2      Port status: BLOCKED
```

Display the detailed information of all the rings in RRPP domain 2.

```
<Sysname> display rrpp verbose domain 2
Domain ID      : 2
Control VLAN   : Major 10     Sub 11
Hello Timer    : 1 sec  Fail Timer : 3 sec

Ring ID        : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Enable Status  : Yes      Active Status: Yes
Primary port   : GigabitEthernet3/0/4      Port status: UP
Secondary port : GigabitEthernet3/0/5      Port status: BLOCKED

Ring ID        : 2
Ring Level     : 1
Node Mode      : Edge
Ring State     : -
Enable Status  : No      Active Status: No
Common port    : GigabitEthernet3/0/4      Port status: -
Edge port      : GigabitEthernet3/0/3      Port status: -
```

Table 316 Field descriptions of the display rrpp verbose command

Field	Description
Domain ID	RRPP domain ID
Control VLAN	Control VLANs of the RRPP domain, including major control VLAN and sub control VLAN
Hello Timer	Hello Timer value configured in seconds
Fail Timer	Fail Timer value configured in seconds
Ring ID	RRPP ring ID
Ring Level	RRPP ring level, with 0 representing primary ring and 1 representing subring
Node Mode	Node mode: master node, transit node, edge node and assistant edge node
Ring State	RRPP ring state. This field makes a sense only when the node mode field is master node. "Complete" appears when the ring is in health state; "Failed" appears when the ring is in disconnect state; and "-" appears in all the other cases.
Enable Status	RRPP ring enable status: Yes indicates enabled and No indicates disabled
Active Status	RRPP ring activation status: Yes indicates active and No indicates inactive The current ring is active only when the RRPP protocol and the RRPP ring are enabled simultaneously. Through this field, you can get to know the enable status of the RRPP protocol.
Primary Port	The primary port field means the node mode is master node or transit node. "-" appears when the port is not configured on the ring or the module to which the port belongs does not start.
Secondary Port	The secondary port field means the node mode is master node or transit node. "-" appears when the port is not configured on the ring or the module to which the port belongs does not start.
Common Port	The common port field means the node mode is edge node or assistant edge node. "-" appears when the port is not configured on the ring or the module to which the port belongs does not start.
Edge Port	The edge port field means the node mode is edge node or assistant edge node. "-" appears when the port is not configured on the ring or the module to which the port belongs does not start.
Port status	Port status includes down, up and blocked; "-" appears in one of the following cases: <ul style="list-style-type: none"> ■ the ring is inactive ■ the port is not configured on the ring ■ the module to which the port belongs does not start

reset rrpp statistics

Syntax `reset rrpp statistics domain domain-id [ring ring-id]`

View User view

Parameters *domain-id*: RRPP domain ID, in the range 1 to 8.

ring-id: RRPP ring ID, in the range 1 to 64.

Description Use the **reset rrpp statistics** command to clear RRPP message statistics.

If you have specified an RRPP ring ID in the command, RRPP message statistics of the specified RRPP ring in the specified RRPP domain on the current device is cleared. Otherwise, RRPP message statistics of all RRPP rings in the specified RRPP domain is cleared.

Related commands: **display rrpp statistics.**

Examples # Clear the RRPP message statistics of ring 10 in RRPP domain 10.
 <Sysname> reset rrpp statistics domain 1 ring 10

ring

Syntax **ring** *ring-id* **node-mode** { { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value* | { **edge** | **assistant-edge** } [**common-port** *interface-type interface-number*] [**edge-port** *interface-type interface-number*] }

undo ring *ring-id*

View RRPP domain view

Parameters *ring-id*: RRPP ring ID, in the range 1 to 64.

master: Specifies the device as the master node of the RRPP ring.

transit: Specifies the device as the transit node of the RRPP ring.

primary-port: Specifies the port as a primary port.

secondary-port: Specifies the port as a secondary port.

interface-type interface-number: Port type and port number.

level-value: RRPP ring level, with 0 representing primary ring and 1 representing subring.

edge: Specifies the device as the edge node of the RRPP ring.

assistant-edge: Specifies the device as the assistant edge node of the RRPP ring.

common-port: Specifies the port as a common port.

edge-port: Specifies the port as an edge port.

Description Use the **ring** command to configure the node mode of the device and the role of the port accessing the RRPP ring.

Use the **undo ring** command to remove the configuration.

The ports accessing the RRPP ring must conform to the following conditions:

- Trunk port;
- Layer 2 Ethernet port or layer 2 GE port;
- Except for aggregation port and loopback port;
- Port with STP, 802.1x, MAC address authentication, voice VLAN disabled;

Note that:

- RRPP ports cannot be configured if the RRPP ring is enabled.
- You must first configure control the VLAN before configuring the RRPP ring.
- You must first configure the primary ring and then the subring when configuring an RRPP domain. A Ring ID cannot be applied to more than one RRPP ring in the same RRPP domain.
- If a device resides on multiple RRPP rings in an RRPP domain, only one primary ring exists within these rings. The device plays a role of either edge node or assistant edge node on other subrings.
- Modifying the node mode, port mode and ring level of an RRPP ring is prohibited after configuration. If needed, you must first delete the existing configuration.
- The common port must be on the primary ring in the domain when you configure the edge node and the assistant edge node.
- You must configure the primary ring and then subrings when you configure the edge node and the assistant edge node.
- Moreover, you must remove all subring configurations before deleting the primary ring configuration of the edge node and the assistant edge node. However, the enabled RRPP ring cannot be deleted.

Related command: **control-vlan** and **ring enable**.

Examples # Specify the device as the master node of primary ring 10 in RRPP domain 1, GigabitEthernet 3/0/1 as the primary port and GigabitEthernet 3/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port gigabit
ethernet3/0/1 secondary-port gigabitethernet 3/0/2 level 0
```

Specify the device as the transit node of primary ring 10 in RRPP domain 1, GigabitEthernet 3/0/1 as the primary port and GigabitEthernet 3/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port gigabi
tethernet 3/0/1 secondary-port gigabitethernet 3/0/2 level 0
```

Specify the device as the master node of subring 20 in RRPP domain 1, GigabitEthernet 3/0/1 as the primary port and GigabitEthernet 3/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] ring 20 node-mode master primary-port gigabit
ethernet 3/0/1 secondary-port gigabitethernet 3/0/2 level 1
```

Specify the device as the transit node of primary ring 20 in RRPP domain 1, GigabitEthernet 3/0/1 as the primary port and GigabitEthernet 3/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] ring 20 node-mode transit primary-port gigabi
tethernet 3/0/1 secondary-port gigabitethernet 3/0/2 level 1
```

Specify the device as the edge node of primary ring 20 in RRPP domain 1, GigabitEthernet 3/0/1 as the common port and GigabitEthernet 3/0/2 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] ring 20 node-mode edge common-port gigabiteth
ernet 3/0/1 edge-port gigabitethernet 3/0/2
```

Specify the device as the assistant edge node of primary ring 20 in RRPP domain 1, GigabitEthernet 3/0/1 as the common port and GigabitEthernet 3/0/2 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] ring 20 node-mode assistant-edge common-port
gigabitethernet 3/0/1 edge-port gigabitethernet 3/0/2
```

ring enable

Syntax **ring** *ring-id* **enable**

undo ring *ring-id* **enable**

View RRPP domain view

Parameters *ring-id*: RRPP ring ID, in the range 1 to 64.

Description Use the **ring enable** command to enable the RRPP ring.

Use the **undo ring enable** command to disable the RRPP ring.

By default, the RRPP ring is disabled.

Note that:

- To enable subrings, you must first enable the primary ring before enabling subrings.

- You must first disable all the subrings in the RRPP domain and then disable the primary ring.
- To activate the RRPP domain, RRPP protocol and the RRPP ring must be enabled simultaneously.

Related commands: **rrpp enable.**

Examples # Enable RRPP ring 10 in RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] ring 10 enable
```

rrpp domain

Syntax **rrpp domain** *domain-id*
undo rrpp domain *domain-id*

View System view

Parameters *domain-id*: RRPP domain ID, in the range 1 to 8.

Description Use the **rrpp domain** command to create an RRPP domain and enter its view.
Use the **undo rrpp domain** command to remove an RRPP domain.

Note that:

- When you delete an RRPP domain, the control VLAN of it will be deleted at the same time.
- When you delete an RRPP domain, you must ensure it has no RRPP ring.
- The data VLAN in one domain must be isolated from the data VLAN in another.

Related commands: **control-vlan, ring, ring enable, rrpp enable, timer.**

Examples # Create RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
Info: Create a new domain.
[Sysname-rrpp-domain1]
```

rrpp enable

Syntax **rrpp enable**
undo rrpp enable

View	System view
Parameters	None
Description	<p>Use the rrpp enable command to enable RRPP protocol.</p> <p>Use the undo rrpp enable command to disable RRPP protocol.</p> <p>By default, RRPP protocol is disabled.</p> <p>To activate the RRPP domain, RRPP protocol and the RRPP ring must be enabled simultaneously.</p>
Related commands:	ring enable.
Examples	<pre># Enable RRPP protocol <Sysname> system-view [Sysname] rrpp enable</pre>

timer

Syntax	timer hello-timer <i>hello-value</i> fail-timer <i>fail-value</i>
	undo timer
View	RRPP domain view
Parameters	<p><i>hello-value</i>: Hello timer value, in the range 1 to 10 seconds.</p> <p><i>fail-value</i>: Fail timer value, in the range 3 to 30 seconds.</p>
Description	<p>Use the timer command to specify the value of the timers of the RRPP domain.</p> <p>Use the undo timer command to restore it to the default value.</p> <p>By default, the Hello timer value is 1 second and the Fail timer value is 3 seconds.</p> <p>Note that the Fail timer value must be greater than or equal to three times of the Hello timer value.</p>
Examples	<pre># Set the Hello timer value to 2 seconds and the Fail timer value to 7 seconds. <Sysname> system-view [Sysname] rrpp domain 1 [Sysname-rrpp-domain1] timer hello-timer 2 fail-timer 7</pre>

