NIKOMAX
Network solutions

Basic Configuration Commands
L3

Chapter 1 System Management Commands 1
Configuring File Management Commands 1
copy 1
delete 2
dir 3
ip address 3
ip route 4
show configuration 5
format 5
more 6
Basic System Management Commands 6
boot flash 7
cd 8
date 9
debug job 10
english 10
md 11
pwd 11
rd 12
rename 12
reboot 13
alias 14
boot system flash 15
help 16
history 16
show 18
show job 19
show break 21
Chapter 2 Terminal Service Configuration Command 22
Telnet Configuration Command 22
telnet 22
ip telnet 24
ctrl-shift-6+x (the current connection is mounted) 26
where 27
resume 28
disconnect 30
clear telnet 31
show telnet 32
debug telnet 32
Terminal Configuration Command 33
attach-port 34
autocommand 35
clear line 35
connect 35
disconnect 36
exec-timeout 37
length 37
line 38
location 38
login authentication 39
monitor 39
no debug all 39
password 40
resume 41
show debug 41
show line 42

terminal length....42
terminal monitor....43
terminal width....43
terminal-type....44
where....45
width....45
Chapter 3 Maintenance and Debugging Tool Commands....47
Network Testing Tool Commands....47
ping....47
traceroute....50
Fault Diagnosis Commands....52
logging....52
logging buffered....53
logging console....55
logging facility....56
logging monitor....58
logging on....59
logging trap....61
logging command....62
logging source-interface....63
logging history alerts....63
logging history critical....64
logging history debugging....64
logging history emergencies....65
logging history errors....65
logging history informational....66
logging history notifications....66
logging history warnings....67
logging history rate-limit....67
logging history size....68
service timestamps....69
clear logging....70
show break....70
show debug....72
show logging....72
Chapter 4 SSH Configuration Commands....74
ip sshd enable....74
ip sshd timeout....74
ip sshd auth-method....75
ip sshd access-class....76
ip sshd auth-retries....77
ip sshd clear....77
ip sshd silence-period....78
ip sshd sftp....79
ip sshd save....79
ip sshd disable-aes....80
ssh....81
show ssh....82
show ip sshd....83
Chapter 5 Network Management Configuration Commands....84
SNMP Commands....84
snmp-server community....85
snmp-server contact....86
snmp-server group....87
snmp-server [host|hostv6]....88
snmp-server location....90
snmp-server packetsize....91

snmp-server queue-length 91
snmp-server trap-source 92
snmp-server trap-timeout 93
snmp-server user 94
snmp-server view 95
snmp-server source-addr 96
snmp-server udp-port 97
snmp-server encryption 98
snmp-server trap-add-hostname 99
snmp-server trap-logs 99
Chapter 6 AAA Authentication Configuration Commands 101
AAA Authentication Configuration Commands 101
aaa authentication enable default 101
aaa authentication login 102
aaa authentication password-prompt 104
aaa authentication username-prompt 105
aaa group server 106
debug aaa authentication 107
enable password 108
server 109
service password-encryption 110
username 111
Chapter 7 RADIUS Configuration Commands 113
RADIUS Configuration Commands 113
debug radius 113
ip radius source-interface 114
radius-server challenge-noecho 115
radius-server deadtime 116
radius-server host 117
radius-server optional-passwords 118
radius-server key 118
radius-server retransmit 119
radius-server timeout 120
radius-server vsa send 121
Chapter 8 WEB Configuration Commands 123
ip http language 123
ip http port 123
ip http secure-port 124
ip http server 124
ip http http-access enable 124
ip http ssl-access enable 125
ip http web max-vlan 125
ip http web igmp-groups 125
show ip http 126
Chapter 9 Interface Configuration Commands 127
Interface Configuration Commands 127
interface 127
description 128
bandwidth 129
delay 129
shutdown 130
show interface 131
show running-config interface 132
Configuration Example 133
Chapter 10 Interface Range Command 135
Interface Range 135
Chapter 11 Interface Physical Characteristic Configuration Commands 136

Interface Physical Characteristic Configuration Commands 136
speed 136
duplex 137
flow control 137
Chapter 12 Port Additional Characteristics Configuration Commands 139
Port Security 139
switchport port-security mode static 139
switchport port-security mode dynamic 139
switchport port-security static mac-address 139
switchport port-security dynamic maximum 139
Port Protection 140
switchport protected 140
Port Storm Control 141
storm-control 141
Rate Limitation 142
switchport rate-limit 142
Chapter 13 Configuring Port Mirroring Commands 143
Port Mirroring Configuration Commands 143
mirror 143
show mirror 143
Chapter 14 Power Over Ethernet Configuration Commands 145
POE Configuration Commands 145
show poe system 145
show poe all 146
show poe power 147
show poe interface 149
poe power-management 150
poe led-time 152
poe mib notification-stop 153
poe pse-unprotect 153
poe counter value 154
poe threshold 155
poe standard 155
poe disable 156
poe max-power 157
poe priority 158
poe PD-discription 159
poe force-power 160
Chapter 15 MAC Address Configuration Commands 161
MAC Address Configuration Commands 161
mac address-table static 161
mac address-table aging-time 161
show mac address-table 162
clear mac address-table 163
Chapter 16 MAC Address Table Characteristics Configuration Commands 165
MAC Address Table Characteristic Configuration Commands 165
mac address-table static 165
show mac address-table 165
clear mac address-table 166
Chapter 17 802.1x Configuration Commands 168
802.1x Configuration Commands 168
dot1x enable 169
dot1x port-control 169
dot1x multiple-hosts 171
dot1x default 172
dot1x max-req 172

dot1x reauth-max 173
dot1x re-authentication 174
dot1x timeout quiet-period 175
dot1x timeout re-authperiod 176
dot1x timeout tx-period 176
dot1x user-permit 177
dot1x authentication method 178
dot1x accounting enable 179
dot1x accounting method 180
dot1x authen-type、dot1x authentication type 180
dot1x guest-vlan 181
dot1x guest-vlan id 182
dot1x forbid multi-network-adapter 183
aaa authentication dot1x 184
debug dot1x error 185
debug dot1x state 185
debug dot1x packet 186
show dot1x 186
Chapter 18 VLAN Configuration Commands 188
VLAN Configuration Commands 188
vlan 188
name 189
switchport pvid 190
switchport mode 190
switchport trunk 191
double-tagging 193
show vlan 194
interface supervlan 195
sub vlan 196
Chapter 19 GVRP Configuration Commands 198
GVRP Configuration Commands 198
gvrp 198
show gvrp statistics 199
show gvrp status 199
debug gvrp event 200
debug gvrp packet 201
GARP Configuration Commands 201
garp timer 201
garp leaveall 202
show garp timer 203
show garp status 204
debug garp event 204
Chapter 20 Private VLAN Configuration Commands 206
Private VLAN Configuration Commands 208
private-vlan 206
private-vlan association 207
switchport mode private-vlan 208
switchport private-vlan host-association 209
switchport private-vlan mapping 209
switchport private-vlan 210
show vlan private-vlan 211
show vlan private-vlan interface 211
Chapter 21 STP Configuration Commands 213
SSTP Configuration Commands 213
spanning-tree mode 213
spanning-tree sstp priority 214
spanning-tree sstp hello-time 214

spanning-tree sstp max-age....215
spanning-tree sstp forward-time....216
spanning-tree sstp cost....217
spanning-tree cost....218
spanning-tree sstp port-priority....219
spanning-tree port-priority....220
show spanning-tree....221
RSTP Configuration Commands....222
spanning-tree mode rstp....222
spanning-tree rstp forward-time....222
spanning-tree rstp hello-time....223
spanning-tree rstp max-age....224
spanning-tree rstp priority....225
spanning-tree rstp cost....225
spanning-tree rstp port-priority....226
Chapter 22 MSTP Configuration Commands....228
MSTP Configuration Command....228
spanning-tree mode mstp....228
spanning-tree mstp name....229
spanning-tree mstp revision....229
spanning-tree mstp instance....230
spanning-tree mstp root....231
spanning-tree mstp priority....232
spanning-tree mstp hello-time....233
spanning-tree mstp forward-time....234
spanning-tree mstp max-age....234
spanning-tree mstp diameter....235
spanning-tree mstp max-hops....236
spanning-tree mstp port-priority....236
spanning-tree mstp cost....237
spanning-tree mstp point-to-point....238
spanning-tree mstp mst-compatible....239
spanning-tree mstp migration-check....239
show spanning-tree mstp....240
show spanning-tree mstp region....241
show spanning-tree mstp detail....242
show spanning-tree mstp interface....244
Chapter 23 STP Optional Characteristic Configuration Commands....247
STP Optional Characteristic Configuration Commands....247
spanning-tree portfast....247
spanning-tree bpduguard....248
spanning-tree bpdufilter....249
spanning-tree uplinkfast....250
spanning-tree backbonefast....250
spanning-tree guard....251
spanning-tree loopguard....252
Chapter 24 Link Aggregation Configuration Commands....254
Link Aggregation Configuration Commands....254
aggregator-group....254
aggregator-group load-balance....255
show aggregator-port....256
show interface port-aggregator....257
debug lacp errors....258
debug lacp state....259
debug lacp packet....260
Chapter 25 PDP Configuration Commands....261
PDP Configuration Commands....261

pdp timer 261
pdp holdtime 262
pdp version 262
pdp run 263
pdp enable 263
show pdp traffic 264
show pdp neighbor 265
Chapter 26 LLDP Configuration Commands 266
LLDP Commands 266
lldp run 266
lldp holdtime 267
lldp timer 267
lldp reinit 268
lldp tlv-select 269
lldp transmit 270
lldp receive 271
Show lldp errors 271
Show lldp interface 272
show lldp neighbors 273
Show lldp neighbors detail 274
Show lldp traffic 276
clear lldp counters 277
clear lldp table 278
debug lldp errors 278
debug lldp events 279
debug lldp packets 280
debug lldp states 281
Chapter 27 FlexLinkLite Configuration Commands 282
FlexLinkLite Commands 282
Setting the Backup Port 282
Setting the Preempt Mode of a Backup Port 283
Setting the Transmission and Reception of TCN Packets 284
Browsing the State of the Port Backup Group 285
Chapter 28 BackupLink Configuration Commands 287
Global Commands 287
backup-link-group id 287
backup-link-group id preemption-mode forced {delay value} 288
backup-link-group id preemption-mode bandwidth {delay value} 288
monitor-link-group id 289
Port Configuration Commands 290
backup-link-group id active 290
backup-link-group id backup 291
share-load vlan vlanmap 292
backup-link-group mmu transmit 293
backup-link-group mmu receive 294
monitor-link-group id uplink 294
monitor-link-group id downlink 295
Show 296
show backup-link-group id 296
show monitor-link-group id 297
Chapter 29 EAPS Configuration Commands 299
Global Commands 299
ether-ring 299
control-vlan 299
master-node 300
transit-node 301
hello-time 302

fail-time....303
pre-forward-time....304
Port Configuration Commands....305
ether-ring primary-port....305
ether-ring secondary-port....306
ether-ring transit-port....307
Show....308
show ether-ring....308
Chapter 30 MEAPS Configuration Commands....310
Global Commands....310
mether-ring id1 domain id2....310
master-node....311
transit-node....312
edge-node....313
assistant-node....314
major-ring....315
sub-ring....316
control-vlan....317
single-subring-mode....318
hello-time....318
fail-time....319
pre-forward-time....320
Port Configuration Commands....321
mether-ring id1 domain id2 primary-port....321
mether-ring id1 domain id2 secondary-port....322
mether-ring id1 domain id2 transit-port....323
mether-ring id1 domain id2 common-port....324
mether-ring id1 domain id2 edge-port....325
Show....326
show mether-ring....326
Chapter 31 ELPS Configuration Commands....328
Global Commands....328
elps id....328
working-vlanmap vlanmap....329
protection-mode {1plus1-bidirectional | 1plus1-unidirectional | 1to1-bidirectional}....329
revertive-mode {revertive | nonrevertive}....331
detect-fault {physical-port-check| continuity-check | both-check}....332
WTR-time....333
hold-off-time....333
Port Configuration Commands....334
elps id {working-transport | protection-transport}....334
elps id mep md md-string ma ma-string level level-id local local-id remote remote-id....336
Control Commands....337
elps id LockOut....337
elps id ForcedSwitch....338
elps id ManualSwitch....338
elps id ManualSwitch-Working....339
elps id Exercise....340
elps id CLEAR....341
Show....342
show elps....342
Chapter 32 UDLD Configuration Commands....344
UDLD Configuration Commands....344
udld enable....344
udld aggressive....345

udld port 346
udld port aggressive 346
udld message 347
udld reset 348
show udld 349
Chapter 33 IGMP-SNOOPING Configuration Commands 352
igmp-snooping 352
igmp-snooping static 353
igmp-snooping immediate-leave 354
igmp-snooping dlf-frames 354
igmp-snooping router age 355
igmp-snooping response time 356
igmp-snooping querier 356
show ip igmp-snooping 357
show ip igmp-snooping timer 358
show ip igmp-snooping groups 358
show ip igmp-snooping statistics 359
debug ip igmp-snooping packet 360
debug ip igmp-snooping timer 360
Chapter 34 IGMP Proxy Commands 362
ip igmp-proxy enable 362
ip igmp-proxy agent-vlan client-vlan map 363
ip igmp-proxy source svlan sport 363
show ip igmp-proxy mcache 364
show ip igmp-proxy 365
debug ip igmp-proxy 366
Chapter 35 MLD Multicast Configuration Commands 368
ipv6 mld-snooping {enable | disable} 368
ipv6 mld-snooping solicitation 369
ipv6 mld-snooping vlan vlan_id static X:X:X:X::X interface intf 370
ipv6 mld-snooping timer router-age timer_value 370
ipv6 mld-snooping timer response-time timer_value 371
ipv6 mld-snooping vlan vlan_id mrouter interface inft_name 372
ipv6 mld-snooping vlan vlan_id immediate-leave 372
show ipv6 mld-snooping 373
show ipv6 mld-snooping timer 374
show ipv6 mld-snooping groups 375
show ipv6 mld-snooping statistics 376
show ipv6 mld-snooping mac 377
Chapter 36 OAM Configuration Commands 378
OAM Configuration Commands 378
ethernet oam 378
ethernet oam {max-rate | min-rate | mode | timeout } 379
ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action 380
ethernet oam remote-loopback {supported | timeout} 381
ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high 382
ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low 383
ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window 384
ethernet oam link-monitor high-threshold action 385
ethernet oam link-monitor negotiation-supported 386
ethernet oam remote-loopback {start | stop} 387
clear ethernet oam statistics 387
show ethernet oam discovery 388
show ethernet oam statistics {pdu | link-monitor | remote-failure} 390

show ethernet oam configuration 391
show ethernet oam runtime....392
debug ethernet oam remote-loopback 394
debug ethernet oam packet {tx | rx} 394
debug ethernet oam discovery-sm....395
debug ethernet oam error....395
Chapter 37 CFM and Y1731 Configuration Commands 397
CFM Configuration Commands....397
Adding the Maintenance Domain and Entering the Maintenance Domain Mode 397
Deleting the Maintenance Domain 398
Browsing the Maintenance Domain....399
Adding a Maintenance Association 399
Deleting the Maintenance Association 400
Browsing the Maintenance Association....401
Adding MIP....402
Deleting MIP....403
Browsing MIP 404
Adding MEP 405
Deleting MEP 406
Browsing MEP....407
Y1731 Configuration Commands 409
Modifying the Transmission Interval of the AIS Frame....409
Performing the Termination Command 410
CFM Maintenance Commands....410
loopback....410
linktrace....411
Deleting the Linktrace Result Table 413
Setting the Size of the Linktrace Result Table 414
Setting the Number of Entries in the Linktrace Result Table....414
Setting the Aging Time of the Linktrace Result Table 415
Deleting the MEP Statistics Data 416
Conducting the Loss Measurement Command 417
Disabling the Loss Measurement Command 418
Enabling the Delay Measurement Command....419
Disabling the Delay Measurement Command....420
CFM Control Commands....421
CFM Stack Control Command 421
CFM Interface Control Command 421
MIP Control Command....422
MEP Control Command 423
CC Control Command....423
CFM Query Commands 424
Browsing the CFM Protocol Stack....424
Browsing the CFM Interface....425
Browsing the Locally Stored Information About the Remote MEP 425
Browsing the LinkTrace Result Table....426
Browsing the Whole Running Status of CFM 428
Y1731 Show Commands....428
Displaying the MEPs That Can Transmit AIS Frames 428
Displaying the Information About Continuous MEG Detection....429
Displaying MEP and MIP Configurations on a Port....430
Displaying the Configuration of all MEG or the Detailed Configuration of a Certain MEG....430
Displaying the Information About All Configured MIPs....431
Displaying the Statistics Information About the Y1731 Module....432

Y1731 Clear Command....433
Deleting the Transmission Statistics Information About the OAM Packets and the System Error Information....433
Chapter 38 DHCP-Relay Snooping Configuration Commands....434
dhcp-relay snooping....434
dhcp-relay snooping vlan....435
dhcp-relay snooping database-agent....436
dhcp-relay snooping db-file....436
dhcp-relay snooping write....437
dhcp-relay snooping information option....438
ip verify source vlan....438
ip arp inspection vlan....439
ip source binding....440
arp inspection trust....440
dhcp snooping trust....441
dhcp snooping deny....442
ip-source trust....442
dhcp-relay agent (L2 switch)....443
dhcp-relay snooping helper-address (L2 switch)....443
show ip dhcp-relay snooping....444
show ip dhcp-relay snooping binding....445
debug ip dhcp-relay snooping....445
debug ip dhcp-relay event....446
debug ip dhcp-relay binding....447
Chapter 39 MACFF Configuration Commands....448
macff enable....448
macff vlan vlan_id enable....449
macff vlan vlan_id default-ar A.B.C.D....449
macff vlan vlan_id enable other_ar A.B.C.D....450
macff disable....451
debug macff....451
Chapter 40 IEEE1588 Transparent Clock Configuration Commands....453
IEEE1588 Transparent Clock Configuration Commands....453
ptp enable (global)....453
ptp enable (port)....454
ptp start....455
ptp delay-mechanism....456
ptp sync-mechanism....457
ptp domain....459
ptp domain-filter....459
ptp pdelay-interval....460
ptp e2e-record-timeout....461
debug p2p....462
show ptp....463
Chapter 41 Layer 2 Protocol Tunneling Configuration Commands....465
Layer 2 Protocol Tunneling Configuration Commands....465
Layer-2 protocol-tunnel....465
Layer 2 Protocol Tunneling Monitor Commands....465
debug layer-2 protocol-tunnel....465
Chapter 42 Loopback Detection Configuration Commands....467
Loopback Detection Configuration Commands....467
loopback-detection....467
loopback-detection enable....468
loopback-detection vlan-control....468
loopback-detection hello-time....469
loopback-detection recovery-time....469
loopback-detection control....470

loopback-detection dest-mac 471
loopback-detection existence 471
show loopback-detection 472
show loopback-detection 473
Chapter 43 QoS Service Configuration Commands 474
QoS Configuration Commands 474
cos default 474
cos map 475
scheduler wrr bandwidth 475
scheduler policy 476
Chapter 44 DoS Attack Prevention Configuration Commands 478
DoS-Attack Prevention Configuration Commands 478
dos enable 478
show dos 479
Chapter 45 Anti-Attack Configuration Commands 481
Anti-Attack Configuration Commands 481
filter period time 481
filter threshold value 481
filter block-time value 482
filter igmp 483
filter arp 483
filter enable 483
show filter 484
Chapter 46 IP Addressing Configuration Commands 485
IP Addressing Configuration Commands 485
arp 485
arp timeout 486
clear arp-cache 487
ip address 488
ip directed-broadcast 489
ip forward-protocol udp 490
ip helper-address 491
ip proxy-arp 492
ip unnumbered 493
keepalive 494
show arp 495
show ip hosts 496
show ip interface 496
Chapter 47 NAT Configuration Commands 499
NAT Configuration Commands 499
ip nat 499
ip nat local-service 501
ip fastaccess 501
ip fastnat 1to1 502
ip nat inside destination 503
ip nat inside source 504
ip nat outside source 507
ip nat pool 509
ip nat service 510
ip nat translation 511
clear ip nat statistics 513
clear ip nat translation 514
show ip nat statistics 515
show ip nat translations 517
debug ip nat 519
Chapter 48 DHCP Client Configuration Command 522
DHCP Client Configuration Command 522

ip address dhcp 522
ip dhcp client 523
ip dhcp-server 524
show dhcp lease 525
show dhcp server 527
debug dhcp 527
Chapter 49 DHCP Server Configuration Commands 529
DHCP Server Configuration Commands 529
ip dhcpd ping packet 529
ip dhcpd ping timeout 530
ip dhcpd write-time 530
ip dhcpd database-agent 531
ip dhcp snooping arp 532
ip dhcpd pool 532
ip dhcpd enable 533
DHCP Address Pool Configuration Commands 534
network 534
range 535
default-router 535
dns-server 536
domain-name 537
lease 537
netbios-name-server 538
ip-bind 539
ip-bind ip-addr hardware-address 539
ip-bind ip-addr client-identifier 540
ip-bind ip-addr client-name 541
DHCP Debugging Commands 541
debug ip dhcpd packet 541
debug ip dhcpd event 542
show ip dhcpd statistic 543
show ip dhcpd binding 543
show ip dhcpd pool 544
clear ip dhcpd statistic 545
clear ip dhcpd binding 545
clear ip dhcpd abandoned 546
Chapter 50 IP Configuration Commands 547
IP Server Configuration Commands 547
clear tcp 548
clear tcp statistics 549
debug arp 550
debug ip icmp 551
debug ip packet 554
debug ip raw 559
debug ip rtp 560
debug ip tcp packet 564
debug ip tcp transactions 565
debug ip udp 568
ip mask-reply 569
ip mtu 569
ip redirects 570
ip route-cache 571
ip source-route 573
ip tcp synwait-time 573
ip tcp window-size 574
ip unreachables 575

show ip cache....576
show ip irdp....577
show ip sockets....578
show ip traffic....578
show tcp....580
show tcp brief....584
show tcp statistics....585
show tcp tcb....587
ACL Configuration Commands....588
deny....589
ip access-group....592
ip access-list....594
permit....595
show ip access-list....598
Chapter 51 IP ACL Application Commands....600
Configuration Commands for Applying IP ACL....600
ip access-group....600
ipv6 access-group....601
Chapter 52 RIP Configuration Commands....604
RIP Configuration Commands....604
auto-summary....605
default-information originate....606
default-metric....606
ip rip authentication....607
ip rip message-digest-key....608
ip rip passive....609
ip rip password....610
ip rip receive version....611
ip rip send version....612
ip rip split-horizon....613
neighbor....614
network....615
offset....616
router rip....617
timers expire....618
timers holddown....619
timers update....620
validate-update-source....621
version....622
distance....623
filter....623
maximum-count....625
show ip rip....626
show ip rip database....627
show ip rip protocol....628
debug ip rip database....629
debug ip rip protocol....630
Chapter 53 BEIGRP Configuration Commands....632
BEIGRP Configuration Commands....632
auto-summary....633
clear ip beigrp neighbors....634
debug ip beigrp....635
debug ip beigrp fsm....635
debug ip beigrp neighbors....636
debug ip beigrp packet....637
debug ip beigrp transmit....638
default-metric....639

distance 640
filter 642
beigrp log-neighbor-changes 643
beigrp router-id 643
ip beigrp bandwidth-percent 644
ip beigrp hello-interval 645
ip beigrp hold-time 646
ip beigrp passive 646
ip beigrp split-horizon 647
ip beigrp summary-address 648
metric weights 649
network 651
offset 652
redistribute 653
router beigrp 654
show ip beigrp interface 655
show ip beigrp neighbors 655
show ip beigrp protocol 657
show ip beigrp topology 658
show ip beigrp traffic 659
Chapter 54 OSPF Configuration Commands 661
OSPF Configuration Commands 661
area authentication 662
area default-cost 663
area range 665
area stub 666
area virtual-link 668
debug ip ospf adj 670
debug ip ospf events 671
debug ip ospf flood 672
debug ip ospf lsa-generation 673
debug ip ospf packet 674
debug ip ospf retransmission 675
debug ip ospf spf 675
debug ip ospf tree 677
default-information originate (OSPF) 678
default-metric 679
distance ospf 680
filter 682
ip ospf cost 683
ip ospf dead-interval 683
ip ospf hello-interval 684
ip ospf message-digest-key 685
ip ospf network 687
ip ospf passive 688
ip ospf password 689
ip ospf priority 689
ip ospf retransmit-interval 690
neighbor 691
network area 693
redistribute 694
router ospf 695
show ip ospf 696
show ip ospf border-routers 697
show ip ospf database 698
show ip ospf interface 700

show ip ospf neighbor 701
show ip ospf virtual-link 702
summary-address....704
timers delay....705
timers hold....705
Chapter 55 BGP Configuration Commands 707
aggregate-address 708
bgp always-compare-med 710
bgp bestpath med....711
bgp client-to-client reflection....712
bgp cluster-id....713
bgp confederation identifier 714
bgp confederation peers....716
bgp dampening....717
bgp default....718
bgp deterministic-med 719
bgp redistribute-internal....720
clear ip bgp....721
debug chat....723
debug dialer....724
debug ip bgp....725
distance 726
filter....727
neighbor default-originate....729
neighbor description 730
neighbor distribute-list 731
neighbor ebgp-multihop....732
neighbor filter-list 733
neighbor maximum-prefix....734
neighbor next-hop-self....735
neighbor password 737
neighbor prefix-list 738
neighbor remote-as 739
neighbor route-map 740
neighbor route-reflector-client 742
neighbor route-refresh....743
neighbor send-community 744
neighbor shutdown 745
neighbor soft-reconfiguration....746
neighbor timers....747
neighbor update-source 748
neighbor weight 750
network (BGP)....751
redistribute(BGP)....752
router bgp 753
show ip bgp 754
show ip bgp community....756
show ip bgp neighbors 757
show ip bgp paths 758
show ip bgp prefix-list....759
show ip bgp regexp 760
show ip bgp summary 760
synchronization 762
table-map 763
timers....763
Chapter 56 IP Hardware Subnet Routing Configuration Commands....765

ip exf....765
ip exf down-up-threshold....765
debug ip exf....766
Chapter 57 IP-PBR Configuration Commands....768
ip pbr....768
show ip pbr....768
show ip pbr policy....769
show ip pbr exf....770
debug ip pbr....771
Chapter 58 VRRP Configuration Commands....772
VRRP Configuration Commands....772
vrrp associate....772
vrrp description....773
vrrp priority....774
vrrp preempt....774
vrrp track....775
vrrp authentication....776
vrrp timers....777
show vrrp....778
debug vrrp....779
Chapter 59 Basic Multicast Commands....780
Basic Multicast Commands....780
debug ip mpacket....780
debug ip mrouting....781
debug ip mroute-cache....782
debug ip multicast....782
ip mroute....784
ip mroute-cache....785
ip multicast-routing....785
ip multicast route-limit....786
ip multicast boundary....787
ip multicast helper-map....788
ip multicast rate-limit....790
ip multicast ttl-threshold....791
show ip mflow....792
show ip mroute-cache....793
show ip mroute mfc....794
Chapter 60 IGMP Configuration Commands....796
IGMP Configuration Commands....796
clear ip igmp group....796
debug ip igmp....797
debug ip igmp-host....797
ip igmp helper-address....798
ip igmp join-group....799
ip igmp immediate-leave group-list....800
ip igmp last-member-query-interval....801
ip igmp querier-timeout....801
ip igmp query-interval....802
ip igmp query-max-response-time....803
ip igmp static-group....804
ip igmp version....805
show ip igmp groups....806
show ip igmp interface....807
show ip igmp-host....808
Chapter 61 PIM-DM Configuration Commands....810
PIM-DM Configuration Commands....810
clear ip mroute pim-dm....810

clear ip pim-dm interface 811
debug ip pim-dm....812
ip pim-dm....814
ip pim-dm dr-priority 815
ip pim-dm hello-interval 816
ip pim-dm state-refresh origination-interval 817
ip pim-dm neighor-filter....818
ip pim-dm state-refresh disable 819
show ip mroute pim-dm 820
show ip pim-dm neighbor 821
show ip pim-dm interface 822
show ip rpf pim-dm 824
Chapter 62 PIM-SM Configuration Commands 825
PIM-SM Configuration Commands....825
ip pim-sm....825
ip pim-sm admin-scope 825
ip pim-sm asrt-hold....827
ip pim-sm bsr-border 828
ip pim-sm dr-pri 828
ip pim-sm hello-intvl....829
ip pim-sm holdtime 830
ip pim-sm horizon-split 831
ip pim-sm jp-hold 832
ip pim-sm jp-intvl 833
ip pim-sm lan-delay 834
ip pim-sm nbma-mode....835
ip pim-sm nbr-filter....836
ip pim-sm nbr-track....837
ip pim-sm override....838
router pim-sm 839
hello-option....840
accept bsm-adv 841
accept crp-adv....842
accept rp-addr 843
accept register....845
anycast-rp....846
reg-rate-limit 849
reg-src 850
spt-threshold....851
ssm....852
c-bsr intf_type intf_name 854
c-bsr admin-scope....855
bsm-policy 856
static-rp....858
c-rp intf_type intf_name....860
intvl-time 862
holdtime....863
log....865
show running-configure 866
show ip pim-sm bsr-router....867
show ip pim-sm interface....868
show ip pim-sm neighbor 868
show ip pim-sm rp 869
show ip pim-sm rp-hash 870
show ip mroute pim-sm 871
show ip rpf pim-sm 872

debug ip pim-sm alert....873
debug ip pim-sm assert....874
debug ip pim-sm bsr....874
debug ip pim-sm rp....875
debug ip pim-sm entry....876
debug ip pim-sm event....876
debug ip pim-sm hello....877
debug ip pim-sm jp....878
debug ip pim-sm nbr....878
debug ip pim-sm packet....879
debug ip pim-sm register....880
debug ip pim-sm timer....880
Chapter 63 Multicast VPN Settings....882
Ip multicast-routing vrf vpn-instance-name....882
mdt share-group group-address binding mtunnel number....883
mdt connect-src interface....884
mdt switch-group-pool group-address group-mask threshold....884
mdt mdt switch-delay....885
mdt hold-down....886
mdt rd-list....887
show ip mroute vrf vpn-instance pim-s jointlv....888
debug ip pim-s mvpn....888
debug ip multicast mvpn....889
Chapter 64 IPv6 Configuration Commands....891
IPv6 Configuration Commands....891
ipv6 address....891
ipv6 address anycast....892
ipv6 address autoconfig....893
ipv6 address eui-64....893
ipv6 address link-local....894
ipv6 enable....895
show ipv6 interface....896
Chapter 65 IPv6 Configuration Commands....899
IPv6 Configuration Commands....899
clear ipv6 traffic....899
debug ipv6 packet....900
ipv6 cur-hoplimit....901
ipv6 general-prefix....902
ipv6 icmp-ratelimit....903
ipv6 mtu....903
ipv6 redirects....904
ipv6 source-route....905
ipv6 traffic-filter....906
ipv6 unreachables....907
show ipv6 general-prefix....908
show ipv6 pmtu....909
show ipv6 traffic....910
Chapter 66 ND Commands....912
debug ipv6 nd....912
show ipv6 neighbors....913
clear ipv6 neighbors....914
ipv6 neighbor....914
ipv6 nd dad attempts....915
ipv6 nd managed-flag....916
ipv6 nd ns-interval....916
ipv6 nd other-flag....917
ipv6 nd prefix....918

Ipv6 nd ra-interval-range 919
ipv6 nd ra-interval....920
ipv6 nd ra-lifetime 921
ipv6 nd reachable-time 921
ipv6 nd router-preference 922
ipv6 nd suppress-ra....923
Chapter 67 Ripng Commands 924
aggregate-address 924
debug ipv6 rip....924
default-information....925
default-metric....926
connect-metric....927
distance 927
filter....928
ipv6 rip enable 929
ipv6 rip passive....930
ipv6 rip poision-reverse 931
ipv6 rip split-horizon 932
router ripng 932
max-path 933
neighbor 934
offset....934
port 935
redistribute....936
show ipv6 rip 937
timers....938
Chapter 68 OSPFv3 Configuration Commands 939
OSPFv3 Configuration Commands....939
area default-cost....940
area nssa....941
area range....943
area stub 944
area virtual-link....945
debug ipv6 ospf....947
debug ipv6 ospf events 948
debug ipv6 ospf ifsm 950
debug ipv6 ospf lsa 952
debug ipv6 ospf nfsm 954
debug ipv6 ospf nsm 956
debug ipv6 ospf packet 957
debug ipv6 ospf route....959
default-information originate....961
default-metric....962
filter....963
ipv6 ospf area....964
ipv6 ospf cost 965
ipv6 ospf database-filter all out....965
ipv6 ospf dead-interval 966
ipv6 ospf hello-interval....967
ipv6 ospf mtu-ignore....968
ipv6 ospf neighbor....969
ipv6 ospf network 970
ipv6 ospf priority 971
ipv6 ospf retransmit-interval 972
ipv6 ospf transmit-delay 973
passive-interface 974

redistribute....974
router ospfv3....975
router-id....976
show ipv6 ospf....977
show ipv6 ospf database....978
show ipv6 ospf interface....980
show ipv6 ospf neighbor....981
show ipv6 ospf route....982
show ipv6 ospf virtual-link....984
summary-prefix....985
timers delay....986
timers hold....987
Chapter 69 BFD Configuration Commands....989
bfd init-mode....989
bfd slow-timers....990
bfd demand enable....991
bfd echo enable....992
bfd enable....993
bfd neighbor....994
bfd min_echo_rx_interval....995
bfd authentication-mode....996
show bfd....997
Chapter 70 SNTP Configuration Commands....998
SNTP Configuration Commands....998
sntp master....998
sntp query-interval....999
sntp server....1000
sntp peer....1000
sntp source....1001
sntp authenticate....1002
sntp authentication-key....1002
sntp trusted-key....1003
show sntp....1004
debug sntp....1005
time-zone....1005
time-range....1006
absolute....1007
periodic....1007
Chapter 71 Cluster Management Configuration Commands....1009
Cluster Management Configuration Comamdns....1009
cluster address-pool....1009
cluster mode....1010
cluster commander-address....1011
cluster member....1012
cluster discovery hop-count....1013
cluster hello-time....1013
cluster hold-time....1014
show cluster....1015
show cluster candidate....1017
show cluster member....1018
show cluster topo....1020
show cluster address pool....1021

Chapter 1 System Management Commands

1.1 Configuring File Management Commands

- copy
- delete
- dir
- ip address
- ip route
- show configuration
- format
- more

1.1.1 copy

To read a file from the tftp server to a switch, use the **copy** command.
copy tftp<*:filename*> {**flash**<*:filename*>|**rom**} [*ip_addr*]

Parameter

Parameter	Description
tftp<:filename>	Read a file from the tftp server. Filename indicates the relevant filename. If not specified the filename, the system will prompt user to input the filename after executing the copy command.
flash <:filename>	Write a file to the flash memory of the switch. Filename indicates the relevant filename. If not specified the filename, the system will prompt user to input the filename after executing the copy command.
rom	Updates bootrom for the switch.
ip_addr	Specifies the IP address of tftp srever. If not specified, the system will prompt user to input the IP address after executing the copy command.

Default

None

Command mode

monitor mode

Instrution

None

Example

monitor#copy tftp:switch.bin flash:switch.bin 192.2.2.1

The example shows how to read the switch.bin from the tftp server to the flash memory of the switch:

Related commands

None

1.1.2 delete

To delete a file, use the **delete** command.

delete *file-name*

Parameter

Parameter	Description
file-name	Specifies the filename (maximum 20 characters)

Default

If not specified the file-name, the system will delete startup-config by default.

Command mode

monitor mode

Instruction

None

Related commands

None

1.1.3 dir

To display filename, use the **dir** command.

dir *file-name*

Parameter

Parameter	Description
file-name	Specifies the filename (maximum 20 characters)

Default

None

Command mode

monitor mode

Instruction

None

Related commands

None

1.1.4 ip address

To set an IP address for an Ethernet interface, use the **ip address** command.
ip address *ip-address mask*

Parameter

Parameter	Description
ip-address	IP address
mask	IP network mask

Default

None

Command mode

monitor mode

Instruction

None

Example

monitor#ip address 192.168.1.1 255.255.255.0

Related commands

ip route
ping

1.1.5 ip route

To specify a default gateway, use the **ip route** default command.
ip route default gw_ip_addr

Parameter

Parameter	Description
gw_ip_addr	Default gateway address

Default

None

Command mode

Monitor mode

Instrution

None

Example

monitor#ip route default 192.168.1.3

Related commands

ip address

1.1.6 show configuration

To display the running configuration file, use the **show configuration** command.
show configuration

Parameter

None

Default

None

Command mode

monitor mode

Instrution

None

Related commands

None

1.1.7 format

To format file system, use the **format** command.
format

Parameter

None

Default

None

Command mode

EXEC

Instrution

All files in the file system will de deleted after executing the format command.

Related commands

None

1.1.8 more

To display the contents of a file, use the **more** command.
more *file-name*

Parameter

Parameter	Description
file-name	Specifies the name of a file (maximum 20 characters)

Default

None

Command mode

EXEC

Instrution

If all files are displayable characters, they will be displayed in ASCII format, or they will be displayed binary format.

Related commands

None

1.2 Basic System Management Commands

- bootflash
- cd
- chinese
- english
- chram
- date
- debub job
- md
- pwd
- rd
- rename

- reboot
- show break
- show memory
- alias
- boot system flash
- help
- history
- job
- jobd
- show alias
- show job

1.2.1 boot flash

To enable the system from the specified file in monitor mode, use the **boot flash** command.
boot flash *filename*

Parameter

Parameter	Description
filename	Specified file name.

Default

None

Command mode

monitor mode

Command mode

Use the boot flash command to enable the device after user entering the monitor mode.

Example

monitor#boot flash switch.bin

Related commands

None

1.2.2 cd

To change the current directory, use the **cd** command.

cd *directory*|..

Parameter:

Parameter	Description
directory	Name of the directory. (maximum 20 characters)
..	Upper directory.

Default

None

Command mode

Monitor mode

Command mode

None

Example

monitor#cd my_dir

Related commands

pwd

1.2.3 chinese

To switch command prompt to chinese mode, use the **chinese** command.

Parameter

None

Default

None

Command mode

monitor mode

Command mode

None

Example

None

Related commands

None

1.2.4 date

To set the absolute time, use the **date** command.

Parameter

None

Default

None

Command mode

Monitor mode

Command mode

This command is used to set the abslute time for the system. For the switch with a battery-powered clock, the clock will be powered by the battery. If the clock doesn't keep good time, you need to change the battery.

For the swich without a battery-powered clock, the system date is configured to July 1st, 1970 after the reboot of the switch, and user needs to set the current time each time when starting the switch.

Example

monitor#date

The current date is 2000-7-27 21:17:24

Enter the new date(yyyy-mm-dd):2000-7-27

Enter the new time(hh:mm:ss):21:17:00

Related commands

1.2.5 debug job

To track the debug condition of the job, run **debug job**.

Parameter

None

Command mode

EXEC

Instrution

Output the debug and execution condition of the job after turn on the debug switch of the job.

Example

config#debug job

JOB: <showver> fired

JOB: job <showver>, cmd "show ver" is parsing

Related commands

job

jobd

show job

1.2.6 english

To switch the command prompt to english mode, use the **english** command.

Parameter

None

Default

None

Command mode

monitor

Instruction

None

Example

None

Related commands

None

1.2.7 md

md *directory*

Parameter

Parameter	Description
directory	Name of directory (maximum 20 characters)

Default

None

Command mode

monitor

Instruction

To set a directory, use the **md** command

Related commands

None

1.2.8 pwd

Parameter

None

Default

None

Command mode

monitor mode

Instruction

To display the current directory, use the **pwd** command

Related commands

None

1.2.9 rd

rd *directory*

Parameter

Parameter	Description
directory	Name of the directory(maximum 20 characters)

Default

None

Command mode

monitor mode

Instruction

The system prompts if the directory is not empty. The system prompts if the directory doesn't exist. To delete a command, use the rd command.

Related commands

None

1.2.10 rename

To rename a file in a file system, use the **rename** command.

rename *old_file_name* *new_file_name*

Parameter

Parameter	Description
old_file_name	The original filename.
new_file_name	The new filename.

Default

None

Command mode

monitor mode

Instruction

None

Related commands

None

1.2.11 reboot

To reboot a switch, use the **reboot** command.

Parameter

None

Default

None

Command mode

monitor mode

Instruction

None

Related commands

None

1.2.12 alias

[no] history [+ <*count*> | - <*count*> | clear]

Parameter

Parameter	Description
+ <count>	To display the count<1-20> historial command from the beginning to the end
- <count>	To display the count<1-20> historial command from the end to the beginning

Default

If there are no more than 20 commands executed, all historical command lines will be displayed from the beginning to the end. If there are more than 20 commands executed, all historical command lines will be displayed from the beginning to the end.

Comand mode

Random command mode

Explanation

The modularized switch can save up to 20 historical commands. You can invoke these commands with the "up" or “down” key or directly use it after edition. The command is used to browse the **history** command. You can run the **[no] history** command to delete the **history** command.

Example

The following example shows the latest five historical commands from the end to the beginning:

switch#history - 5

config

int e0/1

no ip addr

ip addr 192.2.2.49 255.255.255.0

exit

Related command

None

1.2.13 boot system flash

Run the **boot system flash** command to specify the systematic mirroring files when the system is started up. Run the **no boot system flash** command to delete the previous configuration.

boot system flash *filename*

no boot system flash *filename*

Parameter

Parameter	Description
filename	It is the specified filename, which contains no more than 20 characters.

Default

None

Command mode

Global configuration mode

Instruction

If you have not configured the command, the system will execute the first systematic mirroring file in the flash file system. If you have configured multiple commands, the system will execute the mirroring files one by one. If the file does not exist or the check sum is wrong, the system will execute the next file. If both fail, the system will run at the monitoring state.

Example

config#boot system flash switch.bin

Related command

None

1.2.14 help

help

Parameter

None

Default

None

Command mode

Management mode

Instruction

The command is used to display the help system of the switch.

Example

After you enter the command, the help system of the switch is displayed.

switch# help

Help may be requested at any point in a command by entering a question mark '?',If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g.'show ?') and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'interface e?'.)

Related command

None

1.2.15 history

The command is used to check the historical commands. Run the **[no] history** command to delete the historical commands.

[no] history [+ <*count*> | - <*count*> | clear]

Parameter

Parameter	Description
+ <count>	Displays the count<1-20> historial command from the beginning to the end.
- <count>	Displays the count<1-20> historial command from the end to the beginning.

Default

If there are no more than 20 commands executed, all historical command lines will be displayed from the beginning to the end. If there are more than 20 commands executed, all historical command lines will be displayed from the beginning to the end.

Command mode

Abandom command mode

Instruction

The modularized switch can save up to 20 historical commands. You can invoke these commands with the "up" or “down” key or directly use it after edition.

Example

The following example shows the latest five commands from the end to the beginning:

```
switch#history - 5
config
int e1/1
no ip addr
ip addr 192.2.2.49 255.255.255.0
exit
```

Related command

N/A

1.1.1 show

To display the relevant information of the system, which or specific ones of which can be filtered through the filter, run the following command:

show <sub-command> [| <begin | include | exclude | redirect> <*WORD*> [*SEPARATOR WORD*]]

Parameter

Parameter	Description
sub-command	Stands for a child command.
|	Uses the output filter.
begin	Means to show the result of the **show** command starting with a specific word.
include	Means to show the sentences of the result of the **show** command containing a specific word.
exclude	Means not to show the lines of the result of the **show** command containing a specific word.
redirect	Redirects the result of the **show** command to the file in the designated file system.
WORD	Stands for a designated word, which is the designated filename as to the **redirect** command.
SEPARATOR WORD	Stands for the designated separator, which is space by default to separate the words.

Default value

N/A

Command mode

the EXEC mode or the configuration mode

Explanation

This command can be used to filter the useless information in the

result of the **show** command, especially when the result is too much to read. For example, if you want to browse a designated MAC address in an MAC address table, which contains a lot of MAC addresses, this command will give you convenience for you.

Example

The following example shows how to display the lines, in which the word “interface” is contained, in the result of **show running-config**.

```
Switch#show running-config | include interface
Building configuration...


Current configuration:
!
interface GigaEthernet0/1
interface GigaEthernet0/2
interface GigaEthernet0/3
interface GigaEthernet0/4
interface GigaEthernet0/5
interface GigaEthernet0/6
interface GigaEthernet0/7
interface GigaEthernet0/8
```

Related command

N/A

1.2.16 show job

It is used to display the parameters of the job and the information about job execution:
show job {*paramter* | *status*}

Parameter

Parameter	Description
paramter	Displays the parameters of the job.
status	Displays the execution state of the job.

Default

None

Command mode

Management mode or configuration mode

Instruction

Run the **show job** command to browse the defined parameters and the dynamic execution state of the job.

Example

The following example shows how to display the parameters of the job:

```
switch_config#show job parameter
<showver> fires interval, first at 5, re-fires per 5 secs, on error stop
          will do "show ver"
```

The following example shows how to display the dynamic execution state of the job:

```
Jobd disabled at 245218 seconds
 Name:     job's name
 Type:     None - Not scheduled, interval - Fire interval, one-shot - Fire once
 Status: null - Not scheduled, idle - To fire first
           started - Fired ever, to fire again, stopped - Can't fire
 First:    first time to fire
 Last:     last time of firing or restarting
 Next-due: next time to fire(after now)
 Times:    times fired ever
 Cause:    auto - Automatic, error - Error meeting, command - By command
                          Job's status and statistics
                          ==========================
Name        Type        State       First       Last        Next-due   Times       Cause
                  ---------------------------------------------------------------------------
showver     interval    idle        5           *           *           2           auto
                  ---------------------------------------------------------------------------
Total 1 jobs, 0 null, 1 idle, 0 started, 0 stopped
```

Related command

debug job
job
jobd

1.2.17 show break

It is used to display the abnormal information of the system. The system stores all abnormal information in the latest running. The abnormal information contains the times of abnormity, the stack content and the invoked functions when abnormity occurs.

Parameter

None

Default

None

Command mode

Monitoring state

Instruction

The command is only used for debugging.

Related command

None

Chapter 2 Terminal Service Configuration Command

2.1 Telnet Configuration Command

The chapter describes telnet and related commands. The **telnet** command is used to establish a session with the remote server. The **telnet** command is always working at the UNIX operating systems. Option negotiation is required. Telnet does not provide itself the login authentication. Telnet is different from Rlogin because telnet does not provide itself password check.

The following are telnet configuration commands:

- telnet
- ip telnet
- where
- disconnect
- resume
- switchkey
- switchmsg
- sequence-char
- clear Telnet
- show Telnet
- debug Telnet

2.1.1 telnet

The following is a command sentence for establishing a telnet session:

telnet *server-ip-addr/server-host-name* [**/port** *port*][**/source-interface** *interface*] [**/local** *local-ip-addr*] [**/debug**][**echo/noecho**] [**/script** *scriptname*]

Parameter

Parameter	Description
server-ip-addr	Dotted-decimal IP address of the remote server
server-host-name	Name of the remote server, which is configured by the **ip host** command

port	Telnet port of the remote server
interface	Local interface where the telnet connection is originated
local-ip-addr	Local IP address where the telnet connection is originated
/debug	A negotiation process for openning the debug at the client side and printing the connection
echo/noecho	Enable or disable the local echo. The default value is **noecho**.
scriptname	A script name used for auto login

Default

The default port number is 23. The interface has no default number.

Command mode

Management mode

Instruction

You can use one of the following command lines to establish a remote login.

telnet server-ip-addr/server-host-name

In this case, the application program directly sends the telnet login request to port 23 of the remote server. The local IP address is the IP address which is nearest to the peer and found by the routing table.

telnet server-ip-addr/server-host-name /port port

In this case, the application program sends a telnet login request to the port of the peer.

telnet server-ip-addr/server-host-name /source-interface interface

In this case, the application program uses the IP address on the interface ass the local IP address.

telnet server-ip-addr/server-host-name /debug

In this case, the application program opens the debug and exports the connection at the client side.

telnet server-ip-addr/server-host-name echo/noecho

In this case, the application program enables or disables the local echo. The local echo is disabled by default. The echo is completed at the server side. Only when the server is not in charge of echo is the local echo enabled.

telnet server-ip-addr/server-host-name /script scriptname

Before executing the automatic login command of the script, run the command **ip telnet script** to configure the script.

The previous commands can be used together.

During the session with the remote server, you can press the **Q** button to exit the session. If the session is not manually closed, the session will be complete after a 10-second timeout.

Example

Suppose you want to telnet server 192.168.20.124, the telnet port of the server is port 23 and port 2323, and the local two interfaces are e1/1(192.168.20.240) and s1/0(202.96.124.240). You can run the following operations to complete the remote login.

1. telnet 192.168.20.124 /port 2323

In this case, the telnet connection with port 2323 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

2. telnet 192.168.20.124 /source-interface s1/0

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 202.96.124.240.

3. telnet 192.168.20.124 /local 192.168.20.240

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

4. telnet 192.168.20.124 /debug

In this case, the telnet connection negotiation with port 23 of the peer will be printed out.

5. telnet 192.168.20.124 /echo

In this case, the local echo is enabled. If the echo is also enabled at the server side, all input will be echoed twice.

6. telnet 192.168.20.124 /script s1

Use login script S1 for automatic login.

2.1.2 ip telnet

The following are the configuration command formats of the telnet session:

ip telnet source-interface vlan *value*

ip telnet access-class *accesslist*

ip telnet listen-port *start-port [end-port]*

ip telnet script *scriptname 'user_prompt' user_answer 'pwd_prompt' pwd_answer*

Parameter

Parameter	Description
value	Local interface where the telnet request is originated
accesslist	Access list name to limit the source address when the local client receives the connection
start-port	Starting port number designated at the listening port area
end-port	End port number designated at the listening port area
scriptname	Name of the login script
user_prompt	Username prompt returned by the telnet server
user_answer	Username response information from the client side
pwd_prompt	Password prompt returned by the telnet server
pwd_answer	Password response information submitted by the client side

Default

None

Command mode

Global configuration

Instruction

- Run the following command to configure the local interface for originating the telnet connection:

  ip telnet source-interface *interface*

  In this case, all telnet connections originated afterwards are through the interface. The configuration command is similar to the command **telnet source-interface *interface***. However, the **telnet** command has no interface parameters followed. When the interface is configured and the **telnet** command has interface parameters, the interface followed the telnet command is used.
- Run the following command to configure the name of the access list which performs limitation on local telnet connection reception.

  ip telnet access-class *accesslist*

In this case, the access list will be checked when the server accepts all telnet connections.

- Run the following command to configure a port, except the default port 23, to receive the telnet service.

  ip telnet listen-port *start-port [end-port]*

  Explanation: If the end port number is not designated, the listening will be executed at a specific port. The number of the designated ports cannot be bigger than 16 and the port number ranges between 3001 and 3999.

- Run the following command to configure the telnet login script.

  ip telnet script s1 ‘login:’ switch ‘Password:’ test

  Explanation: When the script is configured, the username prompt and password prompt and their answers must be correctly matched, especially the prompt information is capital sensitive and has inverted comma (‘’). If one of them is wrongly configured, the automatic login cannot be performed.

Note:

You can add the NO prefix on the above four commands and then run them to cancel previous configuration.

Example

1．ip telnet source-interface s1/0

In this case, the s1/0 interface will be adopted to originate all telnet connections afterwards.

2．ip telnet access-class abc

In this case, all the received telnet connections use access list **abc** to perform the access list check.

3．ip telnet listen-port 3001 3010

Except port 23, all ports from port 3001 to port 3010 can receive the telnet connection.

4．ip telnet script s1 ‘login:’ switch ‘Password:’ test

The login script **s1** is configured. The username prompt is **login:** and the answer is **switch**. The password prompt is **Password:** and the answer is **test**.

2.1.3 ctrl-shift-6+x (the current connection is mounted)

Run the following command to mount the current telnet connection:

ctrl-shift-6+x

Parameter

None

Default

None

Command mode

Any moment in the current telnet session

Instruction

You can use the shortcut key to mount the current telnet connection at the client side.

Example

switchA>telnet 192.168.20.1

Welcome to Multi-Protocol 2000 Series switch

switchB>ena

switchB#(press ctrl-shift-6+x)

switchA>

You press **ctrl-shift-6+x** to mount the telnet connection to switch B and return to the current state of switch A.

2.1.4 where

Run the following command to check the currently mounted telnet session:

where

Parameter

None

Default

None

Command mode

Global configuration

Instruction

You can use the command to check the mounted outward telnet connection at the client side. The displayed information contains the serial number, peer address, local address and local port.

Note:

The **where** command is different from the **show telnet** command. The former is used at the client side and the displayed information is the outward telnet connection. The latter is used at the server and the displayed information is the inward telnet connection.

Example

switchA>telnet 192.168.20.1

Welcome to Multi-Protocol 2000 Series switch

switchB>ena

switchB#(Press ctrl-shift-6+x)

switchA> telnet 192.168.20.2

Welcome to Multi-Protocol 2000 Series switch

switchC>ena

switchC#(Press ctrl-shift-6+x)

switchA>where

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.1	23	192.168.20.180	20034
2	192.168.20.2	23	192.168.20.180	20035

Enter where at switch A. The mounted outward connection is displayed.

2.1.5 resume

It is used to resume the currently mounted outward telnet connection:

resume *no*

Parameter

Parameter	Description
no	Number of the currently mounted telnet session that is checked

	through the **where** command

Default

None

Command mode

Global configuration

Instruction

The command can be used to resume the currently mounted outward telnet connection at the client side.

Example

switchA>telnet 192.168.20.1

Welcome to Multi-Protocol 2000 Series switch

switchB>ena

switchB#(press ctrl-shift-6+x)

switchA> telnet 192.168.20.2

Welcome to Multi-Protocol 2000 Series switch

switchC>ena

switchC#(press ctrl-shift-6+x)

switchA>where

NO. Remote Addr Remote Port Local Addr Local Port

1 192.168.20.1 23 192.168.20.180 20034

2 192.168.20.2 23 192.168.20.180 20035

switchA>Resume 1

[Resuming connection 1 to 192.168.20.73 . . .]

(enter)

switchB#

After you enter **where** at switch A and the mounted outward connection of switch A is displayed, enter **Resume1**. You will be prompted that connection 1 is resumed. The command prompts of switch B are displayed after the **Enter** key is pressed.

2.1.6 disconnect

The following command is used to clear the currently mounted outward telnet session:

disconnect *no*

Parameter

Parameter	Description
No	Number of the currently mounted telnet session that is checked through the **where** command

Default

None

Command mode

Global configuration

Instruction

The command can be used to clear the currently mounted outward telnet connection at the client side.

Note:

The **disconnect** command is different from the **clear telnet** command. The former is used at the client side and clears the outward telnet connection. The latter is used at the server and clears the inward telnet connection.

Example

switchA>telnet 192.168.20.1

Welcome to Multi-Protocol 2000 Series switch

switchB>ena

switchB#(press ctrl-shift-6+x)

switchA> telnet 192.168.20.2

Welcome to Multi-Protocol 2000 Series switch

switchC>ena

switchC#(press ctrl-shift-6+x)

switchA>where

NO. Remote Addr Remote Port Local Addr Local Port

1 192.168.20.1 23 192.168.20.180 20034

2 192.168.20.2 23 192.168.20.180 20035

switchA>disconnect 1

<Closing connection to 192.168.20.1> <y/n>y

Connection closed by remote host.

switchA>

After you enter **where** at switch A and the mounted outward connection of switch A is displayed, enter **disconnect 1**. You will be prompted whether the connection of switch B is closed. After you enter **Y**, the connection is closed.

2.1.7 clear telnet

The following is a command format to clear the telnet session at the server:

clear telnet *no*

Parameter

Parameter	Description
no	Number of the telnet session that is displayed after the **show telnet** command is run

Default

None

Command mode

Management mode

Instruction

The command is used to clear the telnet session at the server.

Example

clear telnet 1

The telnet session whose sequence number is 1 is cleared at the server.

2.1.8 show telnet

The following is a command format to display the telnet session at the server:
show telnet

Parameter

None

Default

None

Command mode

All command modes except the user mode

Instruction

The command is used to display the telnet session at the server. The displayed information includes the sequence number, peer address, peer port, local address and local port.

Example

Switch# show telnet

If you run the previous command, the result is shown as follows:

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.220	1097	192.168.20.240	23
2	192.168.20.180	14034	192.168.20.240	23

2.1.9 debug telnet

The following is a format of the **debug** command for the telnet session:
debug telnet

Parameter

None

Default

None

Command mode

Management mode

Instruction

The command is used to open the switch of the telnet debug.
If the switch of the telnet debug is opened, the negotiation processes of all the incoming telnet sessions are printed on the window that the debug command invokes. The **debug telnet** command is different from the **telnet debug** command. The former is to export the debug information of the telnet session connected to the server. The latter is to export the debug information of the telnet session that the client originates.

Example

debug telnet

The debug information of the telnet session that is connected to the server is displayed.

2.2 Terminal Configuration Command

The following are terminal configuration commands:

- attach-port
- autocommand
- clear line
- connect
- disconnect
- exec-timeout
- length
- line
- location
- login authentication
- monitor
- no debug all
- password
- printer enable
- printer start
- printer stop

- resume
- script activation
- script callback
- script connection
- script dialer
- script reset
- script startup
- sequence-char
- show debug
- show line
- show tty-status
- switchkey
- switchmsg
- terminal-type
- terminal monitor
- terminal width
- terminal length
- where
- width

2.2.1 attach-port

The following command is to bind the telnet listening port to the **line vty** number and enable the telnet connection at a specific port generates **vty** according to the designated sequence number.

[no] attach-port *PORT*

Parameter

Parameter	Description
port	Listening port of the telnet server (3001-3999)

Default

None

Command mode

Line configuration mode

Example

Bind listening port 3001 to line vty 2 3.

```
switch_config# line vty 2 3
```

switch_config_line#attach-port 3001

2.2.2 autocommand

It is used to set the automatically-run command when user logs in to the terminal. The connection is cut off after the command is executed.

autocommand *LINE*

no autocommand

Parameter

Parameter	Description
LINE	Command to be executed

Command mode

Line configuration mode

Example

switch_conf#line vty 1

switch_conf_line#autocommand pad 123456

After you successfully log in, the host whose X.121 address is 123456 will be automatically padded.

2.2.3 clear line

It is to clear the designated line.

clear line [*aux* | *tty* | *vty*] [*number*]

Parameter

Similar to the **line** command

Command mode

Management mode

Example

switch#clear line vty 0

2.2.4 connect

It is to connect the telnet server.

connect *server-ip-addr/server-host-name* {[/**port** *port*][/**source-interface** *interface*] [/**local** *local-ip-addr*]}

Parameter

Parameter	Description
server-ip-addr/server-host-name	IP address of the server or the host name of the server
port	Port number
interface	Name of the interface where the connection is originated
local-ip-addr	Local IP address where the connection is originated

Command mode

All configuration modes

Example

switch# connect 192.168.20.1

2.2.5 disconnect

It is used to delete the mounted telnet session.

disconnect *N*

Parameter

Parameter	Description
N	Number of the mounted telnet session

Command mode

All configuration modes

Example

switch#disconnect 1

2.2.6 exec-timeout

It is to set the maximum spare time for the terminal.

[**no**] **exec-timeout** [*time*]

Parameter

Parameter	Description
time	Spare time whose unit is second

Default

0 (No time-out limitation)

Command mode

Line configuration mode

Example

Set the spare time of the line to one hour.

switch_config_line#exec-timeout 3600

2.2.7 length

It is used to set the line number on the screen of the terminal.

[**no**] **length** [*value*]

Parameter

Parameter	Description
value	A value between 0 and 512 The value **0** means there is no pause.

Default

24

Command mode

Line configuration mode

2.2.8 line

It is used to enter the line configuration mode.

line [**aux | console | tty | vty**] [*number*]

Parameter

Parameter	Description
aux	Auxiliary line, which has only one number **0**
console	Monitoring line, which has only one number **0**
tty	Asynchronous line
vty	Virtual lines such as Telnet, PAD and Rlogin
number	Number in the line of the type

Command mode

Global configuration

Example

The following example shows how to enter the line configuration mode of VTY 0 to 10.

switch_config#line vty 0 10

2.2.9 location

It is used to recoded the description of the current line.

location [*LINE*]

no location

Parameter

Parameter	Description
LINE	Description of the current line

Command mode

Line configuration mode

2.2.10 login authentication

It is used to set line login authentication:

[**no**] **line login authentication** [**default** | *WORD*]

Parameter

Parameter	Description
Default	Default authentication mode
WORD	Name of the authentication list

Command mode

Line configuration mode

Example

switch_conf_line#login authentication test

In the example, the authentication list of the line is set to **test**.

2.2.11 monitor

It is used to export the log and debugging information to the line:

[**no**] **monitor**

Parameter

None

Command mode

Line configuration mode

Example

switch_config_line#monitor

2.2.12 no debug all

It is used to shut down all debugging output of the current VTY:

no debug all

Parameter

None

Command mode

Management mode

Example

switch#no debug all

2.2.13 password

It is used to set the password for the terminal:

password {*password* | [encryption-type] *encrypted-password* }

no password

Parameter

Parameter	Description
password	Password configured on the line, which is entered in the plaintext form and whose maximum length is 30 bits.
[encryption-type] *encrypted-password*	**encryption-type** means the encryption type of the password. Currently, MY COMPANY products only support two encryption modes: 0 and 7. The number **0** means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number **7** means the password is encrypted through an algorithm defined by MY COMPANY. You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches.

For password encryption, refer to the explanation of the commands **service *password-encryption*** and **enable password**.

Command mode

Line configuration mode

Example

switch_conf#line vty 1

switch_conf_line#password test

The previous example shows the login password of VTY1 is set to

test.

2.2.14 resume

It is used to resume the mounted telnet session:

resume *N*

Parameter

Parameter	Description
N	Number of the mounted telnet session

Command mode

All configuration modes

Example

switch#resume 1

2.2.15 show debug

It is used to display all debugging information of the current VTY:
show debug

Parameter

None

Command mode

Management mode or global configuration mode

Example

Switch# show debug
http authentication debug is on
http cli debug is on
http request debug is on
http response debug is on
http session debug is on
http erro debug is on
http file debug is on

TELNET:

Incoming Telnet debugging is on

2.2.16 show line

It is used to display the status of the current effective line:
show line {[**console** | **aux** | **tty** | **vty**] [*number*]}

Parameter

If there is no parameter followed, the status of all effective lines will be displayed.
The definition of other parameters is similar to that of the **line** command.

Command mode

All configuration modes except the user mode

2.2.17 terminal length

It is used to change the line number on the current terminal screen. The parameter can be obtained by the remote host. The rlogin protocol uses the parameter to notify the remote UNIX host. Run the **no terminal length** command to resume the default value:
terminal length *length*
no terminal length

Parameter

Parameter	Description
Length	Line number displayed on each screen

Default

Pause when 24 lines are displayed on the screen.

Command mode

Global configuration

Instruction

The command is effective only to the current terminal. When the session is complete, the terminal attribute is invalid.

Example

switch#terminal length 40

Related command

line

2.2.18 terminal monitor

It is used to display the debugging output information and system faulty information at the current terminal. The negative form of the command is used to disable the monitoring:

terminal monitor

no terminal monitor

Parameter

None

Default

The system monitoring port (console) is open by default. Other terminals are closed by default.

Command mode

Global configuration

Instruction

The command is effective only to the current terminal. When the session is complete, the terminal attribute is invalid.

Example

switch#terminal monitor

Related command

line

debug

2.2.19 terminal width

In default settings, the switch is to export 80 characters in each line. If the default settings cannot meet your requirements, you can reset it.

The parameter can be obtained by the remote host. Run the **terminal width** command to set the character number in each line. Run the **no terminal width** command to resume to the default value.

terminal width *number*
no terminal width

Parameter

Parameter	Description
number	Character number of each line

Default

80 characters in each line

Command mode

Global configuration

Instruction

The command is effective only to the current terminal. When the session is complete, the terminal attribute is invalid.

Example

switch#terminal width 40

Related command

line

2.2.20 terminal-type

It is used to set the terminal type:
[**no**] **terminal-type** [*name*]

Parameter

Parameter	Description
Name	Terminal name Terminal types currently supported are VT100, ANSI and

	VT100J.

Default

ANSI

Command mode

Line configuration mode

2.2.21 where

It is used to check the currently mounted outward telnet session at the client side:
where

Parameter

None

Command mode

All configuration modes

Example

switch#where

2.2.22 width

It is used to set the terminal width of the line:
[**no**] **width** [*value*]

Parameter

Parameter	Description
Value	A value between 0 and 512 The value **0** means no execution.

Default

80

Command mode

Line configuration mode

Chapter 3 Maintenance and Debugging Tool Commands

3.1 Network Testing Tool Commands

3.1.1 ping

It is used to test host accessibility and network connectivity. After the **ping** command is run, an ICMP request message is sent to the destination host, and then the destination host returns an ICMP response message.

ping [**-f**] [**-i** {source-ip-address | source-interface}] [**-j** host1 [host2 host3 …]] [**–k** host1 [host2, host3 …]] [**-l** length] [**-n** number] [**-r** hops] [**-s** tos] [**-t** ttl] [**-v**] [**-w** *waittime*] **host**

Parameter

Parameter	Description
-f	Sets the DF digit (message is not segmented). If the message required to be sent is larger than the MTU of the path, the message will be dropped by the routing switch on the path and the routing switch will then return an ICMP error message to the source host. If network performance has problems, one node in the network may be configured to a small MTU. You can use the **–f** option to decide the smallest MTU on the path. Default value: No resetting
-i	Sets the source IP address of the message or the IP address of an interface. Default value: Main IP address of the message-sending interface
source-ip-address	Source IP address adopted by the message

source-interface	Message takes the IP address of the **source-interface** interface as the source address.
-j *host1* [*host2 host3*…]	Sets the relaxation source route. Default: Not set
-k *host1* [*host2 host3*…]	Sets the strict source route Default: Not set
-l *length*	Sets the length of ICMP data in the message. Default: 56 bytes
-n *number*	Sets the total number of messages. Default: 5 messages
-r *hops*	Records routes. Up to **hops** routes are recorded. Default: not record
-s *tos*	Sets IP TOS of the message to ***tos***. Default: 0
-t *ttl*	Sets IP TTL of the message to **ttl**. Default: 255
-**v**	Detailed output Default: simple output
-w *waittime*	Time for each message to wait for response Default: 2 seconds
host	Destination host

Command mode

Management mode, global configuration mode and interface configuration mode

Instruction

The command supports that the destination address is the broadcast address or the multicast address. If the destination address is the broadcast address (255.255.255.255) or the multicast address, the ICMP request message is sent on all interfaces that support broadcast or multicast. The routing switch is to export the addresses of all response hosts. By pinging multicast address 224.0.0.1, you can obtain the information about all hosts in directly-connected network segment that support multicast transmission.

Press the **Q** key to stop the **ping** command.

Simple output is adopted by default.

Parameter	Description
!	A response message is received.
.	Response message is not received in the timeout time.
U	The message that the ICMP destination cannot be reached is received.
Q	The ICMP source control message is received.
R	The ICMP redirection message is received.
T	The ICMP timeout message is received.
P	The ICMP parameter problem message is received.

The statistics information is exported:

Parameter	Description
packets transmitted	Number of transmitted messages
packets received	Number of received response messages, excluding other ICMP messages
packet loss	Rate of messages that are not responded to
round-trip min/avg/max	Minimum/average/maximum time of a round trip (ms)

Example

switch#ping -l 10000 -n 30 192.168.20.125

PING 192.168.20.125 (192.168.20.125): 10000 data bytes

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

--- 192.168.20.125 ping statistics ---

30 packets transmitted, 30 packets received, 0% packet loss

round-trip min/avg/max = 50/64/110 ms

3.1.2 traceroute

It is used to detect which routes have already reached the destination. You can transmit to the destination the UDP packets (or ICMP ECHO packets) of different TTLs to confirm which routes have come to the destination. Each router on this path has to deduct 1 from the TTL value before forwarding ICMP ECHO packets. Speaking from this aspect, TTL is an effective hop count. When the TTL value of a packet is deducted to zero, the router sends back to the source system the ICMP timeout message.

By checking the ICMP timetout message sent back by intermedial routers, you can confirm the routers. At the arrival of the destination, the traceroute sends a UPD packet whose port ID is larger than 30000; the destination node hence can only transmit back a Port Unreachable ICMP message. This reception of this message means the arrival of destination.

traceroute [**-i** source-ip-address] [**-m** source-interface}] [**-j** host1 [host2 host3 …]] [**–k** host1 [host2, host3 …]] [**-p** port-number] [**-q** probe-count] [**-r** hops] [**-t** ttl] [**-w** *waittime*] [**-x icmp**] **host**

Parameter

Parameter	Description
-i *source-ip-address*	Sets the source IP address of packet.
-m *source-interface*	Sets the packet-transmitted port.
-j *host1* [*host2 host3…*]	Sets the loose source route.Default: Not set
-k *host1* [*host2 host3…*]	Sets the strict source route. Default: Not set
-p *port-number*	Sets the ID of destination port that transmits UDP packets. Default value: 33434

-q *probe-count*	Sets the number of packets that you detect each time. Default: 3 packets
-r *hops*	Records the routes (at most ***hops*** routes can be recorded). Default: The routes are not recorded.
-t *ttl*	Sets the IP TTL of packets as TTL. Default: the minimum and maximum TTLs are 1 and 30 respectively.
-w *waittime*	Means the time that each packet waits for echo. Default value: 3 seconds
-x icmp	Sets the detection packet to be the ICMP ECHO packet. Default: UDP packet
host	Means the destination host.

Command mode

EXEC or global configuration mode

Explanation

The UDP packet is used for detection by default, but you can run **–x icmp** to replace it with ICMP ECHO for detection.
If you want to stop traceroute, press **q** or **Q**.
By default, the simple output information is as follows.

Parameter	Description
!N	Receives an ICMP-route unreachable packet.
!H	Receives an ICMP-host unreachable packet.
!P	Receives an ICMP-protocol unreachable packet.
!F	Receives an ICMP unreachable (need to be fragmented) packet.
!S	Receive an ICMP unreachable (failing to detect the source-station route) packet.

The exported statistics information is as follows:

Parameter	Description

hops max	Means the maximum detection hops (the threshold of ICMP).
byte packets	Stands for the size of each detection packet.

Example

switch#traceroute 90.1.1.10

traceroute to 90.1.1.10 (90.1.1.10), 30 hops max, 36 byte packets

1 90.2.2.1 0 ms 0 ms 0 ms

2 90.1.1.10 0 ms 0 ms 0 ms

3.2 Fault Diagnosis Commands

The chapter describes the commands used for fault diagnosis. All the following commands are used to detect the reason of the fault. You can use other commands to remove the fault, such as the **debug** command.

The following are fault diagnosis commands:

- logging
- logging buffered
- logging console
- logging facility
- logging monitor
- logging on
- logging trap
- service timestamps
- clear logging
- show break
- show controller
- show debug
- show logging

3.2.1 logging

It is used to record the log information to the **syslog** server.

logging *A.B.C.D*

no logging *A.B.C.D*

Parameter

Parameter	Description
A.B.C.D	IP address of the **syslog** server

Default:

The log information is not recorded to the server.

Command mode

Global configuration

Instruction

It is used to record the log information to the designated **syslog** server.
It can be used for many times to designate multiple **syslog** servers.

Example

logging 192.168.1.1

Related command

logging trap

3.2.2 logging buffered

It is used to record the log information to the memory of the switch.
logging buffered [*size* | *level* | *dump*]

no logging buffered

Parameter

Parameter	Description
size	Size of memory cache Value range: 4096-2147483647 Unit: byte
level	Information level of the log recorded to memory cache Refer to table 1.

dump	When the system has abnormality, the information in the current memory is currently recorded to the flash and the information is resumed after the system is restarted.

Default

The information is not recorded to the memory cache.

Command mode

Global configuration

Instruction

The command records the log information to the memory cache of the switch. The memory cache is circularly used. After the memory cache is fully occupied, the latter information will cover the previous information.

You can use the **show logging** command to display the log information recorded in the memory cache of the switch.

Do not use big memory for it causes the shortage of memory.

Table 1 Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Related command

clear logging
show loggin

3.2.3 logging console

Run the command **logging console** to control the information volume displayed on the console.
Run the command **no logging console** to forbid the log information to be displayed on the console:
logging console *level*
no logging console

Parameter

Parameter	Description
level	Information level of the logs displayed on the console Refer to table 2.

Default

None

Command mode

Global configuration

Instruction

After the information level is specified, information of this level or the lower level will be displayed on the console.
Run the command **show logging** to display the currently configured level and the statistics information recorded in the log.

Table 2 Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT

errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging console alerts

Related command

logging facility
show logging

3.2.4 logging facility

Run the command **logging facility** to configure to record specified error information. To restore to **local7**, run the command **no logging facility**.
logging facility *facility-type*
no logging facility

Parameter

Parameter	Description
facility-type	Facility type Refer to table 3.

Default

local7

Command mode

Global configuration

Instruction

Table 3 Facility type

Type	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Example

logging facility kern

Related command

logging console

3.2.5 logging monitor

Run the command **logging monitor** to control the information volume displayed on the terminal line.
Run the command **no logging monitor** to forbid the log information to be displayed on the terminal line.

logging monitor *level*
no logging monitor

Parameter

Parameter	Description
level	Information level of the logs displayed on the terminal line Refer to table 4.

Default

debugging

Command mode

Global configuration

Instruction

Table 4 Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System is unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE

informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging monitor errors

Related command

terminal monitor

3.2.6 logging on

Run the command **logging on** to control the recording of error information.
Run the command **no logging on** to forbid all records.
logging on
no logging on

Parameter

None

Default

logging on

Command mode

Global configuration

Example

switch_config# **logging on**
switch_config# ^Z
switch#
Configured from console 0 by DEFAULT
switch# **ping 192.167.1.1**

switch#ping 192.167.1.1
PING 192.167.1.1 (192.167.1.1): 56 data bytes
!!!!!

--- 192.167.1.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/4/10 ms

switch#IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

switch_config# **no logging on**

switch_config# ^Z

switch#

switch# **ping** 192.167.1.1

PING 192.167.1.1 (192.167.1.1): 56 data bytes

!!!!!

--- 192.167.1.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/4/10 ms

Related command

logging
logging buffered
logging monitor

logging console

3.2.7 logging trap

Run the command **logging trap** to control the information volume recorded to the syslog server.
Run the command **no logging trap** to forbid the information to be recorded to the syslog server.

logging trap *level*
no logging trap

Parameter

Parameter	Description
level	Information level of the logs displayed on the syslog server Refer to table 5.

Default

Informational

Command mode

Global configuration

Instruction

Table 5 Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System is unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING

notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging 192.168.1.1

logging trap notifications

Related command

logging

3.2.8 logging command

To enable the command execution recording, run **logging command**. After this function is opened, a log will be generated for each of all entered commands, in which the line to execute this command, the command line, the execution result, the login line and the login address will be recorded.

You can use **no logging command** to disable this function.

Parameter

N/A

Default value

no logging command

Command mode

Global configuration mode

Example

Switch_config#logging command

Switch_config#Jul 11 15:26:56 %CMD-6-EXECUTE: `logging command ` return 0, switch(vty 0, 192.168.25.42).

Related command

logging

3.2.9 logging source-interface

This command is used to set the source port of log exchange.
You can use **no logging source-interface** to disable this function.

Parameter

N/A

Default value

no logging source-interface

Command mode

Global configuration mode

Example

Switch_config# logging source-interface vlan 1

Related command

logging

3.2.10 logging history alerts

This command is used to set the level of the historical log table to **alerts** (need to act immediately).

Parameter

N/A

Default value

logging history warnings

Command mode

Global configuration mode

Example

Switch_config#logging history alerts

Related command

logging

3.2.11 logging history critical

This command is used to set the level of the historical log table to **critical**.

Parameter

N/A

Default value

logging history warnings

Command mode

Global configuration mode

Example

Switch_config#logging history critical

Related command

logging

3.2.12 logging history debugging

This command is used to set the level of the historical log table to **debugging**.

Parameter

N/A

Default value

logging history warnings

Command mode

Global configuration mode

Example

Switch_config#logging history debugging

Related command

logging

3.2.13 logging history emergencies

This command is used to set the level of the historical log table to **emergencies**.

Parameter

N/A

Default value

logging history warnings

Command mode

Global configuration mode

Example

Switch_config#logging history emergencies

Related command

logging

3.2.14 logging history errors

This command is used to set the level of the historical log table to **errors**.

Parameter

N/A

Default value

logging history warnings

Command mode

Global configuration mode

Example

Switch_config#logging history errors

Related command

logging

3.2.15 logging history informational

This command is used to set the level of the historical log table to **informational**.

Parameter

N/A

Default value

logging history warnings

Command mode

Global configuration mode

Example

Switch_config#logging history informational

Related command

logging

3.2.16 logging history notifications

This command is used to set the level of the historical log table to **notifications**.

Parameter

N/A

Default value

logging history warnings

Command mode

Global configuration mode

Example

Switch_config#logging history notifications

Related command

logging

3.2.17 logging history warnings

This command is used to set the level of the historical log table to **warnings**.

Parameter

N/A

Default value

logging history warnings

Command mode

Global configuration mode

Example

Switch_config#logging history warnings

Related command

logging

3.2.18 logging history rate-limit

This command is used to set the log output rate.

Parameter

Parameter	Description
<1-512>	Stands for the number of logs which are exported each second.

Default value

logging history rate-limit 0

Command mode

Global configuration mode

Example

Switch_config#logging history rate-limit 256

Related command

logging

3.2.19 logging history size

This command is used to set the number of entries in the historical log table.

Parameter

Parameter	Description
<0-500>	Stands for the number of historical log entries.

Default value

logging history size 0

Command mode

Global configuration mode

Example

Switch_config#logging history size 256

Related command

logging

3.2.20 service timestamps

Run the command **service timestamps** to configure the time stamp that is added when the system is debugged or records the log information.
Run the command **no service timestamps** to cancel the time stamp that is added when the system is debugged or records the log information.

service timestamps [log|debug] [*uptime*| *datetime*]
no service timestamps [log|debug]

Parameter

Parameter	Description
log	Adds the time stamp before the log information.
debug	Adds the time stamp before the debug information.
uptime	Duration between the startup of the switch and the current time
datetime	Real-time clock time

Default

Service timestamps log date
Service timestamps debug date

Command mode

Global configuration

Instruction

The time stamp in the **uptime** form is displayed like HHHH:MM:SS, meaning the duration from the start-up of the switch to the current time. The time stamp in the **date** form is displayed like YEAR-MON-DAY HH:MM:SS, meaning the real-time clock time.

Example

Service timestamps debug uptime

3.2.21 clear logging

It is used to clear the log information recorded in the memory cache.
clear logging

Parameter

None

Command mode

Management mode

Related command

logging buffered
show logging

3.2.22 show break

It is used to display the information about abnormal breakdown of the switch.
show break [*map-filename*]

Parameter

Parameter	Description
map-filename	Specifies the filename of the function mapping table.

Default

None

Command mode

Management mode

Instruction

It is used to display the information about abnormal breakdown of the switch, helping to find the cause of the abnormality.

Example

```
switch#sh break
Exception Type:1400-Data TLB error
BreakNum: 1 s date: 2000-1-1    time: 0:34:6
r0          r1          r2          r3          r4          r5          r6
00008538-01dbc970-0054ca18-00000003-80808080-fefefeff-01dbcca1-
r7          r8          r9          r10         r11         r12         r13
00000000-00009032-00000000-7ffffff0-00008588-44444444-0054c190-
r14         r15         r16         r17         r18         r19         r20
000083f4-000083f4-00000000-00000000-00000000-00000000-00000000-
r21         r22         r23         r24         r25         r26         r27
00000000-0000000a-00000001-00000000-00000000-004d6ce8-01dbd15c-
r28         r29         r30         r31         spr8        spr9        ip
00000002-00467078-00010300-00000300-00000310-00008588-00000370-
Variables :
00008538-44444444-01dbd15c-01dbcaac-00000002-00000000-004d6ce8-
01dbca18-
 00008538 ---   do_chram_mem_sys_addr---bspcfg.o
 0001060c ---   subcmd---cmdparse.o---libcmd.a
 000083e4 ---   do_chram_mem_sys---bspcfg.o
 0000fb24 ---   lookupcmd---cmdparse.o---libcmd.a
 0000f05c ---   cmdparse---cmdparse.o---libcmd.a
 003e220c ---   vty---vty.o---libvty.a
 00499820 ---   pSOS_qcv_broadcast---ksppc.o---os\libsys.a
```

The whole displayed content can be divided into six parts:

1 RROR:file function.map not found

The prompt information means that the system has not been installed the software **function.map**, which does not affect the system running. If the version of the software **function.map** is not consistent with that of the switch, the system prompts that the version is not consistent.

2 Exception Type—Abnormal hex code plus abnormal name

3 BreakNum

It is the current abnormal number. It means the number of abnormalities that the system has since it is powered on in the latest time. It is followed by the time when the abnormality occurs.

4 Content of the register

The common content of the register is listed out.

5 Variable area
The content in the stack is listed out.

6 Calling relationship of the number
If the **map** file is not installed on the system, only the function's address is displayed. If the **map** file is installed on the system, the corresponding function name, **.o** file name and **.a** file name are displayed.
The calling relationship is from bottom to top.

3.2.23 show debug

It is used to display all the enabled debugging options of the switch.
show debug

Parameter

None

Command mode

Management mode

Example

```
switch# show debug

Crypto Subsystem:
  Crypto Ipsec debugging is on
  Crypto Isakmp debugging is on
  Crypto Packet debugging is on
```

Related command

debug

3.2.24 show logging

It is used to display the state of logging (syslog).
show logging

Parameter

None

Command mode

Management mode

Instruction

It is used to display the state of logging (syslog), including the login information about the console, monitor and syslog.

Example

switch# show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
Console logging: level debugging, 12 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 4 messages logged
Trap logging: level informations, 0 message lines logged

Log Buffer (4096 bytes):
2000-1-4 00:30:11 Configured from console 0 by DEFAULT
2000-1-4 00:30:28 User DEFAULT enter privilege mode from console 0, level = 15

Related command

clear logging

Chapter 4 SSH Configuration Commands

4.1.1 ip sshd enable

Command description

ip sshd enable
no ip sshd enable

Parameter

None

Default

1024 bits

Instruction

It is used to generate the rsa encryption key and then monitor the connection to the ssh server. The process of generating encryption key is a process of consuming the calculation time. It takes one or two minutes.

Command mode

Global configuration mode

Example

In the following example, the SSH service is generated.

device_config#ip sshd enable

4.1.2 ip sshd timeout

Command description

ip sshd timout *time-length*
no ip timeout

Parameter

Parameter	Description

time-length	Maximum time from the establishment of connection to the authentication approval Value range: 60-65535

Default

180 seconds

Instruction

To prevent the illegal user from occupying the connection resources, the connections that are not approved will be shut down after the set duration is exceeded.

Command mode

Global configuration mode

Example

In the following example, the timeout time is set to 360 seconds:

device_config#ip sshd timeout 360

4.1.3 ip sshd auth-method

Command description

ip sshd auth-method *method*

no sshd auth-method

Parameter

Parameter	Description
method	Sets authentication method list.

Default

The **default** authentication method list is used.

Instrunction

The ssh server uses the authentication method list of the login type.

Command mode

Global configuration mode

Example

In the following example, an **auth-ssh** authentication method list is configured and it is applied to the ssh server:

device_config#aaa authentication login auth-ssh local

device_config#ip sshd auth-method auth-ssh

4.1.4 ip sshd access-class

Command description

ip sshd access-class *access-list*
no ip sshd access-class

Parameter

Parameter	Description
access-list	Standard IP access list

Default

No access control list

Instrunction

It is used to configure the access control list for the ssh server. Only the connections complying with the regulations in the access control list can be approved.

Command mode

Global configuration mode

Example

In the following example, an **ssh-accesslist** access control list is configured and applied in the ssh server:

device_config# ip access-list standard ssh-accesslist

device_config_std_nacl#deny 192.168.20.40

device_config#ip sshd access-class ssh-accesslist

4.1.5 ip sshd auth-retries

Command description

ip sshd auth-retries *times*
no ip sshd auth-retries

Parameter

Parameter	Description
times	Maximum re-authentication times Value range: 0-65535

Default

3 times

Instrunction

The connection will be shut down when the re-authentication times exceeds the set times.

Command mode

Global configuration mode

Example

In the following example, the maximum re-authentication times is set to five times:

device_config#ip sshd auth-retries 5

4.1.6 ip sshd clear

Command description

ip sshd clear *ID*

Parameter

Parameter	Description
ID	Number of the SSH connection to the local device Value range: 0-65535

Default

N/A

Instruction

It is used to mandatorily close the incoming ssh connection with the specified number. You can run the command **show ip sshd line** to check the current incoming connection's number.

Command mode

Global configuration mode

Example

In the following example, the No.0 incoming connection is mandatorily closed:

device_config#ip sshd clear 0

4.1.7 ip sshd silence-period

Syntax

ip sshd silence-period *time-length*
no ip sshd silence-period

Parameter

Parameter	Description
time-length	Means the time of the silence, which ranges from 0 to 3600.

Default value

60s

Remarks

This command is used to set the login silence period. After the accumulated login failures exceed a certain threshold, the system regards that there exist attacks and disables the SSH service in a period of time, that is, the system enters the login silence period.
The silence period is set by the **ip sshd silence-period** command. The default silence period is 60 seconds. The allowable login failures are set by the **ip sshd auth-retries** command, whose default value is 6.

Command mode

Global configuration mode

Example

The following example shows how to set the silence period to 200 seconds.
switch_config#ip sshd silence-period 200

4.1.8 ip sshd sftp

Syntax

ip sshd **sftp**
no ip sshd **sftp**

Parameter

N/A

Default value

N/A

Remarks

This command is used to enable the SFTP function. The SFTP function refers to the secure file transmission system based on SSH, of which the authentication procedure and data transmission are encrypted. Though it has low transmission efficiency, network security is highly improved.

Command mode

Global configuration mode

Example

The following example shows how to enable the SFTP function.
switch_config#ip sshd sftp

4.1.9 ip sshd save

Syntax

ip sshd save

no ip sshd save

Parameter

N/A

Default value

N/A

Remarks

This command is used to save the initial key. When the SSH server is restarted, the key will be first read from the flash; if the key reading is successful, the recalculation of key will be avoided and the startup time will be shortened.

Command mode

Global configuration mode

Example

The following example shows how to enable the key protection function.
switch_config#ip sshd save

4.1.10 ip sshd disable-aes

Syntax

ip sshd disable-aes
no ip sshd disable-aes

Parameter

N/A

Default value

The AES encryption algorithm is forbidden.

Remarks

This command is used to decide whether to use the AES algorithm during the encryption algorithm negotiation. The AES algorithms such as aes128-cbc and aes256-cbc are not used by default.

Command mode

Global configuration mode

Example

The following example shows how to disable the AES encryption algorithm.
switch_config#ip sshd disable-aes

4.1.11 ssh

Command description

ssh –l *userid* **–d** *destIP* **[-c {des|3des|blowfish }] [-o** *numberofpasswdprompts***] [-p** *port***]**

Parameter

Parameter	Description
–l userid	User account on the server
–d destI	Destination IP address in the dotted decimal system
-o numberofpasswdprompts	Re-authentication times after the first authentication fails Actual re-authentication times is the set value plus the smallest value set on the server. Its default value is three times. Value range: 0-65535
-p port	Port number that the server monitors Its default value is 22. Value range: 0-65535
-c {des|3des|blowfish}	Encryption algorithm used during communication The encryption algorithm is 3des by default.

Default

N/A

Instruction

The command is used to create a connection with the remote ssh server.

Command mode

Privileged mode

Example

In the following example, a connection with the ssh server whose IP address is 192.168.20.41 is created. The account is **zmz** and the encryption algorithm is **blowfish**:

device#ip ssh –l zmz –d 192.168.20.41 –c blowfish

4.1.12 show ssh

Command description

show ssh

Parameter

None

Default value

N/A

Instrunction

It is used to display the sessions on the ssh server.

Command mode

Privileged mode

Example

In the following example, the sessions on the ssh server are displayed:

device#show ssh

4.1.13 show ip sshd

Command description

show ip sshd

Parameter

None

Default value

N/A

Instrunction

It is used to display the current state of the ssh server.

Command mode

Privileged mode

Example

In the following example, the current state of the ssh server is displayed:

device#show ip sshd

Chapter 5 Network Management Configuration Commands

5.1 SNMP Commands

SNMP commands are listed below:

- snmp-server community
- snmp-server contact
- snmp-server group
- snmp-server host/hostv6
- snmp-server location
- snmp-server packetsize
- snmp-server queue-length
- snmp-server trap-source
- snmp-server trap-timeout
- snmp-server user
- snmp-server view
- snmp-server source-addr
- snmp-sever udp-port
- snmp-server encryption
- Snmp-server trap-add-hostname
- snmp-server trap-logs
- snmp-server set-snmp-dos-max
- snmp-server keep-alive
- snmp-server encode
- snmp-server event-id
- show snmp
- debug snmp

5.1.1 snmp-server community

To set the community access string of the accessible SNMP protocol, run **snmp-server community** in global configuration mode.

snmp-server community [0|7] *string* [**view** *view-name*] [**ro | rw**] [*word*]

no snmp-server community *string*

no snmp-server community

Parameter

Parameter	Description
0	Sets the community string of the text.,
7	Sets the encrypted public string of the text.
string	Means the community string of the accessible SNMP protocol, which is similar to the password.
view view-name	(optional) stands for the previously defined view's name. In this view, the MIB objects, which are effective to the community, are defined.
ro	(Optional) Designates the read-only permission. Those authorized workstations can only read the MIB objects.
rw	(Optional) Designates the read-write permission. Those authorized workstations can read and modify the MIB objects.
word	(optional) Specifies the name of IP ACL of the SNMP proxy, which can be accessed by the community string.

Default value

By default, the SNMP community string allows the read-only permission to all objects.

Command mode

Global configuration mode

Explanation

The following command shows how to delete a designated community.

no snmp-server community *string*

The following command shows how to delete all communities.

no snmp-server community

Example

The following example shows how to distribute the “comaccess” string to SNMP, allow the read-only access and designate IP ACL to use the community string.

snmp-server community comaccess ro allowed

The following example shows how to distribute the “mgr” string to SNMP, allow to read and write the objects in the **Restricted** view。

snmp-server community mgr view restricted rw

The following example shows how to delete the “comaccess” community.

no snmp-server community comaccess

Related command

access-list

snmp-server view

5.1.2 snmp-server contact

To set the information about the contact person in a management node, run **snmp-server contact *text***.

snmp-server contact *text*

no snmp-server contact

Parameter

Parameter	Description
text	Means the string of the information about the contact person.

Default value

The information about contact person is not set.

Command mode

Global configuration mode

Explanation

It corresponds to the **sysContact** of the **MIB** variable in the **System** group.

Example

The following example shows the information about the contact person in a node.

snmp-server contact Dial_System_Operator_at_beeper_#_27345

5.1.3 snmp-server group

To create or update a SNMP group in global configuration mode, run the following first command; to cancel this SNMP group, run the following second command.

snmp-server group [*groupname* { **v3 [auth | noauth | priv**]}][**read** readview][**write** writeview] [**notify** notifyview] [**access** access-list]

Parameter

Parameter	Description
groupname	Stands for the name of the created or modified SNMP group.
v3	Means the version ID of the SNMP protocol.
auth|noauth|priv	Stands for the lowest security level of users in the SNMPv3 group.
readview	Means the access permission of GET operations, which is defined by the view.
writeview	Means the access permission of SET operations, which is defined by the view.
notifyview	Stands for the access permission during the transmission of Trap packets, which is defined by the view.
access-list	Allows users in the SNMP group to get through the IP access control list.

Default value

The readview allows all leaves of the Internet sub-tree to be accessed.

Command mode:

Global configuration mode

Instruction

The SNMP group is used to designate the access permission of the users in this group.

Example

In the following example, an SNMP group is set and named as **setter**, the version ID of the SNMP protocol is 3, the security level is authentication and encryption, and the view that is accessed by the **set** operation is **v-write**.

snmp-server group setter v3 priv write v-write

Related command

snmp-server view

snmp-server user

5.1.4 snmp-server [host|hostv6]

To specify the receiver of SNMP trap operation, run the first of the following commands in global configuration mode. To cancel this designated host, run the following second command.

snmp-server host|hostv6 *host* **[vrf** *word***] [udp-port** *port-num***] [permit|deny** *event-id***] {{version [v1 | v2c | v3]} | {[informs | traps] | [auth |noauth]}}** *community-string/user* **[authentication | configure| snmp]**

no snmp-server host *host community-string*

Parameter

Parameter	Description
host|hostv6	Sets the IPv4 or IPv6 host.
host	Means the host's name or the address of the Internet.
[vrf *word***]**	(Optional) binds VRF.
[udp-port *port-num***]**	(Optional) Specifies the ID of the UDP port, which transmits the traps.
[permit|deny *event-id***]**	(Optional) Allows or blocks to transmit a designated event.
{version [v1|v2c|v3]}	(Optional) Means the version ID of the SNMP protocol, which is used to transmit traps.
[informs | traps]	(Optional) Specifies the type of trap for version V2C. Informs: means the type of trap is "informs". Traps: means the type of trap is "traps".
[auth |noauth]	Specifies the trap authentication mode for version V3. auth: authentication

	noauth: no authenticatication
community-string/user	Means a community string in version 1 and version 2c which is similar to the password and sent with the trap operations or means the username in version 3.
[authentication | configure| snmp]	(optional) if no trap is designated, all generated traps will be sent to the host. authentication: allows to transmit those authentication-error traps. configure: allows to transmit the SNMP-configure traps. snmp: allows to transmit the SNMP traps.

Default value

This command is invalid in default settings. That is to say, no trap will be sent by default.

Command mode

Global configuration mode

Explanation

If this command is not entered, the traps will not be sent. In order to enable a switch to send the SNMP traps, you must run **snmp-server host**. If the keyword “trap-type” is not contained in this command, all kinds of traps of this host will be activated. If the keyword “trap-type” is contained in this command, all trap types related with this keyword are activated. You can specify multiple trap types in this command for each host.

If you designate multiple **snmp-server host** commands on the same host, the SNMP trap messages that are sent to the host will be decided by the community string and the trap type filtration in this command. (Only one trap type can be configured for a same host and a same community string).

The availability of the **trap-type** option depends on the switch type and the attributes of routing software, which is supported by this switch.

Example

The following example shows how to transmit the RFC1157-defined SNMP traps to host 10.20.30.40. The community string is defined as **comaccess**.

```
snmp-server host 10.20.30.40 comaccess snmp
```

The following example shows that the switch uses the **public** community string to send all types of traps to host 10.20.30.40.

```
snmp-server host 10.20.30.40 public
```

The following example shows that only the authentication traps are effective and can be sent to host **bob**.

```
snmp-server host bob public authentication
```

Related command

snmp-server queue-length

snmp-server trap-source

snmp-server trap-timeout

snmp-server event-id

snmp-server user

5.1.5 snmp-server location

To set the location string of a node, run the first one of the following two commands in global configuration mode. To cancel this location string, run the following second command.

snmp-server location *text*

no snmp-server location

Parameter

Parameter	Description
text	Describes the location string of a node.

Default value

The location string of a node is not set by default.

Command mode

Global configuration mode

Explanation

It corresponds to the **sysLocation** of the **MIB** variable in the **System** group.

Example

The following example shows how to define the actual location of a switch.

```
snmp-server location Building_3/Room_214
```

Related command

snmp-server contact

5.1.6 snmp-server packetsize

To define the maximum size of the SNMP packet when the SNMP server receives requests or responds, run the following first command in global configuration mode.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameter

Parameter	Description
byte-count	Stands for the integer bytes between 484 and 17940. The default value is 3000 bytes.

Default value

3000 byte

Command mode

Global configuration mode

Explanation

It corresponds to the **sysLocation** of the **MIB** variable in the **System** group.

Example

The following example shows how to set up a filter to filter those packets whose maximum length is 1024 bytes.

snmp-server packetsize 1024

Related command

snmp-server queue-length

5.1.7 snmp-server queue-length

To set the queue length for each trap host, run the following first command in global configuration mode.

snmp-server queue-length *length*

no snmp-server queue-length

Parameter

Parameter	Description
length	Stands for the number of trap events which can be saved in the queue (1-1000).

Default value

10 trap events.

Command mode

Global configuration mode

Explanation

This command is used to set the queue length for each trap host. Once the trap messages are successfully transmitted, the switch will empty the queue.

Example

The following example shows how to set up a message queue which can capture four events.

snmp-server queue-length 4

Related command

snmp-server packetsize

5.1.8 snmp-server trap-source

To designate an interface to be the source address of all traps, run the following first command in global configuration mode. To cancel this interface, run the following second command.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter

Parameter	Description
interface	Stands for the interface where SNMP traps generate. The parameters include the interface type and interface ID of the

	syntax mode of specific platform.

Default value

The interface is not designated.

Command mode

Global configuration mode

Explanation

When the SNMP server sends out a SNMP trap on whichever interface, the SNMP trap shall carry a trap address. If you want to use the trap address for tracking, you can use this command.

Example

The following example shows how to designate interface vlan1 as the source address of all traps.

snmp-server trap-source vlan1

Related command

snmp-server queue-length

snmp-server host

5.1.9 snmp-server trap-timeout

To set the timeout value of retransmitting traps, run the following first command in global configuration mode.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter

Parameter	Description
seconds	Means an interval for retransmitting traps, whose unit is second (1-1000).

Default value

30 seconds

Command mode

Global configuration mode

Explanation

Before switch software tries to send traps, it is used to look for the route of destination address. If no routes exists, traps will be saved in the retransmission queue. The **server trap-timeout** command decides the retransmission interval.

Example

The following example shows how to set the retransmission interval to 20 seconds:

snmp-server trap-timeout 20

Related command

snmp-server host

snmp-server queue-length

5.1.10 snmp-server user

To create or update an SNMP user in global configuration mode, run the following first command; to cancel this SNMP user, run the following second command. If the **remote** parameter is designated, a remote user will be configured; when a remote user is configured, the SNMP engine ID that corresponds to the IP address of this management station must exist.命令格式如下

snmp-server user *username groupname* **{ v3 [encrypted | auth] [md5 | sha]** *auth-password* **}**

Parameter

Parameter	Description
username	Stands for the name of the created or modified SNMP user.
groupname	Stands for the group where the user is.
v3	Stands for the SNMP version.
[encrypted | auth]	Encryption type: Encrypted: packet encryption auth: packet authentication
[md5 | sha]	Means the method of encryption authentication.
auth-password	Stands for the authentication password of the user. If this password is localized, it will be used as the authentication key

	and the encryption key of SNMPv3.

Default value

N/A

Command mode

Global configuration mode

Explanation

This command is used to set the username and the password.

Example

In the following example, an SNMP user is created, whose name is **set-user** and which belongs to group **setter**, the version of the SNMP protocol is version 3, the security level is authentication and encryption, the password is 12345678, and MD5 is used as the harsh algorithm.

snmp-server user set-user setter v3 encrypted auth md5 12345678

Related command

snmp-server view

snmp-server group

5.1.11 snmp-server view

To create or update a MIB view, run the first one of the following two commands in global configuration mode. To cancel a view in the SNMP server, run the second one of the following two commands.

snmp-server view *view-name oid-tree* {**included | excluded**}

no snmp-server view *view-name*

Parameter

Parameter	Description
view-name	Updates or creates the label of a view.
oid-tree	Means the object IDs of the ASN.1 sub-tree that must be contained or excepted from a view. The identifier sub-tree is used to designate a numeral-contained string, e.g., 1.3.6.2.4 or

	a **system** sub-tree. The sub-tree name can be found in all MIB trees.
included | excluded	Means the view type. The parameter “included” or “excluded” must be specified.

Default value

N/A

Command mode

Global configuration mode

Explanation

If other SNMP commands need a view as a parameter, you can use this command to create a view. By default, you need not define the view and you can see all the views, equivalent to Cisco-predefined everything views.

Example

The following example shows how to create the views of all objects in the MIB-II sub-tree.

snmp-server view mib2 mib-2 included

The following example shows how to create the views of all objects, including those objects in the system group.

snmp-server view phred system included

The following example shows how to create the views of all objects that includes the objects in the system groups but excludes the objects in system7 and interface 1.

snmp-server view agon system included
snmp-server view agon system.7 excluded

Related command

snmp-server community

5.1.12 snmp-server source-addr

To specify a source address for answering all SNMP requests, run the second one of the following two commands in global configuration mode. To cancel this address, run the second one of the following commands.

snmp-server source-addr *a.b.c.d*

no snmp-server source-addr

Parameter

Parameter	Description
a.b.c.d	Means the source address for all SNMP requests to be answered.

Default value

The default source address is the nearest routing address.

Command mode

Global configuration mode

Explanation

When the SNMP server transmits an SNMP request, you can run this command to designate a special source address.

Example

The following example shows how to designate the IP address “1.2.3.4” of the designated interface as the source address of all SNMP packets.

snmp-server source-addr 1.2.3.4

Related command

N/A

5.1.13 snmp-server udp-port

To specify the port number for the SNMP agent to receive packets, run the following first command in global configuration mode.

snmp-server udp-port *portnum*

no snmp-server udp-port

Parameter

Parameter	Description
udp-port	Stands for the ID of the destination port to which SNMP traps are sent, which cannot be a command port ID.

Default value

It is the listening port of SNMP agent by default, that is, port 162.

Command mode

Global configuration mode

Explanation

The SNMP agent will listen to this port when SNMP server transmits SNMP packets.

Example

The following example shows how to specify the listening port of SNMP agent to port 1234.

snmp-server udp-port 1234

Related command

N/A

5.1.14 snmp-server encryption

TO display the configured SNMP community, the SHA encryption password and the MD5 encryption password, run **snmp-server encryption** in global mode. This command is a once-for-all command, which cannot be saved or canceled by its negative form.

snmp-server encryption

Parameter

N/A

Default value

The default settings is to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text.

Command mode

Global configuration mode

Explanation

This command is used to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text. In this way, the security of the password is guaranteed.

Example

The following example shows how to show in the plain text the SNMP community, the SHA encryption password and the MD5 encryption password, which are set for host 90.0.0.3.

snmp-server encryption

Related command

snmp-server community

snmp-server user

5.1.15 snmp-server trap-add-hostname

snmp-server trap-add-hostname

no snmp-server trap-add-hostname

Parameter

None

Default value

Command mode

Global configuration mode

5.1.16 snmp-server trap-logs

snmp-server trap-logs

no snmp-server trap-logs

Parameter

The command has no parameters or keywords.

Command mode

Global configuration mode

Chapter 6 AAA Authentication Configuration Commands

6.1 AAA Authentication Configuration Commands

This chapter describes the commands used to configure AAA authentication methods. Authentication identifies users before they are allowed access to the network and network services.

For information on how to configure authentication using AAA methods, refer to the "Configuring Authentication" chapter. For configuration examples using the commands in this chapter, refer to the "Authentication Examples" section located at the end of the "Configuring Authentication" chapter.

AAA Authentication Configuration Commands include：

- aaa authentication enable default
- aaa authentication login
- aaa authentication password-prompt
- aaa authentication username-prompt
- aaa group server
- debug aaa authentication
- enable password
- server
- service_password-encryption
- username

6.1.1 aaa authentication enable default

To enable AAA authentication to determine if a user can access the privileged command level, use the aaa authentication enable default global configuration command. Use the no form of this command to disable this authentication method.

aaa authentication enable default *method1* [*method2...*]

no aaa authentication enable default *method1* [*method2...*]

parameter

parameter	description
method	At least one of the keywords described in Table 1.

default

If the default list is not set, only the enable password is checked. This has the same effect as the following command:

aaa authentication enable default enable

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway.

command mode

Global configuration

instruction

Use the aaa authentication enable default command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 1. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

Table 1-1 aaa authentication enable default Methods

Keyword	Description
group name	Uses the server group for authentication.
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
group radius	Uses RADIUS authentication.

example

The following example creates an authentication list that first tries to contact a TACACS+ server. If no server can be found, AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

aaa authentication enable default line enable none

related commands

enable password

6.1.2 aaa authentication login

To set authentication, authorization, and accounting (AAA)authentication at login, use the aaa authentication login command in global configuration mode. To disable AAA authentication, use the no form of this command.

aaa authentication login {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication login {**default** | *list-name*} *method1* [*method2...*]

parameter

parameter	description
Default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method	At least one of the keywords described in Table 2.

default

If the default list is not set, only the local user database is checked. This has the same effect as the following command:

aaa authentication login default none

command mode

Global configuration

instruction

The default and optional list names that you create with the aaa authentication login command are used with the login authentication command.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed.

Table 1-2 AAA authentication login Methods

Keyword	Description
enable	Uses the enable password for authentication.
group	Uses the server group for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Used RADIUS for authentication.

example

The following example creates an AAA authentication list called TEST. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+

returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

aaa authentication login TEST tacacs+ enable none

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

aaa authentication login default tacacs+ enable none

related commands

none

6.1.3 aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt global configuration command. Use the no form of this command to return to the default password prompt text.

aaa authentication password-prompt *text-string*

no aaa authentication password-prompt *text-string*

parameter

parameter	description
test-string	String of text that will be displayed when the user is prompted to enter a password.

default

There is no user-defined text-string, and the password prompt appears as "Password."

command mode

Global configuration

instruction

Use the aaa authentication password-prompt command to change the default text that the software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The no form of this command returns the password prompt to the default value:

Password:

The aaa authentication password-prompt command does not change any dialog that is supplied by a remote TACACS+ server.

example

The following example changes the text for the username prompt:

aaa authentication password-prompt YourPassword:

related commands

aaa authentication username-prompt

enable password

6.1.4 aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the aaa authentication username-prompt global configuration command. Use the no form of this command to return to the default username prompt text.

aaa authentication username-prompt text-string

no aaa authentication username-prompt text-string

parameter

parameter	description
text-string	String of text that will be displayed when the user is prompted to enter a username.

default

There is no user-defined text-string, and the username prompt appears as "Username."

command mode

Global configuration

instruction

Use the aaa authentication username-prompt command to change the default text that the software displays when prompting a user to enter a username. The no form of this command returns the username prompt to the default value:

Username:

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the aaa authentication username-prompt command will not change the username prompt text in these instances.

Note：

The aaa authentication username-prompt command does not change any dialog that is supplied by a remote TACACS+ server.

example

The following example changes the text for the username prompt:

aaa authentication username-prompt YourUsernam:

related commands

aaa authentication password-prompt

6.1.5 aaa group server

To group different RADIUS server hosts into distinct lists and distinct methods, enter the aaa group server radius command in global configuration mode. To remove a group server from the configuration list, enter the no form of this command.

aaa group server radius *group-name*

no aaa group server radius *group-name*

parameter

parameter	description
group-name	Character string used to name the group of servers.

default

No default behavior or values.

command mode

Global configuration

instruction

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

Example

The following example adds a radius server group named radius-group:

aaa group server radius radius-group

related commands

server

6.1.6 debug aaa authentication

To display information on authentication, authorization, and accounting (AAA) TACACS+ authentication, use the debug aaa authentication command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug aaa authentication

no debug aaa authentication

parameter

none

default

disabled

command mode

EXEC

instruction

Use this command to learn the methods of authentication being used and the results of these methods.

example

The following is sample output from the debug aaa authentication command.

switch#debug aaa authentication
AAA: Authen start (0x1f74208), user=, authen_type=ASCII, priv=0, method-list=default
AAA: Use authen method LOCAL (0x1f74208).
AAA: Authen CONT, need username.
AAA: Authen CONT, need password.
AAA: Authen ERROR (0x1f74208)! Use next method.
AAA: Authen FAIL(0x1f74208)! Method-list polling finish.

Output information	description
Authen start (0x1f74208), user=, authen_type=ASCII, priv=0, method-list=default	The authentication starts and the username is unknown. Uses ASCII-type authentication. The privileged level required for the user to enter is 0. Uses the default authentication method list. UserID = 0x1f74208
Use authen method LOCAL (0x1f74208)	Uses local authentication method. UserID = 0x1f74208
Authen CONT, need username	Prompts for username
Authen CONT, need password	Prompts for password
Authen ERROR (0x1f74208)! Use next	Indicates that the local authentication fails,

method	Uses the next method in the list.
Authen FAIL(0x1f74208)! Method-list polling finish	Method-list polling is finished. The authentication fails.

related commands

none

6.1.7 enable password

To set a local password to control access to various privilege levels, use the enable password command in global configuration mode. To remove the password requirement, use the no form of this command.

enable password { *password* | [*encryption-type*] *encrypted-password* } [level *number*]

no enable password [level *number*]

parameter

parameter	description
password	Password users type to enter enable mode.
encryption-type	Algorithm used to encrypt the password.
encrypted-password	Encrypted password you enter, copied from another router configuration.
level	Level for which the password applies.
number	Number between 1 and 15 that specifies the privilege level for the user.

default

No password is defined.

command mode

Global configuration

instruction

Can not have spaces in the password that the switch configures. When using the enable password command, you cannot input space if you enter a clear text password. The length of the clear text password cannot exceed 126 characters.

The default level parameter is 15 without inputting the level parameter. If a privilege level is not configured password, then no authentication is performed when a user entering this priviledge level.

Our switch system only supports two types of encryption. The encryption type is 0 and 7 respectively. Parameter O indicates no password is defined and you enter a clear text password in the following encrypted-password blank. Parameter 7 indicates a

self-defined algorithm is used for encryption and you enter encrypted text password in the following encrypted-password blank. This encryted text password can be copied from the configuration file of other switch.

example

The following example adds password clever for the privige level 10, uses encryption-type 0, that is, the clear text password:

enable password 0 clever level 10

The following example adds password Oscar for the default privilege (15), uses encryption-type 7, that is, the encrypted text password:

enable password 7 074A05190326

Assuming the encrypted text password of Oscar is 074A05190326, which is obtained from the configuration file of other switch.

related commands

aaa authentication enable default

service password-encryption

6.1.8 server

To add a server in the AAA server group, use the server command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the no form of this command.

server A.B.C.D

no server A.B.C.D

parameter

parameter	description
A.B.C.D	IP address of the server.

default

No server

command mode

Server-group configuration

instruction

You can add 20 different servers in a server group at most.

example

The following example adds a server at 12.1.1.1 to the server group:

server 12.1.1.1

related commands

aaa group server

6.1.9 service password-encryption

To encrypt passwords, use the service password-encryption command in global configuration mode. To restore the default, use the no form of this command.

service password-encryption

no service password-encryption

parameter

none

default

No encryption

command mode

global configuration

instruction

Currently in the realization of our switch system, this command is related to username password, enable password and password. If this command is not configured on the switch (namely default state), and the system uses the clear text storage method in the above three commands, then the configured clear text of the password can be displayed in the show running-config command. If this command is configured on the switch, then the configured password of the above three commands will be encrypted, then the configured clear text of the password cannot be displayed in the show running-config command, even using the no service password-encryption cannot restore the clear text of the password. Please make sure of the configured password before using this command for encryption. The no service password-encryption command only has effect on the password configured by the service password-encryption command.

example

Use the following command to encrypt for the configured clear text password and also to encrypt for the clear text password that configured after using this command.

switch_config#service password-encryption

related commands

username username password
enable password

password

6.1.10 username

To establish a username-based authentication system, use the username command in global configuration mode. Use the no form of this command to remove an established username-based authentication.

username *username* [**password** { *password* | [encryption-type] *encrypted-password* }] [**user-maxlinks** *number*] [**autocommand** *command*]

no username *username*

parameter

parameter	description
Username	Username character string
password	Password a user enters.
password	Clear text of the password character string
encryption-type	Encryption type
encrypted-password	Encrypted password a user enters.
user-maxlinks	Limits the user's number of inbound links.
number	Link number that established simultaneously.
autocommand	Causes the specified command to be issued automatically after the user logs in. The autocommand must be used in the end of the command line.
command	Executes automatically command character string

default

No username-based authentication system is established.

command mode

global configuration

instruction

The password is considered as empty character string when there is no password parameter. The trust-host will bind the user to the specified host. This user and other hosts cannot pass authentication when logging in switch. The user-maxlinks command limit the user's number of inbound links. User can use the show users command to check which kind of authentication that each online user passes.

White spaces are not allowed in the configured password of our switch. This also applies to the enable password command.

Our switch system only supports two types of encryption. The encryption type is 0 and 7 respectively. Parameter O indicates no password is defined and you enter a clear text password in the following encrypted-password blank. Parameter 7 indicates a

self-defined algorithm is used for encryption and you enter encrypted text password in the following encrypted-password blank. This encryted text password can be copied from the configuration file of other switch.

example

The following example adds a local user, its username is someone, its password is someother:

username someone password someother

The following example adds a local user, its user name is Oscar, its password is Joan, uses encryption-type 7, that is, the encrypted text password:

enable password 7 1105718265

Assuming the encrypted text password is 1105718265, which is obtained from the configuration file of other switch.

related commands

aaa authentication login

Chapter 7 RADIUS Configuration Commands

This chapter describes the commands used to configure RADIUS. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

For information on how to configure RADIUS, refer to the chapter "Configuring RADIUS".

7.1 RADIUS Configuration Commands

RADIUS Configuration Commands include：

- debug radius
- ip radius source-interface
- radius-server challenge-noecho
- radius-server deadtime
- radius-server host
- radius-server optional-passwords
- radius-server key
- radius-server retransmit
- radius-server timeout
- radius-server vsa send

7.1.1 debug radius

To display information associated with RADIUS, use the debug radius command in EXEC mode. To disable debugging output, use the no form of this command.

debug radius {*event* | *packet*}

no debug radius {*event* | *packet*}

parameter

Parameter	description
Event	Displays radius event
Packet	Displays radius packet.

default

none

command mode

EXEC

instruction

Use this command to debug network system to locate the authentication failure reason.

Switch#debug radius event

RADIUS:return message to aaa, Give me your username

RADIUS:return message to aaa, Give me your password

RADIUS:inital transmit access-request [4] to 192.168.20.126 1812 <length=70>

RADIUS:retransmit access-request [4] to 192.168.20.126 1812 <length=70>

RADIUS:retransmit access-request [4] to 192.168.20.126 1812 <length=70>

RADIUS:192.168.20.126 is dead to response [4]

RADIUS:Have tried all servers，return error to aaa

output information	description
return message to aaa, Give me your username	It needs username
return message to aaa, Give me your password	It needs the password that corresponds to the username
inital transmit access-request [4] to 192.168.20.126 1812 <length=70>	Sends authentication request to RADIUS server for the first time. The server address is 192.168.20.126, port number 1812, packet length 70
retransmit access-request [4] to 192.168.20.126 1812 <length=70>	The server doesn't respond to the request in time. The authentication request will be retransmitted.
192.168.20.126 is dead to response [4]	The server doesn't respond after many times of retransmittion. This serve is marked as dead.
Have tried all servers，return error to aaa	RADIUS cannot complete this authentication and returns to error.

example

The following example debugs RADIUS event:

debug radius event

7.1.2 ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the ip radius source-interface command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.

ip radius source-interface *interface-name*

no ip radius source-interface

parameter

Parameter	description
interface-name	Name of the interface that RADIUS uses for all of its outgoing packets.

default

No default behavior or values

command mode

global configuration

instruction

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the subinterface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses.

This command is especially useful in cases where the router has many subinterfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

The specified subinterface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in the down state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the subinterface to the up state.

example

The following example shows how to configure RADIUS to use the IP address of vlan 1 for all outgoing RADIUS packets:

ip radius source-interface vlan 1

related commands

ip tacacs source-interface

7.1.3 radius-server challenge-noecho

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the radius-server challenge-noecho command in global configuration mode. To return to the default condition, use the no form of this command.

radius-server challenge-noecho

no radius-server challenge-noecho

parameter

none

default

All user responses to Access-Challenge packets are echoed to the screen.

command mode

global configuration

instruction

none

example

radius-server challenge-noecho

7.1.4 radius-server deadtime

To improve RADIUS response times when some servers might be unavailable and cause the unavailable servers to be skipped immediately, use the radius-server deadtime command in global configuration mode. To set dead-time to 0, use the no form of this command.

radius-server deadtime minutes

no radius-server deadtime

parameter

Parameter	description
Minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).

default

Dead time is set to 0.

command mode

global configuration

instruction

Use this command to cause the software to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as "dead" is skipped by additional requests for the duration of minutes or unless there are no servers not marked "dead."

example

The following example specifies five minutes deadtime for RADIUS servers that fail to respond to authentication requests:

radius-server deadtime 5

related commands

radius-server host

radius-server retransmit

radius-server timeout

7.1.5 radius-server host

To specify a RADIUS server host, use the radius-server host command in global configuration mode. To delete the specified RADIUS host, use the no form of this command.

radius-server host *ip-address* [*auth-port port-number1*] [acct-port *port-number2*]

no radius-server host ip-address

parameter

Parameter	Description
ip-address	IP address of the RADIUS server host.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
port-number1	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
port-number2	(Optional) Specifies the UDP destination port for accounting requests; the host is not used for accounting if set to 0.

default

No RADIUS host is specified;

command mode

global configuration

instruction

You can use multiple radius-server host commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

example

The following example specifies host 1.1.1.1 as the RADIUS server and uses default ports for both accounting and authentication

radius-server host 1.1.1.1

The following example specifies port 12 as the destination port for authentication requests and port 16 as the destination port for accounting requests on the RADIUS host named host1:

radius-server host 1.2.1.2 auth-port 12 acct-port 16

related commands

aaa authentication

radius-server key

tacacs server

username

7.1.6 radius-server optional-passwords

To specify that the first RADIUS request to a RADIUS server be made without password verification, use the radius-server optional-passwords command in global configuration mode. To restore the default, use the no form of this command.

radius-server optional-passwords

no radius-server optional-passwords

parameter

This command has no parameters or keywords.

default

disabled

command mode

global configuration

instruction

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

example

The following example configures the first login to not require RADIUS verification:

radius-server optional-passwords

related commands

radius-server host

7.1.7 radius-server key

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the radius-server key command in global configuration mode. To disable the key, use the no form of this command.

radius-server key *string*

no radius-server key

parameter

Parameter	description
String	Spedifies the encrypted key. This encrypted key must match the encrypted key that RADIUS server uses.

default

The encrypted key is the empty character string.

command mode

Global configuration

instruction

The key entered must match the key used on the RADIUS daemon. All leading spaces are ignored, and all white spaces cannot be included in the encrypted key.

example

The following example sets the encryption key to " firstime ":

radius-server key firstime

related commands

radius-server host

tacacs server

username

7.1.8 radius-server retransmit

To specify the number of times the software searches the list of RADIUS server hosts before giving up, use the radius-server retransmit command in global configuration mode. To disable retransmission, use the no form of this command.

radius-server retransmit *retries*

no radius-server retransmit

parameter

parameter	description
retries	Maximum number of retransmission attempts. The default is 3 attempts.

default

3 attemps

command mode

global configuration

instruction

This command is generally used with the radius-server timeout command, indicating the interval for which a router waits for a server host to reply before timing out and the times of retry after timing out.

example

The following example specifies a retransmit counter value of five times:

radius-server retransmit 5

related commands

radius-server timeout

7.1.9 radius-server timeout

To set the interval for which a router waits for a server host to reply, use the radius-server timeout command in global configuration mode. To restore the default, use the no form of this command.

radius-server timeout *seconds*

no radius-server timeout

parameter

parameter	description
seconds	Number that specifies the timeout interval, in seconds. The default is 5 seconds.

default

5 seconds

command mode

global configuration

instruction

This command is generally used with the radius-server retransmit command.

example

Use this command to set the number of seconds a router waits for a server host to reply before timing out.

radius-server timeout 10

related commands

none

7.1.10 radius-server vsa send

To configure the network access server to recognize and use vendor-specific attributes, use the radius-server vsa send command. To restore the default, use the no form of this command.

radius-server vsa send [**authentication**]

no radius-server vsa send [**authentication**]

parameter

parameter	description
authentication	(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

default

disabled

command mode

global configuration

instruction

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The radius-server vsa send command enables the network access server to recognize and use both accounting and authentication vendor-specific attributes. Use the accounting keyword with the radius-server vsa send command to limit the set of recognized vendor-specific attributes to just accounting attributes. Use the authentication keyword with the radius-server vsa send command to limit the set of recognized vendor-specific attributes to just authentication attributes.

example

The following example configures the network access server to recognize and use vendor-specific accounting attributes:

radius-server vsa send accounting

related commands

radius-server host

Chapter 8 WEB Configuration Commands

8.1 ip http language

Syntax

ip http language {chinese | english}

It is used to set the prompt language when a command is configured.

Parameter

Parameter	Remarks
chinese	Sets the language to Chinese.
english	Sets the language to English.

Default value

N/A

Remarks

This command is configured in global configuration mode.

Example

The following example shows how to set the language to English.

Switch_config#ip http language english

8.2 ip http port

Syntax

ip http port { *portNumber* }

It is used to set the HTTP port.

no ip http port

It is used to resume the HTTP port to be the default port 80.

Parameter

Parameter	Remarks
portNumber	Means the HTTP port's valid range is from 1 to 65535.

Default value

80

Remarks

This command is configured in global configuration mode.

Example

The following example shows how to set the HTTP port to 1234.

Switch_config#ip http port 1234

8.3 ip http secure-port

Syntax

ip http secure-port {*portNumber*}

It is used to set the HTTPS port.

no ip http secure-port

It is used to resume the HTTPS port to be the default port 443.

Parameter

Parameter	Remarks
portNumber	Means the HTTPS port's valid range is from 1 to 65535.

Default value

443

Remarks

This command is configured in global configuration mode.

Example

The following example shows how to set the HTTPS port to 1234.

Switch_config# ip http secure-port 1234

8.4 ip http server

Syntax

[no] ip http server

It is used to set the HTTP service.

Remarks

This command is configured in global configuration mode.

Example

It is used to set the HTTP service.

Switch_config# ip http server

8.5 ip http http-access enable

Syntax

[no] ip http http-access enable

It is used to set the HTTP access mode.

Remarks

This command is set in global configuration mode and used to access the website, which starts with http://.

Example

The following example shows how to set the HTTP access mode.

Switch_config# ip http http-access enable

8.6 ip http ssl-access enable

Syntax

[no] ip http ssl-access enable

It is used to set the HTTPS access mode.

Remarks

This command is set in global configuration mode and used to access the website, which starts with http://.

Example

The following example shows how to set the HTTPS access mode.

Switch_config# ip http ssl-access enable

8.7 ip http web max-vlan

Syntax

ip http web max-vlan { *max-vlan* }

It is used to set the maximum number of VLAN entries displayed in a web page.

no ip http web max-vlan

It is used to resume the default maximum number of VLAN entries to 100.

Parameter

Parameter	Remarks
max-vlan	Means the maximum number of vlan entries in the web page, which ranges from 1 to 4094.

Default value

100

Remarks

This command is configured in global configuration mode.

Example

The following example shows how to set the maximum number of VLAN entries displayed in a web page to 123.

Switch_config# ip http web max-vlan 123

8.8 ip http web igmp-groups

Syntax

ip http web igmp-groups { *igmp-groups* }

It is used to set the maximum number of multicast entries displayed in a web page.

no ip http web igmp-groups

It is used to resume the default maximum number of multicast entries to 15.

Parameter

Parameter	Remarks
igmp-groups	Means the maximum number of multicast entries in the web page, which ranges from 1 to 100.

Default value

15

Remarks

This command is configured in global configuration mode.

Example

The following example shows how to set the maximum number of multicast entries displayed in a web page to 12.

Switch_config#ip http web igmp-groups 12

8.9 show ip http

Syntax

show ip http

Remarks

It is used to browse whether the HTTP server is enabled.

Example

Switch_config#show ip http

Http server is running

Chapter 9 Interface Configuration Commands

9.1 Interface Configuration Commands

The following are interface configuration commands:

- Interface
- description
- bandwidth
- delay
- shutdown
- show interface
- show running-config interface

9.1.1 interface

Syntax

[no] interface *port*

To enter the interface configuration mode, run the above-mentioned command. If the logical port is inexistent, you have to create this port first and then enter the port mode. If the physical port is inexistent, the command will fail to be executed. The negative form of this command has different functions for the physical port and the logical port.

The **no interface physical-port** command is used to resume the default settings of the physical port.

The **no interface *logical-port*** command is used to delete the logical port.

Parameter

Parameter	Description
Port	Stands for the existent physical or logical port.

Default value

The default mode is not the port mode.

Remarks

When you execute this command in configuration mode, you have to enable this command to be in port configuration mode first. When the port command is configured, you shall use the **exit** command to exit from the port mode.

Example

The following example shows how to enter the port mode of port g0/1.

Switch_config#
Switch_config#interface gigaEthernet0/1
Switch_config_g0/1#exit
Switch_config#

9.1.2 description

Syntax

[no] description *line*

To set the description information of a port, run the above-mentioned command.

Parameter

Parameter	Description
line	Stands for the character string of the description information, among which space may exist.

Default value

There is no description information by default.

Remarks

This command is configured in port configuration mode.

Example

The following example shows how to set the description information of port g0/1 to **up link**.

Switch_config# interface gigaEthernet0/1
Switch_config_g0/1# description uplink

9.1.3 bandwidth

Syntax

[no] bandwidth *kilobps*

To set the bandwidth of an interface, ran the above-mentioned command.

Parameter

Parameter	Description
kilobps	Means the bandwidth of port, which ranges from 1 to 10000000 kbps.

Default value

The default bandwidths of the 100M port, gigabit port and 10G port are 100000kbps, 1000000kbps and 10000000kbps respectively.

Remarks

This command is configured in port configuration mode.

Note:

The configured bandwidth does not mean the actual bandwidth of a port, but is used by some protocol to calculate the port cost.

Example

The following example shows how to set port g0/1 to 10000000.

Switch_config # interface gigaEthernet0/1
Switch_config_g0/1# bandwidth 10000000

9.1.4 delay

Syntax

[no] delay *tensofmicroseconds*

To set the delay of an interface, run the above-mentioned command.

Parameter

Parameter	Description

tensofmicroseconds	端口延迟，取值范围为1-10000000 （十微秒）。

Default value

The default value of the delay is 1.

Remarks

This command is configured in port configuration mode.

Example

The following example shows how to set the delay of an interface to 10.

```
Switch_config_g0/1# delay 10
```

9.1.5 shutdown

Syntax

[no] shutdown

To close a port, run **shutdown**; to restart a port, run **no shutdown**.

Parameter

N/A

Default value

The physical port is in **enabled** status by default.

Remarks

This command can be used in port mode to open or close a port.

Example

The following example shows how to enable port g0/1.

```
Switch_config_g0/1#
Switch_config_g0/1# no shutdown
Switch_config_g0/1#
```

9.1.6 show interface

Syntax

show interface <*port*>

To browse the state of an interface, run the above-mentioned command.

Parameter

Parameter	Description
Port	Name of an interface If a specific port is not in the command, the system will show the statuses of all ports.

Default value

N/A

Remarks

This command can be used in EXEC and configuration modes to show the physical status and packet reception statistics of a port.

Example

The following example shows the information about port g0/1:

```
Switch_config# show interface gigaEthernet 0/1
GigaEthernet0/1 is administratively down, line protocol is down
  Hardware is Giga-Combo-FX, address is 00e0.0fe4.d083 (bia 00e0.0fe4.d083)
  MTU 1500 bytes, BW 1000000 kbit, DLY 10 usec
  Encapsulation ARPA
  Auto-duplex,    Auto-speed
  flow-control off
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
     Received 0 packets, 0 bytes
     0 broadcasts, 0 multicasts
     0 discard, 0 error, 0 PAUSE
     0 align, 0 FCS, 0 symbol
     0 jabber, 0 oversize, 0 undersize
     0 carriersense, 0 collision, 0 fragment
     0 L3 packets, 0 discards, 0 Header errors
     Transmited 0 packets, 0 bytes
     0 broadcasts, 0 multicasts
     0 discard, 0 error, 0 PAUSE
```

0 sqettest, 0 deferred
0 single, 0 multiple, 0 excessive, 0 late
0 L3 forwards

9.1.7 show running-config interface

Syntax

show running-config interface *port*

To display the settings of a port, run the above-mentioned command.

Parameter

Parameter	Description
Port	Stands for the existent port.

Default value

N/A

Remarks

This command can be executed in EXEC or configuration mode to browse the settings of a port.

Example

The following example shows the settings of port g1/1:

```
Switch_config#show running-config interface g0/1
Building configuration...

Current configuration:
!
interface GigaEthernet0/1
  shutdown
  description uplink
  bandwidth 10000000
  delay 10
Switch_config#
```

9.2 Configuration Example

The following example shows how to create a VLAN port, set its description information and IP address and browse the status and settings of this port.

```
Switch_config#

Switch_config# interface vlan1

Switch_config_v1# description uplink

Switch_config_v1#

Switch_config_v1# ip address 192.168.1.1 255.255.255.0

Switch_config_v1# exit

Switch_config#

Switch_config# show running-config interface vlan1

Building configuration...

Current configuration:

!

interface VLAN1

 description uplink

 ip address 192.168.1.1 255.255.255.0

Switch_config# show interface vlan1

VLAN1 is up, line protocol is down

   Description uplink

   Hardware is EtherSVI, Address is 00e0.0fe4.d06a(00e0.0fe4.d06a)

   Interface address is 192.168.1.1/24

   MTU 1500 bytes, BW 1000000 kbit, DLY 2000 usec

   Encapsulation ARPA

   ARP type: ARPA, ARP timeout 04:00:00

   Peak input rate 0 pps, output 0 pps

      0 packets input, 0 bytes

      Received 0 broadcasts, 0 multicasts

      0 mpls unicasts, 0 mpls multicasts, 0 mpls input discards
```

0 input errors, 0 input discards

0 packets output, 0 bytes

Transmited 0 broadcasts, 0 multicasts

0 mpls unicasts, 0 mpls multicasts, 0 mpls output discards

0 output errors, 0 discards

Switch_config#

Chapter 10 Interface Range Command

10.1 Interface Range

Description

interface range *type slot*/<*port1 - port2* | port3>[<port1 - port2|port3>]

Parameter

Name	Description	Description
type	Interface type	All legal interface types except for the management interface on the main contril board of the rack-mounted switch.
slot	Slot number	All legal slot numbers
port1	Beginning value of the port number	All legal port numbers on the slot.
port2	Ending value of the port number	All legal port numbers on the slot except for port 1.
port3	A single port.	All legal port numbers on the slot.

Default

none

Instruction

Use this command to enter the interface range mode.

Example

Use the following command to enter the enterface configuration mode, including slot 0 and fast Ethernet port 1,2,3,6,8,10,11,12:

switch_config#interface range 1 - 3 , 6 , 8 , 10 - 12

switch_config_if_range#

Chapter 11 Interface Physical Characteristic Configuration Commands

11.1 Interface Physical Characteristic Configuration Commands

Interface physical characteristic configuration commands include：

- speed
- duplex
- flow-control

11.1.1 speed

Description

To set the speed rate of the port, run **speed**.

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

no speed

Parameter

Parameter	Description
10, 100, 1000	Configures the interface to transmit at 10M、100M、1000M。
auto	Turns on the Fast Ethernet auto-negotiation capability.

Default

TX interface is auto-negotiation operation, gigabit TX interface is 1000M, gigabit optical interface is 1000M.

Instruction

Use this command in layer-2 interface configuration mode.

Note：

The optical interface speed is fixed. The **auto** parameter following the **speed** command indicates that the auto-negotiation feature can be enabled on this interface. If there is no **auto** parameter behind the **speed** command, the auto-negotiation cannot be configured on the interface.

Example

The following example sets the interface g0/1 speed to 100M:

Switch (config)# interface GigaEthernet0/1
Switch (Switch_config_g0/1)# speed 100

11.1.2 duplex

Description

To configure the duplex operation on an interface, use the **duplex** command.

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

no duplex

Parameter

Parameter	Description
auto	Specifies the auto-negotiation operation.
full	Specifies the full-duplex operation.
half	Specifies the half-duplex operation.

Default

The **Tx** interface is for auto-negotiation operation, while the optical interface is for full-duplex operation.

Instruction

Use this command in the layer 2 configuration mode.

Note：

The duplex operation of the optical interface is fixed, that is, full-duplex operation.

Example

The following example configures interface g0/1 to full-duplex operation:

```
Switch (config)# interface GigaEthernet0/1
Switch (config-if)# duplex full
```

11.1.3 flow control

Description

To configure flow control on an interface, use the **flow control** command. Use the no form of this command to disable the flow control.

flow-control{*on* | *off*}

no flow-control

Parameter

Parameter	Description
on	Enables flow control.
off	Disables flow control.

Default

Disabled

Instruction

Use this command in the layer 2 configuration mode.

Example

The following example enables the flow-control on an interface:

```
Switch (config-if)# flow-control on
```

Chapter 12 Port Additional Characteristics Configuration Commands

Chapter 12.1 Port Security

12.1.1 switchport port-security mode static

Command description

switchport port-security mode static {**accept** | **reject**}

no switchport port-security mode

Set the static mode of the security port.

12.1.2 switchport port-security mode dynamic

Command description

switchport port-security mode dynamic

no switchport port-security mode

Add/delete the dynamic mode of the security port.

12.1.3 switchport port-security static mac-address

Command description

switchport port-security static mac-address *mac-addr*

no switchport port-security static mac-address

Configure the static MAC address of the security port.

12.1.4 switchport port-security dynamic maximum

Command description

switchport port-security dynamic maximum *value*

no switchport port-security dynamic maximum

Add/delete the maximum number of dynamic MAC addresses of the security port.

Chapter 12.2 Port Protection

12.2.1 switchport protected

Command description

[**no**] **switchport protected**

Configure the port isolation function.

Parameter

None

Default

The port is not isolated.

Explanation

The command must be configured in layer-2 port configuration mode.

Example

Configure port f0/1 not to forward the unknown unicast frame.

Switch(config)# interface fastethernet0/1

Switch(config-if)# switchport protected

Chapter 12.3 Port Storm Control

12.3.1 storm-control

Command description

Configure the storm control function of the port.

storm-control {**broadcast** | **multicast** | **unicast**} **threshold** *count*

no storm-control {**broadcast** | **multicast** | **unicast**} **threshold** *count*

Parameter

Parameter	Description
broadcast | **multicast** | **unicast**	Defines the storm control of the broadcast, multicast and unicast.
threshold *count*	Defines the flow percent of the storm control. The **count** parameter defines the flow caps that lead to the storm. <1-127>, n*64Kbps(n<=28);(n-27)Mbps(n>28)

Default

The storm control function is not enabled.

Explanation

The command must be configured in layer-2 port configuration mode.

Example

Set the storm control of the unknown unicast frame on port f0/1 to 192 Kbps.

```
Switch(config)# interface fastethernet0/1
Switch(config-f0/1)# storm-control unicast   threshold 3
```

Chapter 12.4 Port Rate Limitation

12.4.1 switchport rate-limit

Command description

[**no**] **switchport rate-limit** *band* { **ingress**|**egress**}

Configure the flow rate limitation for the port.

Parameter

Parameter	Description
Band	Flow rate n*64Kbps(n<=28); (n-27)Mbps(n>28)
ingress	Functions at the incoming port.
egress	Functions at the outgoing port.

Default

The port has no port rate limitation.

Explanation

Layer-2 port configuration mode

Example

Set the incoming flow rate limitation on port f0/1 to 1M.

```
Switch(config)# interface f0/1
Switch(config-if)# switchport rate-limit 28 ingress
```

Chapter 13 Configuring Port Mirroring Commands

13.1 Port Mirroring Configuration Commands

The following are port mirroring configuration commands:

- mirror
- show mirror

13.1.1 mirror

Description

[**no**] **mirror session** *session_number* {**destination** {**interface** *interface-id* } | **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**] }

It is used to configure the command.

Parameters

Parameter	Description
session_number	Number of port mirroring, whose value is 1
destination	Information about the destination port mirroring
source	Information about the mirrored port
both | *rx* | *tx*	Data flow that will be mirrored **rx** means that the input data is mirrored. **tx** means that the output data is mirrored. **both** means that input and output data are mirrored.

Instruction

The command is configured in global configuration mode. S2524GT, S2524GX and S2516 only support the tx mirroring output of one port and the **both** dataflow of another port.

Example

Port g0/2 functions as the output mirror of port g0/1.

```
Switch(config)# mirror session 1 destination interface g0/2
Switch(config)# mirror session 1 source interface g0/1 tx
```

13.1.2 show mirror

Description

show mirror [session *session_number]*

It is used to display the port mirroring information.

Parameter

Parameter	Description
session_number	Number of port mirroring, whose value is 1

Default

None

Instruction

It is used to display the port mirroring information.

Example

All port mirroring information is displayed.

```
Switch# show mirror
Session 1
---------
Source Ports:
RX Only: g0/3
TX Only: None
Both: None
Source VLANs:
RX Only: None
TX Only: None
Both: None
```

Chapter 14 Power Over Ethernet Configuration Commands

14.1 POE Configuration Commands

14.1.1 show poe system

It is used to display the information about POE-related systems.

show poe system

Parameter

N/A

Default value

N/A

Command mode

Monitoring mode

Explanation

POE DRIVER: means the drive of the chip.

POE CHIP: means the detailed chip type.

POE Port Num: means the maximum POE ports.

PSE PowerManagement: means the power source management mode (automatic, preempt, non-preempt).

PSE Total Power: Total power of the power source equipment

PSE Usage Threshold: power alarm (it is set according to the percentage)

PSE Alarm Power: means the power alarm threshold.

PSE Lower-Port-Disable Power: The threshold of the power supply for the relatively high priority preempt, which is effective only in non-automatic mode

PSE Lower-Port-NoConnect Power: The threshold of the power supply to forbid the lower or same-level priority preempt, which is effective only in non-automatic mode

PSE Consumed Power: the used power consumption

PSE Peak Power: peak power of the power source equipment, which is effective when the power statistics is enabled

PSE Mib Notification: MIB notification occurs when the power supply for a port changes or the power changes.

PSE Temperature PSE: temperature of the chip

Example

Switch#show poe system

POE DRIVER:PETH PD69012 DRV

POE CHIP:PD69012

POE Port Num:24

PSE PowerManagement:Preemptive

PSE Total Power:80000 mW

PSE Usage Threshold:80%

PSE Alarm Power:64000 mW

PSE Lower-Port-Disable Power:62000 mW

PSE Lower-Port-NoConnect Power:44000 mW

PSE Consumed Power:47500 mW

PSE Peak Power:101300 mW

PSE Mib Notification:Disable

PSE Temperature:38 degree

Related command

N/A

14.1.2 show poe all

Displays the information description table of the POE port.

show poe all

Parameter

N/A

Default value

N/A

Command mode

Monitoring mode

Explanation

Port enabled/disabled: To enable or disable power supply for a port

Port Detection Statu: means the power supply state of a port, which may be disabled, searching-power or fault.

delivering-power: means the power supply is normal.

Port pairs: the ordering of the power line of a port, of which **signal** means the power supply by way of the signal line and **spare** that by way of the spare line

Port priority: means the priority for port's power supply and it from high to low is critical, high and low.

Example

Switch#show poe all

Port	Enable	Status	Pair	Priority
f0/3	enabled	disabled	signal	low
f0/4	enabled	disabled	signal	low
f0/2	enabled	disabled	signal	low
f0/1	enabled	disabled	signal	low
f0/5	enabled	disabled	signal	low
f0/6	enabled	disabled	signal	low
f0/7	enabled	disabled	signal	low
f0/8	enabled	disabled	signal	low
f0/9	enabled	searching	signal	high
f0/10	enabled	searching	signal	high
f0/11	enabled	searching	signal	high
f0/12	enabled	searching	signal	high
f0/13	enabled	delivering-power	signal	high
f0/14	enabled	searching	signal	high
f0/15	enabled	delivering-power	signal	high
f0/16	enabled	searching	signal	high
f0/17	enabled	disabled	signal	low
f0/18	enabled	disabled	signal	low
f0/19	enabled	disabled	signal	low
f0/20	enabled	disabled	signal	low
f0/21	enabled	disabled	signal	low
f0/22	enabled	delivering-power	signal	low
f0/23	enabled	delivering-power	signal	low
f0/24	enabled	delivering-power	signal	critical

Related command

N/A

14.1.3 show poe power

It is used to display the information about the power supply of all ports.

show poe power

Parameter

N/A

Default value

N/A

Command mode

Monitoring mode

Explanation

Max: means the maximum power limitation of a port.

Current: means the current power of a port.

Average: means the average power of a port, which is effective only when the power statistics table is enabled.

Peak: means the peak power of a port, which is effective when the power statistics is enabled.

Bottom: means the bottom power of a port, which is effective only when the power statistics table is enabled.

Example

Switch#show poe power

Port	Current	Max	Average	Peak	Bottom
f0/3	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/4	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/2	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/1	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/5	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/6	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/7	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/8	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/9	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/10	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/11	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/12	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/13	7600 mW	30000 mW	7620 mW	7800 mW	7600 mW
f0/14	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/15	7600 mW	30000 mW	7600 mW	7800 mW	7600 mW
f0/16	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/17	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/18	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/19	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/20	0 mW	30000 mW	0 mW	0 mW	0 mW

f0/21	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/22	15900 mW	30000 mW	15890 mW	16200 mW	14900 mW
f0/23	7700 mW	30000 mW	7780 mW	7800 mW	7700 mW
f0/24	8400 mW	30000 mW	9850 mW	22500 mW	6500 mW

Related command

N/A

14.1.4 show poe interface

It is used to display the detailed POE information of a designated port.

show poe interface *type slot/port*

Parameter

Parameter	Description
type	Interface type
slot	Slot ID
Port	Port ID

Default value

N/A

Command mode

Monitoring mode

Explanation

PSE Port Number: means the ID of an internal port.

Port Power Enabled: means to enable the power supply for a port.

Port Force Power: means to enable the forced power supply or the power supply for a low-priority port.

Port detection: the power supply state of a port, which may be disabled, searching-power or fault

Port Fault Status: means the error information about a port.

Port Last Disconnection Reason: means the reason of the latest power cutoff on a port.

Port pairs: means the ordering of the power line of a port, of which **signal** means the power supply by way of the signal line and **spare** that by way of the spare line.

Port IEEE Class: means the class of a port.

Port priority: means the priority for port's power supply and it from high to low is critical, high and low.

Port Current : stands for the present current on a interface.

Port Voltage: means the current voltage of a port, which cannot be shown by some chips.

Port Current Power: stands for the current power on an interface.

Port Average Power: means the average power of a port, which is effective only when the power statistics table is enabled.

Port Peak Power : means the peak power of a port, which is effective when the power statistics is enabled.

Port Bottom Power: means the bottom power of a port, which is effective only when the power statistics table is enabled.

Port Max Powe: means the maximum power limitation of a port.

Port PD Discription: stands for the description of a port.

Example

Switch#show poe interface f0/24

PSE Port Number : 23

Port Power Enabled : enable

Port Force Power : disable

Port Detection Status : delivering-power

Port Fault Status :

Port Last Disconnection Reason : Port was disabled

Port Pairs : signal

Port IEEE Class : 0

Port Priority : critical

Port Current : 163 mA

Port Current Power : 8400 mW

Port Average Power : 8440 mW

Port Peak Power : 22500 mW

Port Bottom Power : 6500 mW

Port Max Power : 30000 mW

Port PD Discription : AP

Related command

N/A

14.1.5 poe power-management

It is used to set the power supply management mode for a switch.

poe power-management {auto | preemptive | non-preemptive | lowDisable | lowNoConnect } *value*

Parameter

Parameter	Description
auto	Sets the power-supply management mode of a switch to **automatic**.
preemptive	Sets the power-supply management mode of a switch to **preemptive**.
non-preemptive	Sets the power-supply management mode of a switch to **non-preemptive**.
lowDisable	When the total power exceeds **lowDisable**, the port cannot be powered; when the total power is less than **lowDisable**, the power supply can go again. lowDisable = total power - value
lowNoConnect	When the total power exceeds **lowNoConnect**, those ports whose priorities are lower than or equal to the priority of the currently powered port, which is lowest priority among the powered ports, will be cut off from the power supply.lowNoConnect = lowDisable – value

Default value

The power supply management mode is **auto** by default.

Command mode

Global configuration mode

Explanation

Auto: The maximum power limitation of a port cannot be set and the port's power supported by the chip is considered by default as the maximum power.

The power-supply priority of a port cannot be set and the default priority of this port is **low**.

Preemptive: It is to enable the function of limiting the maximum power of a port.

It is also to enable the power supply priority of a port.

Non-preemptive: it is to enable the function of limiting the maximum power of a port.

It is also to enable the power supply priority of a port.

Preempt means that a new PD device will be normally powered by a high-priority power supply port if the new PD device is connected to this high-priority port in full load and at the same time the port with the lowest power-supply priority will be cut off from power supply.

Non-preempt means that the power supply port with high priority will be notified that a PD device has accessed when this port is connected to a PD device in full load.

Example

The following example shows how to set the power supply management mode to **preemptive**.

Switch_config#poe power-management preemptive

Switch_config#poe power-management lowDisable 18000

Switch_config#poe power-management lowNoConnect 18000

Related command

poe max-power

poe priority

14.1.6 poe led-time

It is used to set the lasting time of the LED in PoE mode.

poe led-time *time*

no poe led-time

Parameter

Parameter	Description
time	Unit: second

Default value

The lasting time of LED in POE mode is 30 seconds.

Command mode

Global configuration mode

Explanation

The **no poe led-time** command can set the lasting time back to the default value.

Example

The following example shows how to set the lasting time to 10 seconds.

Switch_config#poe led-time 10

Related command

N/A

14.1.7 poe mib notification-stop

To stop sending the trap notification to users when power supply changes or power alarm occurs, run the following command:

poe mib notification-stop

no poe mib notification-stop

Parameter

N/A

Default value

In the default settings, the change of power supply or the occurrence of power alarm will lead the system to send the trap notification to users.

Command mode

Global configuration mode

Explanation

The “no” form of this command can be used to resume the default settings.

Example

The following example shows how to stop sending the trap notification to users when power supply changes or power alarm occurs:

Switch_config#poe mib notification-stop

Related command

N/A

14.1.8 poe pse-unprotect

To set power supply protection for a port, run the following command:

poe pse-unprotect

no poe pse-unprotect

Parameter

N/A

Default value

The power supply protection for ports is enabled by default.

Command mode

Global configuration mode

Explanation

The “no” form of this command can be used to resume the default settings.

Example

The following example shows how to disable the power supply protection:

Switch_config# poe pse-unprotect

Related command

N/A

14.1.9 poe counter value

To enable the power statistics globally, run the following command:

poe counter *value*

no poe counter

Parameter

Parameter	Description
value	Stands for the sampling interval, whose unit is second.

Default value

The power statistics is disabled by default.

Command mode

Global configuration mode

Explanation

The “no” form of this command can be used to resume the default settings.

Example

The following example shows how to set the sampling interval of the power statistics to 5 seconds.

Switch_config# poe counter 5

Related command

N/A

14.1.10 poe threshold

Sets the percentage between alarm power and the total power.

poe threshold *value*

no poe threshold

Parameter

Parameter	Description
value	Sets the percentage between alarm power and the total power.

Default value

The default percentage between alarm power and the total power is 100%.

Command mode

Global configuration mode

Explanation

The “no” form of this command can be used to resume the default settings.

Example

The following example shows how to set the percentage between the alarm power and the total power to 50%:

Switch_config#poe threshold 50

Related command

poe power-management

14.1.11 poe standard

To set the standard of PSE power supply, run the following command:

poe threshold {AF| AT| MAX}

Parameter

Parameter	Description
AF	If you select the AF standard, the power supply for a port can reach up to 15.4W.
AT	If you select the AT standard, the power supply for a port can reach up to 30W.
MAX	If you select MAX, it means that as to the switch with support of both AF and AT, the AT standard will be selected, and as to the switch only supporting AF, the AF standard will be selected.

Default value

The switch support MAX by default.

Command mode

Global configuration mode

Explanation

If you select the AF standard, the power supply for a port can reach up to 15.4W.

If you select the AT standard, the power supply for a port can reach up to 30W.

If you select MAX, it means that as to the switch with support of both AF and AT, the AT standard will be selected, and as to the switch only supporting AF, the AF standard will be selected.

Example

The following example shows how to set the PSE power supply standard to AF.

Switch_config#poe standard AF

Related command

N/A

14.1.12 poe disable

Enabling the Power Supply of a Port

poe disable { time-range *name* | <cr>}

no poe disable {time-range | <cr>}

Parameter

Parameter	Description
time-range *name*	The parameter **name** stands for the name of the power-off time range.
<cr>	Means to enter **poe disable** alone and shut down the port.

Default value

Power supply on a port is enabled and there is no time limit to power supply.

Command mode

Interface configuration mode

Explanation

poe disable: means to shut down power supply.

no poe disable: means to open power supply.

Example

The following example shows how to disable the power supply of port f0/1.

Switch_config_f0/1#poe disable

Related command

time-range

14.1.13 poe max-power

It is used to set the maximum power of a port.

poe max-power *value*

no poe max-power

Parameter

Parameter	Description
value	Means the maximum power of a

	port, whose unit is mW.

Default value

The default maximum power of a port is 30000mW.

Command mode

Interface configuration mode

Explanation

The "no" form of this command can be used to resume the default maximum power.

Example

The following example shows how to set the maximum power of port f0/1 to 15000mW.

Switch_config_f0/1#poe max-power 15000

Related command

poe power-management

14.1.14 poe priority

Setting the Power Supply Priority for a Port

poe priority {critical | high | low }

Parameter

Parameter	Description
critical	Stands for the highest priority.
high	Stands for the high priority.
low	Stands for the lowest priority.

Default value

The power supply priority of a port is **low** by default.

Command mode

Interface configuration mode

Explanation

N/A

Example

The following example shows how to set the power supply priority of port f0/1 to **critical**.

Switch_config_f0/1#poe priority critical

Related command

poe power-management

14.1.15 poe PD-discription

It is used to set the port description (usually for PD).

poe PD-discription *string*

no poe PD-discription

Parameter

Parameter	Description
string	Stands for the character string of port's description.

Default value

The default value is null.

Command mode

Interface configuration mode

Explanation

The "no" form of this command is used to delete the description character string.

Example

The following example shows how to set POE description to **AP-1**.

Switch_config_f0/1#poe PD-discription AP-1

Related command

N/A

14.1.16 poe force-power

It is used to set the forced power supply.

poe force-power

no poe force-power

Parameter

N/A

Default value

The forced power supply is disabled by default.

Command mode

Interface configuration mode

Explanation

The “no” form of this command is used to disable the forced power supply.

Example

The following example shows how to set the forced power supply for the POE port.

Switch_config_f0/1#poe force-power

Related command

poe power-management

Chapter 15 MAC Address Configuration Commands

15.1 MAC Address Configuration Commands

15.1.1 mac address-table static

Syntax

[**no**] **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

To add a static MAC address, run **mac address-table static *mac-addr* vlan *vlan-id* interface *interface-id***. *To cancel the static MAC address, run* ***no*** **mac address-table static *mac-addr* vlan *vlan-id* interface *interface-id***.

Parameter

Parameter	Description
mac-addr	Means an MAC address. Value range: H.H.H
vlan-id	A VLAN that the MAC address belongs to Value range: 1-4094
interface-id	Physical port that the MAC address belongs to

Default value

N/A

Explanation

This command is configured in global configuration mode.

Example

The following example shows how to bind MAC address 0004.5600.67ab to port G0/2 of VLAN1.

Switch_config# mac address-table static 0004.5600.67ab vlan 1 interface g0/2

15.1.2 mac address-table aging-time

Syntax

mac address-table aging-time [**0** | **10-1000000**]

To configure the aging time of the MAC address table, run the previous command.

Parameter

Parameter	Description
0	Means that the MAC address never ages.
10-1000000	Aging time of the MAC address whose unit is second

Default value

300s.

Explanation

This command is configured in global configuration mode.

Example

The following example shows how to set the aging time of the MAC address to 100 seconds.

Switch_config# mac address-table aging-time 100

15.1.3 show mac address-table

Syntax

show mac address-table [dynamic [interface *interface-id* | **vlan** *vlan-id***]** | **static | brief | multicast | interface** *interface-id* **| vlan** *vlan-id* **| H.H.H]**

To display the MAC address table of the switch, run **show mac address-table {dynamic [interface *interface-id* | vlan *vlan-id*] | static | brief | multicast | interface** *interface-id* **| vlan** *vlan-id* **| H.H.H]**.

Parameter

Parameter	Description
dynamic	Dynamically-learned MAC address table
interface-id	Name of an interface
vlan-id	VLAN ID。 Value range: 1-4094
static	Static MAC address table
brief	Brief information about the MAC address
multicast	Multicast MAC address table
Interface	Port's MAC address table
Vlan	Vlan mac address table

H.H.H	Specific address

Default value

N/A

Explanation

This command is used to display the MAC address table.

Example

The following example shows how to display all dynamic MAC address tables.

Switch_config#show mac address-table

Mac Address Table (Total 2)

Vlan	Mac Address	Type	Ports
1	0026.5a7c.fad3	DYNAMIC	g0/24
1	0000.0000.0004	DYNAMIC	g0/24

15.1.4 clear mac address-table

Syntax

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

To delete a dynamic MAC address, run the above-mentioned command:

Parameter

Parameter	Description
address mac-addr	Means an MAC address. Value range: H.H.H
interface-id	Means a name of a L2 interface.
vlan-id	VLAN ID。 Value range: 1-4094

Default value

N/A

Remarks

This command is used in EXEC mode.

Example

The following example shows how to clear all dynamically learned MAC addresses on interface g0/2.

```
Switch# clear mac address-table dynamic interface g0/2
```

Chapter 16 MAC Address Table Characteristics Configuration Commands

16.1 MAC Address Table Characteristic Configuration Commands

16.1.1 mac address-table static

Description

To add/delete a static MAC address, use the **mac address-table static** command.

[**no**] **mac address-table static** *mac-addr* vlan *vlan-id* interface *interface-id*

Parameter

Parameter	Description
mac-addr	MAC address. Value format: H.H.H.
vlan-id	Vlan id of the MAC address, in the range from 1 to 4094.
interface-id	Interface id of the MAC address.

Default

None

Command mode

Global configuration

Example

The following example binds the MAC address 0004.5600.67ab to the interface g0/2 of VLAN 1:

Switch(config)# mac address-table static 0004.5600.67ab vlan 1 interface g0/2

16.1.2 show mac address-table

Description

To display the content of the switch MAC address table, use the **show mac address-table** command.

show mac address-table {dynamic [interface *interface-id* | vlan *vlan-id*] | static}

Parameter

Parameter	Description

dynamic	The MAC address table that acquires dynamically.
interface-id	Interface name
vlan-id	VLAN ID, in the range from 1 to 4094.
static	The static MAC address table.

Default

None

Instruction

Use this command to display MAC address table.

Example

The following example displays all static MAC address tables:

```
Switch# show mac address-table static
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- ---- -----
All 0000.0000.0001 STATIC CPU
All 0000.0000.0002 STATIC CPU
All 0000.0000.0003 STATIC CPU
All 0000.0000.0009 STATIC CPU
All 0000.0000.0012 STATIC CPU
All 0180.c200.000b STATIC CPU
All 0180.c200.000c STATIC CPU
All 0180.c200.000d STATIC CPU
All 0180.c200.0010 STATIC CPU
```

16.1.3 clear mac address-table

Description

To delete a dynamic MAC address, run **clear mac address-table**

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

Parameter

Parameter	Description
dynamic	The dynamic MAC address
address mac-addr	The MAC address. Value range: H.H.H.
interface-id	Layer 2 interface name.
vlan-id	VLAN ID, in the range from 1 to 4094.

Default

None

Command mode

EXEC

Example

The following example deletes all MAC addresses that acquire dynamically on interface f0/2:

```
Switch# clear mac address-table dynamic interface f0/2
```

Chapter 17 802.1x Configuration Commands

17.1 802.1x Configuration Commands

802.1x configuration commands include：

- dot1x enable
- dot1x port-control
- dot1x multiple-hosts
- dot1x default
- dot1x max-req
- dot1x reauth-max
- dot1x re-authentication
- dot1x timeout quiet-period
- dot1x timeout re-authperiod
- dot1x timeout tx-period
- dot1x user-permit
- dot1x authentication method
- dot1x authen-type、dot1x authentication type
- dot1x guest-vlan
- dot1x guest-vlan id
- aaa authentication dot1x
- debug dot1x error
- debug dot1x state
- debug dot1x packet
- show dot1x

17.1.1 dot1x enable

Description

dot1x enable

no dot1x enable

Parameter

None

Default

None

Instruction

Use this command to enable 802.1x feature. The 802.1x feature cannot be enalbed on an interface. If 802.1x feature is disabled, then all 802.1x packets will be forwarded like other multi-cast packets in VLAN rather than be received by CPU.

Command mode

Global configuration

Example

The following example enables dot1x:

```
Switch(config)#dot1x enable
Switch(config)#
```

17.1.2 dot1x port-control

Description

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

no dot1x port-control

Parameter

Parameter	Description

auto	Enables 802.1x protocol authentication method
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Default

force-authorized

Instruction

The 802.1X protocol is supported on Layer 2 static-access ports. You can use the auto keyword only if the port is not configured as one of these types:

•Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.

•EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

•Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

Command mode

interface configuration

Example

The following example enables 802.1x on interface f0/24:

```
Switch(config_f0/24)# dot1x port-control auto
Switch(config_f0/24)#
```

The following example configures interface f0/23 as the vlan trunk port and enables 802.1x:

```
Switch(config_f0/23)#switchport mode trunk
Switch(config_f0/23)#dot1x port-control auto
802.1x Control Failed, 802.1x cannot cmd on vlanTrunk port(f0/23)
Switch(config_f0/23)#
```

17.1.3 dot1x multiple-hosts

Description

To allow multiple hosts (clients) on an 802.1X-authorized switch port that has the dot1x port-control interface configuration command set to auto, use the dot1x multiple-hosts command. To return to the default setting, use the no form of this command.

dot1x multiple-hosts

no dot1x multiple-hosts

Parameter

None

Default

disabled

Instruction

In multi-host mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access (the multi-host mode authenticates one client, but after the client is authenticated, traffic is allowed from all other MAC addresses.). If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

The single-host mode allows only one client per port, that is, one MAC address to authenticate, and all others are blocked.

Command mode

interface configuration

Example

The following example enables multiple-hosts on interface f0/24:

Switch(config_f0/24)# dot1x *multiple-hosts*
Switch(config_f0/24)#

17.1.4 dot1x default

Description

To reset the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard, use the dot1x default command.

dot1x Default

Parameter

None

Default

None

Instruction

To reset the global 802.1X authentication parameters to their default values.

Command mode

Global configuration

Example

The following example shows how to reset the global 802.1X parameters:

Switch(config)#dot1x *default*
Switch(config)#

17.1.5 dot1x max-req

Description

To set the maximum number of times that a networking device or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the dot1x max-req command in interface configuration or global configuration mode. To set the number of times to the default setting of 2, use the no form of this command.

dot1x max-req *count*

no dot1x max-req

Parameter

Parameter	Description
count	Maximum number of retries. The value is from 1 through 10.

Default

2

Instruction

Change the maximum number of retries to ensure to pass the authentication between certain clients and authentication servers.

Command mode

Global configuration

Example

The following example sets 4 as the maximum number of times:

Switch(config)#dot1x *max-req 4*
Switch(config)#

17.1.6 dot1x reauth-max

Description

dot1x reauth-max *count*

no dot1x reauth-max

Parameter

Parameter	Description
count	Maximum number of retries. The value is from 1 through 10.

Default

4

Instruction

Use this command to set maximum number of reauthentications. The authentication will be suspended when there is no response from client on exceeding the number of this configured reauthentication times.

Command mode

Global configuration

Example

The following example set 5 as the maximum number of reauthentications:

Switch(config)#dot1x *reauth-max 5*
Switch(config)#

17.1.7 dot1x re-authentication

Description

To enable the periodic reauthentication of the client, use the dot1x re-authentication command. To return to the default setting, use the no form of this command.

dot1x re-authentication

no dot1x re-authentication

Parameter

None

Default

None

Instruction

You configure the amount of time between the periodic reauthentication attempts by using the dot1x timeout re-authperiod global configuration command.

Command mode

Global configuration

Example

This example shows how to enable the periodic reauthentication:

Switch(config)#dot1x *re-authentication*
Switch(config)#

17.1.8 dot1x timeout quiet-period

Description

dot1x timeout quiet-period *time*

no dot1x timeout quiet-period

Parameter

Parameter	Description
time	Period of reenabling authentication, in the range from 0 to 65535 seconds

Default

60s

Instruction

There will be a period of quiet time after authentication failure during which swith doesn't receive or enable any authentication.

Command mode

Global configuration

Example

The following example configures quiet period value to 40:

Switch(config)#dot1x *timeout quiet-period 40*
Switch(config)#

17.1.9 dot1x timeout re-authperiod

Description

dot1x timeout re-authperiod *time*

no dot1x timeout re-authperiod

Parameter

Parameter	Description
time	Period of reauthentication, in the range from 1 to 4294967295 seconds

Default

3600s

Instruction

This command is valid only after enabling the **dot1x re-authentication command**.

Command mode

Global configuration

Example

The following example configures dot1x reauthentication period to 7200s:

Switch(config)# dot1x *timeout re-authperiod 7200*
Switch(config)#

17.1.10 dot1x timeout tx-period

Description

dot1x timeout tx-period *time*

no dot1x timeout tx-period

Parameter

Parameter	Description
time	Time is from 1 to 65535s。

Default

30s

Instruction

This command specifies the time interval of the host client to respond to the authentication request. The switch will resend the authentication request when exceeding this time interval.

Command mode

Global configuration

Example

The following command sets 24 as the timeout period:

Switch(config_f0/0)# dot1x *timeout tx-period 24*
Switch(config_f0/0)#

17.1.11 dot1x user-permit

Description

dot1x user-permit xxx yyy zzz

no dot1x user-permit

Parameter

Parameter	Description
xxx	Username
yyy	Username
zzz	Username

Default

All users are allowed to pass without user-bind.

Instruction

Use this command to bind user on the interface, eight users can be binded on each interface. When enabled 802.1x authentication, the authentication is only available to the binding user.

Command mode

interface configuration

Example

The following example configures a,b,c,d as the binding user on interface f0/1:

Switch(config_f0/1)# *dot1x user-permit a b c d*

Switch(config_f0/1)#

17.1.12 dot1x authentication method

Description

dot1x authentication method xxx

no dot1x authentication method

Parameter

Parameter	Description
xxx	Method name

Default

“default”method

Instruction

Use this command to configure authentication method on an interface. This command is one of the authentication methods that AAA provides. Each interface only uses one authentication method. When AAA performs authentication for users of 802.1x, it will select the configured authentication method to perform.

Command mode

interface configuration

Example

The following example configures abcd as the authentication method on interface f0/1; this method uses local username for authentication. The following example configures efgh as the authentication method on interface f0/2:

Switch(config) #aaa authentication dot1x abcd local
Switch(config) #aaa authentication dot1x efgh radius
Switch(config) #int f0/1
Switch(config_f0/1)# dot1x authentication method abcd
Switch(config_f0/1)# int f0/2
Switch(config_f0/2)# dot1x authentication method efgh

17.1.13 dot1x accounting enable

Description

dot1x accounting enable

no dot1x accounting enable

Parameter

Parameter	Description
None	

Default

The accounting function is disabled.

Explanation

The accounting function must be used together with the authentication function. You'd better enable the dotx re-authentication function.

Command mode

Port configuration mode

Example

The following commands are used to configure the dot1x authentication function on port f0/1 and enable the accounting function:

Switch(config) #dot1x enable
Switch(config) #int f0/1
Switch(config_f0/1)# dot1x port atuo

Switch(config_f0/1)# dot1x accounting enable

17.1.14 dot1x accounting method

Description

dot1x accounting method xxx

no dot1x accounting method

Parameter

Parameter	Description
xxx	Name of the accounting method

Default

the **default** method

Explanation

The accounting method configured by this command must be one of the AAA accounting methods. Each port has only one accounting method. After the dot1x accounting function is enabled, the method is used for accounting.

Command mode

Port configuration mode

Example

In the following example, an **abcd** accounting method is set for port f0/1. The radius server must be used in this method.

Switch(config) # aaa accounting network abcd start-stop group radius
Switch(config) #radius host 192.168.20.100
Switch(config) #int f0/1
Switch(config_f0/1)# dot1x accounting method abcd

17.1.15 dot1x authen-type、dot1x authentication type

Description

To configure global dot1x authentication type, use the **dot1x authen-type command. Use the no form of this command to restore the default value.**

dot1x authen-type {**chap**|**eap**}

no dot1x authen-type

Parameter

None

Default

Default global is chap.

Default on an interface refers to the default global.

Instruction

Use this command to configure authentication type. The authentication type will decide AAA to use Chap or Eap. The challenge that MD5 needs will be formed locally when using Chap. The challenge that MD5 needs will be formed on the authentication server when using Eap. Each interface only uses one kind of authentication type. It is the globally-configured one by default. The interface will not stop using this kind of authentication type until the no form of this command is used.

Command mode

Interface and global configuration

Example

The following example configures Chap and Eap as the authentication type and the global authentication type on the interface f0/1

Switch(config) #dot1x *authen-type eap*

Switch(config) #int f0/1

Switch(config_f0/1)# dot1x authentication type chap

17.1.16 dot1x guest-vlan

Description

To specify an active VLAN as an IEEE 802.1x guest VLAN, use the dot1x guest-vlan command in interface configuration mode. To return to the default setting, use the no form of this command.

dot1x guest-vlan

no dot1x guest-vlan

Parameter

None

Default

No guest VLAN is configured.

Instruction

When you enable the guest-vlan command, the software will assign the corresponding port to a guest VLAN when it does not receive a response from the client.

This command is used with the dot 1x guest-valan id inteface configuration command.

Command mode

Global configuration

Example

The following example enables global guest-vlan feature:

Switch(config) #dot1x guest-vlan

17.1.17 dot1x guest-vlan id

Description

To configure dot1x guest-vlan id value on an interface, use the dot1x guest-vlan command. Use the no form of this command to restroe the default value.

dot1x guest-vlan id

no dot1x guest-vlan

Parameter

Id：guest vlan value，which can be any configured vlan id in the system

Default

0

Instruction

When you enable the guest-vlan command, the software will assign the corresponding port to a guest VLAN when it does not receive a response from the client.

This command is used with the dot 1x guest-valan global configuration command.

Command mode

interface configuration

Example

The following example configures guest-vlan id value on an interface:

Switch(config_if) #dot1x guest-vlan 2

17.1.18 dot1x forbid multi-network-adapter

Description

dot1x forbid multi-network-adapter

no dot1x forbid multi-network-adapter

Run **dot1x forbid multi-network-adapter** to configure the Supplicant to shut down multiple network adapters. Run **no dot1x forbid multi-network-adapter** to resume the default configuration.

Parameter

None

Default

None

Explanation

This command can disable the Supplicant with multiple network adapters to prevent the agent.

Command mode

Port configuration mode

Example

The following command is run in port mode to disable the Supplicant with multiple network adapters.

Switch(config_if) # dot1x forbid multi-network-adapter

17.1.19 aaa authentication dot1x

Description

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the aaa authentication dot1x command. To disable authentication, use the no form of this command

aaa authentication dot1x {**Default**} *method1* [*method2...*]

no aaa authentication dot1x {**Default**} *method1* [*method2...*]

Parameter

Parameter	Description
Default	Uses the listed authentication methods that follow this parametert as the default list of methods when a user logs in.
method1 [*method2...*]	enable 、group radius、line、local、local-case、None

Default

No authentication is performed.

Instruction

The method parameter identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 802.1X-compliant is the group radius method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the local and local-case methods use the username and password that are saved in the configuration file. The enable and line methods use the enable and line passwords for authentication.

Command mode

Global configuration

Example

The following example configures RADIUS as the dot1x authentication method:

Switch(config)#aaa authentication dot1x default radius
Switch(config)#

17.1.20 debug dot1x error

Description

debug dot1x error

Parameter

None

Default

None

Instruction

This command is used to dubug all error information during dot1x running to locate errors.

17.1.21 debug dot1x state

Description

debug dot1x state

Parameter

None

Default

None

Instruction

Output format is as follows:

2003-3-18 17:40:09 802.1x:AuthSM(F0/10) state Connecting-> Authenticating, event rxRespId

2003-3-18 17:40:09 802.1x:F0/10 Create user for Enter authentication

2003-3-18 17:40:09 802.1x:BauthSM(F0/10) state Idle-> Response, event authStart

2003-3-18 17:40:09 802.1x:F0/10 user "myname" denied, Authentication Force Failed

2003-3-18 17:40:09 802.1x:F0/10 Authentication Fail

2003-3-18 17:40:09 802.1x:BauthSM(F0/10) state Response-> Fail, event aFail

17.1.22 debug dot1x packet

Description

debug dot1x packet

Parameter

None

Default

None

Instruction

2003-3-18 17:40:09 802.1x:F0/10 Tx --> Supplicant(0008.74bb.d21f)
EAPOL ver:01, type:00, len:5
EAP code:01, id:03, type:01, len:5
00
2003-3-18 17:40:09 802.1x:F0/10 Rx <-- Supplicant(0008.74bb.d21f)
EAPOL ver:01, type:00, len:10
EAP code:02, id:03, type:01, len:10
62 64 63 6f 6d a5

17.1.23 show dot1x

Description

To show 802.1x configuration information, use the show dot1x command.

show dot1x [interface *intf-id*]

Parameter

Parameter	Description
intf-id	The concrete physical interface.

Default

None

Instruction

This command is used to show 802.1x configuration information.

Command mode

EXEC

Example

The following example configures dot1x port-control auto on the interface f0/10:

```
Switch_config#sho dot1x
802.1X Parameters
reAuthen          No
reAuth-Period     3
quiet-Period      10
Tx-Period         30
Supp-timeout      30
Server-timeout    30
reAuth-max        4
max-request       2
authen-type       Eap
IEEE 802.1x on port F0/10 enabled
Authorized                  Yes
Authen Type                 Eap
Authen Method               default
Permit Users                All Users
Multiple Hosts              Disallowed
Supplicant                  aaa(0008.74bb.d21f)
Current Identifier          21
Authenticator State Machine
State                   Authenticated
Reauth Count                0
Backend State Machine
State                   Idle
Request Count               0
Identifier (Server)         20
Port Timer Machine
Auth Tx While Time          16
Backend While Time          16
reAuth Wait Time            3
Hold Wait Time              0
```

Chapter 18 VLAN Configuration Commands

18.1 VLAN Configuration Commands

VLAN configuration commands include：

- vlan
- name
- switchport pvid
- switchport mode
- switchport trunk
- show vlan

18.1.1 vlan

To add a VLAN, use the **vlan** command. Use the no form of this command to delete a VLAN.

[**no**] **vlan** *vlan-id*

Parameter

Parameter	Description
vlan-id	ID of the VLAN. Range is from 1 to 4094。

Default

None

Command mode

Global

Instruction

Use this command to enter the VLAN configuration mode and to modify some attributes of the VLAN.

Example

This example shows how to add a new VLAN:

Switch_config#
Switch_config#vlan 2
Switch_config_vlan_2#

18.1.2 name

To assign a name to a VLAN, use the **name** command. Use the no form of this command to remove the name assigned to a VLAN.

[**no**] **name** *str*

Parameter

Parameter	Description
str	Name of the defined VLAN。The name consists of up to 32 characters.

Default

The default VLAN name is 'Default'. Other VLAN name is VLANxxxx (xxxx is 4-digit stack ID).

Command mode

VLAN configuration mode

Instruction

This command can modify VLAN name to indicate special VLAN according to special requirements.

Example

The following command modify vlan200 to main405.

Switch_config#
Switch_config#
Switch_config#vlan 200
Switch_config_vlan_200#name ?
  WORD The ascii name of VLAN(32bytes)
Switch_config_vlan_200#name main405

18.1.3 switchport pvid

To configure port VLAN of in the access mode, use the **switchport pvid** command.

switchport pvid *vlan-id*

no switchport pvid

Parameter

Parameter	Description
vlan-id	VLAN ID of the port。 Range is from 1 to 4094。

Default

All ports are subordinate to VLAN 1.

Command mode

Interface configuration mode

Instruction

Vlan of the pvid must exist before configuring this command. The port can be access mode or frame relay mode.

Example

The following example configures interface fastethernet 0/1 as the access interface of VLAN 10:

Switch(config)#interface f0/1
Switch(config)#vlan10
Switch(config-f0/1)#switchport pvid 10

18.1.4 switchport mode

To configure the interface mode, use the **switchport mode** command.

switchport mode {*access* | *dot1q-tunnel* | *trunk*}

Parameter

Parameter	Description
access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.

dot1q-tunnel	Sets the trunking mode to TUNNEL unconditionally.
trunk	Specifies a trunking VLAN Layer 2 interface.

Default

Access mode

Command mode

Interface configuration mode

Instruction

If you enter access mode, the interface goes into permanent non-trunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

If you enter trunk mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not agree to the change.

If you enter dot1q-tunnel mode, the port is set unconditionally as an 802.1Q tunnel port.

The switchport mode command conflicts with 802.1X protocol. You cannot configure 802.1X protocol in trunk mode. 802.1X protocol is valid only in access mode.

Example

The following example configures the port to the trunk mode:

```
Switch(config-f0/1)#switchport mode trunk
```

18.1.5 switchport trunk

To set the trunk characteristics, use the **switchport trunk** command. To reset all of the trunking characteristics back to the original defaults, use the no form of this command.

[**no**] **switchport trunk** {*vlan-allowed vlan-list*} | {*vlan-untagged vlan-list* }

Parameter

Parameter	Description
vlan-allowed	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format. Value is from 1 to 4094.
vlan-untagged	Sets the list of allowed VLANs that transmit traffic from this interface in untagged format.Value is from 1 to 4094.

Default

The default native vlan ID is 1.

The valid VLAN ID is from 1 to 4094 (all VLANs).

Command mode

Interface configuration

Instruction

You can use this command on an interface no matter it is in access or trunk mode. But this command is valid only when the interface is in trunking mode.

The vlan-allowed parameter sets the list of allowed VLANs that transmit traffic from this interface in tagged format. The vlan-untagged parameter sets the list of allowed VLANs that transmit traffic from this interface in untagged format.

The vlan-list format is all | none | add | remove | except vlan-list[,vlan-list...] where:

•all—Specifies all VLANs from 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.

•none—Indicates an empty list. This keyword is not supported in the switchport trunk allowed vlan form of the command.

•add—Adds the defined list of VLANs to those currently set instead of replacing the list.

•remove—Removes the defined list of VLANs from those currently set instead of replacing the list.

•except—Lists the VLANs that should be calculated by inverting the defined list of VLANs.

•vlan-list—Is either a single VLAN number from 1 to 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.

Example

The following example configures VLAN ID range to 1-10:

```
Switch(config-f0/1)#switchport trunk vlan-allowed 1-10,20-30,55
Switch(config-f0/1)#switchport trunk vlan-untagged 2-1000
```

18.1.6 double-tagging

To configure global VLAN tunnel characteristic, use the **double-tagging** command.

[**no**] **double-tagging**

Note：

Since the realization of the switch chip features vary widely, some switches can only enable/disable VLAN tunnel characteristic in global configuration mode, and some can also be configured on an interface.

The supporting capability in dot1q-tunnel of various models is as follows:

Model	Supporting capability in dot1 q-tunnel
2116 / 2224 / 2224M / 2226 / 2448B / 3224 / 3224M / 3424 / 6508	Not supported
2224D	Global
2448 / 2516 / 2524 / 3448 / 3512	port

For unlisted models or new models, please refer to the technical supporting engineers or download the latest instructions for reference.

Parameter

none

Default

disabled

Command mode

Interface configuration

Instruction

Some switch chips don’t support port-based VLAN tunnelling configuration. They only support enabling or disabling this characteristic at the same time on all interfaces (please refer to the model description of the configuration manual). The switch that uses this kind of switch doesn’t provide the switchport mode dot1q-tunnel command in the interface configuration mode. It provides the double-tagging command in the global configuration mode instead to enable or disable the double-tagging characteristic in the global configuration.

Example

The following example enables global vlan tunnel characteristic of the switch:

Switch(config)#double-tagging

18.1.7 show vlan

To display VLAN information, use the show vlan command.

show vlan [**id** *vlan-id* | **interface** *intf-id*]

Parameter

Parameter	Description
id	Displays information about a single VLAN that is identified by a VLAN ID number; valid values are from 1 to 4094.
interface	Displays the specified interface

Default

None

Command mode

EXEC/ All configuration modes

Instruction

None

Example

The following example shows all VLAN information:

```
Switch#sho vlan
VLAN Status   Name            Ports
---- ------- ---------------- ------------------------------------------------
1    Static   Default         F0/1, F0/2, F0/3, F0/4, F0/5, F0/6, F0/7, F0/8
                              F0/9, F0/10, F0/11, F0/12, F0/13, F0/14, F0/15
                              F0/16, F0/17, F0/18, F0/19, F0/20, F0/21, F0/22
                              F0/23, F0/24, G1/1, G2/1, P1
2    Static   VLAN0002        F0/3
3    Static   VLAN0003        F0/3
4    Static   VLAN0004        F0/3
5    Static   VLAN0005        F0/3
6    Static   VLAN0006        F0/3
```

Status: it indicates the source of VLAN. Static: indicates the VLAN is formed by configuration. Dynamic: indicates the VLAN is dynamically formed by GVRP protocol.

The following example shows the concrete information of a VLAN:

```
Switch> show vlan id 1
VLAN id: 1, Name: default, TotalPorts:11

Ports            Atttributes
-----------------------------------------------------------------
F0/1             Trunk,Untagged
F0/2             Access
F0/5             Trunk,Untagged
F0/7             Trunk,Tagged
F0/8             Trunk,Tagged
F0/9             Trunk,Tagged
F0/11            Access
F0/12            Access
F0/14            Trunk,Tagged
F0/15            Trunk,Tagged
F0/16            Trunk,Untagged
```

The following example shows the relevant information about a VLAN on an interface:

```
Switch#sho vlan int f0/6

Interface          VLAN
Name               Property PVID Vlan-Map        uTagg-VLan-Map
-------------------- -------- ---- ---------------- ----------------
FastEthernet0/6      Trunk    1    3,5,7,9,11,13,15 none
                                   17,19
Switch#sho vlan int f0/7

Interface          VLAN
Name               Property PVID Vlan-Map        uTagg-VLan-Map
-------------------- -------- ---- ---------------- ----------------
FastEthernet0/7      Access   7    7               ----
```

18.1.8 interface supervlan

Description

[**no**] **interface supervlan** *index*

It is used to configure the SuperVLAN interface.

Parameter

Parameter	Description
index	Index of the SuperVlan port, ranging from 1 to 32

Default

None

Explanation

The command is configured in global configuration mode. It is used to configure a SuperVLAN port and enable the system to enter the port configuration mode. Its “no” form can be used to delete the configured interface.

Example

See the **sub vlaN** command.

18.1.9 sub vlan

Description

[**no**] **sub vlan** [*string*] [**add** *add-string*] [**remove** *rem-string*]

It is used to configure a SubVLAN on the SuperVLAN interface. Its “no” form can be used to delete all SubVlans on the SuperVLAN interface. Only one subcommand can be used each time.

Parameter

Parameter	Description
string	Sets SubVlan in a SuperVLAN. If you set a SubVlan, the original configuration will be deleted. **string** here means the VLAN list, for example, 2, 4, 5 and 6 stand for VLAN 2, VLAN 4, VLAN 5 and VLAN 6 respectively.
add-string	Adds the **add-string** VLAN list to the original SubVlan. The format is the same as above.
rem-string	Removes the **del-string** VLAN list from the original SubVlan. The format is the same as above.

Default

The SubVlan in SuperVlan is null by default.

Explanation

A SubVLAN list can be configured in the SuperVLAN.

Example

In the following example, interface SuperVlan 5 is configured and SubVLANs are set. Interface SuperVlan 5 has the SubVlan lists 2, 3, 5, 6, 7, 9, 11 and 12, that is, Vlan 2, Vlan 3, Vlan 5, Vlan 6, Vlan 7, Vlan 9, Vlan 11 and Vlan 12.

```
interface supervlan 5
subvlan 2,3,5-7
subvlan add 7,9-12
subvlan remove 10
```

Chapter 19 GVRP Configuration Commands

19.1 GVRP Configuration Commands

19.1.1 gvrp

Description

To enable GVRP globally on a device and on an interface, use the **gvrp** command. To disable GRVP, use the no form of this command.

gvrp

no gvrp

Parameter

none

Default

GVRP is administratively diasbled.

GRVP is administratively enabled on each interface.

Instruction

- When GVRP is enabled in the system,VTP cannot be enabled, and vice versa.
- GVPRP can be enabled globally or on an interface in the system, and GVRP is not enabled until both of them are enabled.

Example

The following example configures global gvrp on the device and interfaces:

```
Switch(config)# gvrp
Switch(config)#
```

The following example enables gvrp on interface 1:

```
Switch(config-if-Ethernet0/1) # gvrp
Switch(config-if-Ethernet0/1) #
```

19.1.2 show gvrp statistics

Description

To show gvrp statistics, use the **show gvrp statistics** command.

show gvrp statistics [interface *intf-id*]

Parameter

Parameter	Description
intf-id	Concrete physical interface

Default

none

Instruction

Show GVRP statistics.

Example

The following example show GVRP statistics on port Ethernet0/1:

GVRP statistics on port Ethernet0/1
GVRP Status: Enabled
GVRP Failed Registrations: 0
GVRP Last Pdu Origin: 0000.0000.0000
GVRP Registration Type: Normal

19.1.3 show gvrp status

Description

To show GVRP status information, use **show gvrp status** command.

show gvrp status

Parameter

none

Default

none

Instruction

Show GVRP status information.

Example

The following command shows GVRP status information of the switch:

GVRP is enabled

19.1.4 debug gvrp event

Description

To enable debugging GVRP event information, use the **debug gvrp event** command. Use the no form of this command to disable debugging.

debug gvrp event

no debug gvrp event

Parameter

none

Default

none

Instruction

Enable/disable debugging GVRP event information.

Example

Switch# debug gvrp event
Switch#

19.1.5 debug gvrp packet

Description

To enable debugging GVRP packet information, use the **debug gvrp event** command. Use the no form of this command to disable debugging.

debug gvrp packet

no debug gvrp packet

Parameter

none

Default

none

Instruction

Enable/disable debugging GVRP packet information.

Example

```
switch# debug gvrp packet
switch#
```

19.2 GARP Configuration Commands

GARP is the basic module of GVRP/GMRP. It is intended to scheduler GVRP/GMRP operation and provide service.

19.2.1 garp timer

Description

To set the GARP timer values, use the **garp timer** command. Use the no form of this command to restore the default value.

garp timer { **hold** | **join** | **leave** } *time_value*

no garp timer { **hold** | **join** | **leave** }

Parameter

Parameter	Description
timer_value	Timer value Value range: 10 – 32760 centiseconds

Default

hold timer: 10 centiseconds.

join timer: 20 centiseconds.

leave timer: 60 centiseconds.

Instruction

(1) It is used to send out VLAN registration information periodically.

(2) When the VLAN registration information is received on the port, the joinin message will not be sent out promptly to register this VLAN information. A hold timer is started up instead, and the joinin message will not be sent out before the timer expires. This could save bandwidth and accept more VLAN information.

(3) If the timer expires before the corresponding VLAN registration information is received on that port, the vlan information will be logged out.

(4) leave timer: It must twice lager than or euqal to the value of join time.

Example

The following example configures 30 centiseconds as the garp hold timer:

```
Switch(config-if-Ethernet0/1)# garp timer hold 30
Switch(config-if-Ethernet0/1)#
```

19.2.2 garp leaveall

Description

To configure garp leaveall timer, use the **garp timer leaveall** command. Use the “no” form of this command to restore the default value.

garp timer leaveall *time_value*

no garp timer leaveall

Parameter

Parameter	Description
timer_value	Global leaveall timer value Value range: 10–32765 centseconds

Default

1000 centiseconds

Instruction

Bridge will clear all registed VLAN information and send out leaveall message after leaveall timer expires.

Example

The following example configures leaveall timer on the switch:

```
Switch(config)# garp timer leaveall 20000
Switch(config)#
```

19.2.3 show garp timer

Description

To show the timer information that GARP configures, use the **show garp timers** command.

show garp timers [interface *intf_id*]

Parameter

Parameter	Description
intf-id	Concrete physical interface

Default

none

Instruction

Use this command to show the timer information that GARP configures, including the value of global leaveall timer, hold timer, join timer and leave timer on the interface.

Example

The following example shows the timer configuration information on interface Ethernet0/1:

Switch# show garp timers interface e0/1
GARP timers on port Ethernet0/1

Garp Join Time: 200 milliseconds
Garp Leave Time: 600 milliseconds
Garp LeaveAll Time: 10000 milliseconds
Garp Hold Time: 100 milliseconds

19.2.4 show garp status

Description

To show the currently-running garp application example, use the **show garp** command**.**

show garp

Parameter

none

Default

none

Instruction

none

Example

The following example shows GARP statistics on interface Ethernet0/1:

Switch_config#show garp status
No GARP application is running.

19.2.5 debug garp event

Description

To enable debugging garp event, use the **debug garp event** command. Use the no form of this command to disable debugging.

debug garp event

no debug garp event

Parameter

none

Default

none

Instruction

Use this command to enable/disable debugging GARP event information.

Example

```
Switch# debug garp event
Switch#
```

Chapter 20 Private VLAN Configuration Commands

20.1 Private VLAN Configuration Commands

The following are private VLAN configuration commands:

- private-vlan
- private-vlan association
- switchport mode private-vlan
- switchport private-vlan host-association
- switchport private-vlan mapping
- switchport private-vlan
- show vlan private-vlan
- show vlan private-vlan interface

20.1.1 private-vlan

private-vlan {primary|community|isolated}

To configure the features of private VLAN, run the aforementioned command.

Parameter

Parameter	Description
primary	Sets VLAN to the primary VLAN.
community	Sets VLAN to the community VLAN.
isolated	Sets VLAN to the isolated VLAN.

Default value

No configuration is done to any type of private VLAN.

Command mode

VLAN configuration mode

Explanation

Primary VLAN: It is relevant to a promiscuous port and only one primary VLAN exists in the private VLAN. Each port in the primary VLAN is a member in the primary VLAN.

Isolated VLAN: No layer-2 communication can be conducted between two ports in the same isolated VLAN. Also, there is only one isolated VLAN in a private VLAN. The isolated

VLAN must be related with the primary VLAN.

Community VLAN: Layer-2 communication can be conducted between two ports in the same VLAN, but they have no communication with the ports in another community VLAN. One private VLAN may contain multiple community VLANs. The community VLAN must be related with the primary VLAN.

Example

The following example shows how to set VLAN2 to be the primary VLAN.

```
Switch_config#
Switch_config#vlan 2
Switch_config_vlan2#private-vlan primary
```

20.1.2 private-vlan association

private-vlan association **{***svlist* **| add** *svlist* **| remove** *svlist***}**

no private-vlan association

To configure the private VLAN's association, run the first one of the above-mentioned commands.

Parameter

Parameter	Description
svlist	Sets the to-be-associated secondary VLAN.

Default value

No secondary VLAN is associated.

Command mode

VLAN configuration mode

Explanation

This command is used to associate primary VLAN with secondary VLAN to enable them to realize VLAN learning sharing in the whole private VLAN. This command is run only in primary VLAN configuration mode.

When svlist is used, you can add or remove the lists to or from secondary VLAN. The entered lists are separated by the comma or the hyphen. For example, "1, 3, 5, 7" stands for "vlan 1, vlan 3, vlan 5, vlan 7", while "1, 3-5, 7" stands for "vlan 1, vlan 3, vlan 4, vlan 5, vlan 7".

The validation of the whole private VLAN depends on the correct configurations of all features in private VLNA.

Example

The following example shows how to associate primary VLAN 2 with community VLAN 3 or community VLAN 4.

```
Switch_config#
Switch_config#vlan 2
Switch_config_vlan2#private-vlan association 3-4
```

20.1.3 switchport mode private-vlan

switchport mode private-vlan {*host* **|** *promiscuous***}**

To set the mode for a layer-2 port in private VLAN, run the above-mentioned command.

Parameter

Parameter	Description
host	Sets the layer-2 port to be in host's port mode.
promiscuous	Sets the layer-2 port to be in promiscuous port mode.

Default value

No mode in any private VLAN is configured.

Command mode

Port configuration mode

Explanation

This command is used to set the mode in private VLAN for layer-2 port: the promiscuous port mode or the host port mode. The latter can be classified into the public port and the isolated port.

Promiscuous port: it belongs to the primary VLAN. It can communicate with all other ports, including the isolated port and community port of a secondary VLAN in the same private VLAN.

Isolated port: It is the host port in the isolated VLAN. In the same private VLAN, the isolated port is totally L2 isolated from other ports except the promiscuous port, so the flows received from the isolated port can only be forwarded to the promiscuous port.

Community port: It is the host port in the community VLAN. In a private VLAN, the community ports of the same community VLAN can conduct L2 communication each other or with the promiscuous port, but not with the community ports of other VLANs and the isolated ports in the isolated VLANs.

Example

The following example shows how to set interface g0/1 to a promiscuous port:

```
Switch_config#
Switch_config#interface g0/1
Switch_config_g0/1#switchport mode private-vlan promiscuous
```

20.1.4 switchport private-vlan host-association

switchport private-vlan host-association *p_vid s_vid*

To set the private VLAN associating with the L2 host port, run the above-mentioned command.

Parameter

Parameter	Description
p_vid	Sets the VLAN ID of the to-be-associated primary VLAN, which ranges between 1 and 4094.
s_vid	Sets the VLAN ID of the to-be-associated secondary VLAN, which ranges between 1 and 4094.

Default value

No association is set for private VLAN.

Command mode

Port configuration mode

Explanation

This command is mainly used to set the L2 host port to associate primary and secondary VLANs. This newly configured host port takes no effect on the associated primary and secondary VLANs until you set it to be the host port, the private VLAN type of the two associated VLANs is set correctly and the association of the two VLANs is correctly set.

Example

The following example shows how to build up the host association between port g0/1 and primary VLAN2 and secondary VLAN3.

Switch#config

Switch_config#interface g0/1

Switch_config_g0/1#switchport private-vlan host-association 2 3

20.1.5 switchport private-vlan mapping

switchport private-vlan mapping

*p_vid***{***svlist* **| add** *svlist* **| remove** *svlist***}**

To set the private VLAN associating with the L2 promiscuous port, run the above-mentioned command.

Parameter

Parameter	Description
p_vid	Sets the VLAN ID of the to-be-associated primary VLAN, which ranges between 1 and 4094.

svlist	Sets the to-be-associated secondary VLAN.

Default value

No association is set for private VLAN.

Command mode

Port configuration mode

Explanation

This command is mainly used to set the L2 promiscuous port to associate primary and secondary VLANs. This newly configured port takes no effect on the associated primary and secondary VLANs until you set it to be the promiscuous port, the private VLAN type of the two associated VLANs is set correctly and the association of the two VLANs is correctly set.

When svlist is used, you can add or remove the lists to or from secondary VLAN. The entered lists are separated by the comma or the hyphen. For example, “1, 3, 5, 7” stands for "vlan 1, vlan 3, vlan 5, vlan 7”, while “1, 3-5, 7” stands for "vlan 1, vlan 3, vlan 4, vlan 5, vlan 7”.

Example

The following example shows how to build up the promiscuous association between port g0/1 and primary VLAN2 and secondary VLANs 3-5.

Switch#config

Switch_config#interface g0/1

Switch_config_g0/1#switchport private-vlan mapping 2 3-5

20.1.6 switchport private-vlan

switchport private-vlan { tag-pvid *p_vid* **| tag-pri** *priority* **| untagged }**

no switchport private-vlan untagged

To set the tag and its field of the egress packets on the L2 port of the private VLAN, run the first of the above-mentioned two commands.

Parameter

Parameter	Description
p_vid	Stands for the VLAN ID in the tag, which ranges from 1 to 4094.
priority	Sets the priority field in the tag, which ranges from 0 to 7.
untagged	Sets the egress packets to have the tag or not.

Default value

The default VLAN ID in the tag is 1.

The default priority is 0.

The egress has no tag by default.

Command mode

Port configuration mode

Explanation

This command is mainly used to set the tag of egress packets in private VLAN or set whether egress packets have the tag. This command takes effect after private VLAN, the association between private VLANs in the private VLAN domain, the L2 port mode in private VLAN, and the association between L2 port and private VLAN are all correctly set.

20.1.7 show vlan private-vlan

show vlan private-vlan

To display the configurations of VLAN and L2 port in the private VLAN, run the above-mentioned command.

Parameter

N/A

Default value

N/A

Command mode

Port configuration mode, VLAN configuration mode and EXEC mode

Explanation

This command is used to display the configurations of VLAN and L2 port in the private VLAN.

Example

The following example shows how to display the configuration of private VLAN.

```
Switch_config#
Switch_config#show vlan private-vlan
Primary  Secondary  Type               Ports
-------  ---------  -----------------  ------------------------------------------
      2          3  community          G0/1, G0/2, G0/3
      2          4  isolated           G0/1, G0/4
      2          5  community          G0/1, G0/5
```

20.1.8 show vlan private-vlan interface

show vlan private-vlan interface *interface*

To display the configurations of the L2 port in the private VLAN, run the above-mentioned command.

Parameter

Parameter	Description
Interface	Stands for the to-be-shown interface.

Default value

N/A

Command mode

Port configuration mode, VLAN configuration mode and EXEC mode

Explanation

This command is used to display the configuration of L2 port in the private VLAN.

Example

The following example shows how to display the configuration of L2 interface g0/1 in the private VLAN.

```
Switch_config#
Switch_config#show vlan private-vlan interface g0/1
port type: promiscuous port
private-vlan host-association: primary vlan 2 secondary vlan 3
private-vlan mapping: primary vlan 2 secondary vlan 3-5
Native VLAN tagging enable: untagged
Native VLAN tagging priority 0
Native VLAN tagging pvid: 1
```

Chapter 21 STP Configuration Commands

21.1 SSTP Configuration Commands

21.1.1 spanning-tree mode

Description

To switch between RSTP and SSTP modes, use the **spanning-tree mode** command. To return to the default settings, use the negative form of this command.

spanning-tree mode {**rstp|sstp**}

no spanning-tree mode

Parameter

Parameter	Description
rstp	Enables RSTP mode
sstp	Enbales SSRP mode

Default

SSTP

Instruction

None

Command mode

Global configuration

Example

The following example enables SSTP mode:

```
Switch(config)# spanning-tree mode sstp
Switch(config)#
```

21.1.2 spanning-tree sstp priority

Description

To set the sstp bridge priority, use the **spanning-tree sstp priority** command. To return to the default settings, use the negative form of this command.

spanning-tree sstp priority *value*

no spanning-tree sstp priority

Parameter

Parameter	Description
value	Value is from 0 to 61440.

Default

32768

Instruction

The switch becomes the root of the whole network spanning-tree when configured the priority value. You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

Command mode

Global configuration

Example

This example shows how to set the SSTP priority:

```
Switch(config)# spanning-tree sstp priority 4096
Switch(config)#
```

21.1.3 spanning-tree sstp hello-time

Description

To set the hello-time delay timer, use the **spanning-tree sstp hello-time** command. To return to the default settings, use the negative form of this command.

spanning-tree sstp hello-time *time*

no spanning-tree sstp hello-time

Parameter

Parameter	Description
time	Number of seconds to set the hello-time delay timer; valid values are from 1 to 10 seconds.

Default

4s

Instruction

The hello-time configured by the local switch is valid only when the local switch is the root switch.

Command mode

Global configuration

Example

The following example sets the SSTP hello-time to 8 seconds:

```
Switch(config)# spanning-tree sstp hello-time 8
Switch(config)#
```

21.1.4 spanning-tree sstp max-age

Description

To set the SSTP max-age timer, use the **spanning-tree sstp max-age** command. To return to the default settings, use the negative form of this command.

spanning-tree sstp max-age *time*

no spanning-tree sstp max-age

Parameter

Parameter	Description
seconds	Number of seconds to set the max-age timer; valid values are from 6 to 40 seconds.

Default

20s

Instruction

None

Command mode

Global configuration

Example

This example shows how to set the max-age timer：

Switch(config)# spanning-tree sstp max-age 24
Switch(config)#

21.1.5 spanning-tree sstp forward-time

Description

To set the forward-delay timer, use the **spanning-tree sstp forward-time** command in global configuration mode. To return to the default settings, use the negative form of this command.

spanning-tree sstp forward-time *time*

no spanning-tree sstp forward-time

Parameter

Parameter	Description
time	Number of seconds to set the forward-delay timer; valid values are from 4 to 30 seconds.

Default

15 seconds

Instruction

None

Command mode

Global configuration

Example

The following example shows how to set forward delay timer:

```
Switch(config)# spanning-tree sstp forward-delay 20
Switch(config)#
```

21.1.6 spanning-tree sstp cost

Description

To set the path cost of the interface for SSTP calculations, use the **spanning-tree sstp cost** command in interface configuration mode. To revert to the default value, use the negative form of this command.

spanning-tree sstp cost *value*

no spanning-tree sstp cost

Parameter

Parameter	Description
value	Path cost. Valid values are from 1 to 200000000

Default

10M Ethernet:100

100M Ethernet: 19

1000M Ethernet: 1

Instruction

None

Command mode

Interface configuration

Example

This example shows how to set a path cost value of 100 for the spanning tree VLAN associated with the interface F1/10:

```
Switch(config_f0/10)#spanning-tree sstp cost 100
Switch(config_f0/10)#
```

21.1.7 spanning-tree cost

Description

To set the path cost of the interface for Spanning Tree Protocol (STP) calculations, use the **spanning-tree cost** command in interface configuration mode. To revert to the default value, use the negative form of this command.

spanning-tree cost *value*

no spanning-tree cost

Parameter

Parameter	Description
value	Path cost; valid values are from 1 to 200000000

Default

The default path cost is computed based on the bandwidth setting of the interface.

Instruction

The configuration result of this command is valid to all spanning-tree modes. In STP mode, the path cost of all VLAN spanning-trees on the interface will be updated. In MSTP mode, the path cost of all spanning-tree examples will be updated.

However, the configuration result of the command will not influence the independent configuration in various modes. For example, the switch respectively configured with

the spanning-tree sstp cost 100 and the spanning-tree cost 110 in SSTP mode, the port priority will be 100.

Command mode

Interface configuration mode

Example

This example shows how to set a path cost value of 24 for the spanning tree VLAN associated with that interface:

```
Switch(config_f0/0)# spanning-tree cost 24
Switch(config_f0/0)#
```

21.1.8 spanning-tree sstp port-priority

Description

To set the priority value in SSTP mode, use the spanning-tree sstp port-priority command. Use the negative form of this command to restore the default value.

spanning-tree sstp port-priority *value*

no spanning-tree sstp port-priority

Parameter

Parameter	Description
value	Port priority Value range is from 0 to 255.

Default

128 (0x80)

Instruction

The port priority must be set in increments of 16 only.

Command mode

Interface configuration

Example

The following example sets 32 as the priority value on interface f0/0:

Switch(config_f0/0)# spanning-tree sstp port-priority 32
Switch(config_f0/0)#

21.1.9 spanning-tree port-priority

Description

To prioritize an interface when two bridges compete for position as the root bridge, use the **spanning-tree port-priority** command. The priority you set breaks the tie. To revert to the default setting, use the negative form of this command.

spanning-tree port-priority *value*

no spanning-tree port-priority

Parameter

Parameter	Parameter
value	Port priority。Value is from 0 to 255，

Default

Port priority value is 128

Instruction

The configuration result of this command is valid to all spanning-tree modes. In STP mode, the priority of all VLAN spanning-trees on the interface will be updated. In MSTP mode, the priority of all spanning-tree examples will be updated.

But the configuration result of the command will not influence the independent configuration in various modes. For example, the switch respectively configured with the spanning-tree sstp port-priority 100 and the spanning-tree port-priority 110 in SSTP mode, the port priority will be 100.

Command mode

Interface configuration

Example

This example shows how to set the priority value:

Switch(config_f1/10)#spanning-tree port-priority 16
Switch(config_f1/10)#

21.1.10 show spanning-tree

Description

To display spanning-tree information for the specified spanning-tree instances, use the show spanning-tree command.

show spanning-tree [detail | interface *intf-i*]

Parameter

Parameter	Description
intf-i	Pory name，like F0/10, G1/1

Default

None

Instruction

Show spanning-tree state.

Command mode

Interface configuration/EXEC/global configuration

Example

```
Switch_config#show span

Spanning tree enabled protocol SSTP

SSTP
  Root ID         This bridge is the root

  Bridge ID       Priority                32768
                  Address                 00E0.0F64.8365
                  Hello/MaxAge/FwdDly     4/20/15(s)

Intf        Port ID                         Designated              Port ID
Name        Pri.Nbr Role Sts Cost           Bridge ID               Pri.Nbr Cost
--------- ------- ---- --- --------- -------------------- ------- ---------
F0/47       128.47  Desg LIS 12             32768 00E0.0F64.8365 128.47   0
```

Switch_config#

21.2 RSTP Configuration Commands

21.2.1 spanning-tree mode rstp

Description

To enable RSTP feature, use the **spanning-tree mode rstp** command. Use the negative form of this command to disable RSTP.

spanning-tree mode rstp

no spanning-tree mode

Parameter

None

Default

RSTP disabled, SSTP enabled

Instruction

None

Example

The following example enables rstp on the switch:

```
switch(config)# spanning-tree mode rstp
switch(config)#
```

21.2.2 spanning-tree rstp forward-time

Description

To set the rstp forward-delay timer, use the **spanning-tree rstp forward-time** command in global configuration mode. To return to the default settings, use the negative form of this command.

spanning-tree rstp forward-time *time*

no spanning-tree rstp forward-time

Parameter

Parameter	Description
time	Number of seconds to set the forward-delay timer; valid values are from 4 to 30 seconds.

Default

15 seconds

Instruction

None

Example

The following example sets 20 seconds as the rstp forward-delay timer:

```
switch(config)# spanning-tree rstp forward-time 20
switch(config)#
```

21.2.3 spanning-tree rstp hello-time

Description

To set the RSTP hello-time delay timer, use the **spanning-tree rstp hello-time** command in global configuration mode. To return to the default settings, use the negative form of this command.

spanning-tree rstp hello-time *time*

no spanning-tree rstp hello-time

Parameter

Parameter	Description
time	Number of seconds to set the hello-time delay timer; valid values are from 1 to 10 seconds.

Default

4 seconds

Instruction

The hello-time configured by the local switch is valid only when the local switch is the root switch.

Example

The following example sets 8 seconds as the rstp hello-time:

```
switch(config)# spanning-tree rstp hello-time 8
switch(config)#
```

21.2.4 spanning-tree rstp max-age

Description

To set the RSTP max-age timer, use the **spanning-tree rstp max-age** command. To return to the default settings, use the negative form of this command.

spanning-tree rstp max-age *time*

no spanning-tree rstp max-age

Parameter

parameter	description
time	Number of seconds to set the max-age timer; valid values are from 6 to 40 seconds.

Default

20 seconds

Instruction

None

Example

The following example sets 24 seconds as the rstp max-age timer:

```
switch(config)# spanning-tree rstp max-age 24
switch(config)#
```

21.2.5 spanning-tree rstp priority

Description

To set the rstp bridge priority, use the **spanning-tree rstp priority** command. To return to the default settings, use the negative form of this command.

spanning-tree rstp priority *value*

no spanning-tree rstp priority

Parameter

Parameter	Description
value	Bridge priority。Value is from 0 to 61440，

Default

32768

Instruction

none

Example

The following example sets 4096 as the bridge priority:

```
switch(config)# spanning-tree rstp priority 4096
switch(config)#
```

21.2.6 spanning-tree rstp cost

Description

To set the path cost of the interface, use the **spanning-tree rstp cost** command. To revert to the default value, use the negative form of this command.

spanning-tree rstp cost *value*

no spanning-tree rstp cost

Parameter

Parameter	Description
value	Path cost Value range is from 1 to 200000000.

Default

The default path cost is computed based on the bandwidth setting of the interface.

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

Instruction

none

Example

The following example sets a path cost value of 24 for the interface f0/0:

```
switch(config_f0/0)# spanning-tree rstp cost 24
switch(config_f0/0)#
```

21.2.7 spanning-tree rstp port-priority

Description

To set an interface priority, use the **spanning-tree rstp port-priority** command. To revert to the default value, use the negative form of this command.

spanning-tree rstp port-priority *value*

no spanning-tree rstp port-priority

Parameter

Parameter	Description
value	Port priority; valid values are from 0 to 255.

Default

128

Instruction

None

Example

The following example sets 24 as the priority value on interface f0/0:

```
switch(config_f0/0)# spanning-tree rstp port-priority 24
switch(config_f0/0)#
```

Chapter 22 MSTP Configuration Commands

Note:

Switches such as S2116, S2448, S3448 and 6508 support the MSTP mode. See relative documents about device models and version explanation.

22.1 MSTP Configuration Command

22.1.1 spanning-tree mode mstp

Command description

spanning-tree mode mstp

no spanning-tree mode

Run the **spanning-tree mode mstp** command to set the running mode of STP to **MSTP**. Run the **no spanning-tree mode** command to disable STP.

Parameter

None

Default

The MSTP mode is closed, while the SSTP mode is running.

Usage description

None

Example

The following commands are used to enable the MSTP protocol on the switch:

```
switch(config)# spanning-tree mode mstp
switch(config)#
```

22.1.2 spanning-tree mstp name

Command description

spanning-tree mstp name *string*

no spanning-tree mstp name

Run the **spanning-tree mstp name *string*** command to configure the regional name of the STP. Run the **no spanning-tree mstp name** command to resume the default name.

Parameter

Parameter	Description
String	Configures the character string of the name. The character string can have up to 32 characters, capital sensitive. The default value is in the form of character string like the MAC address of the switch.

Default

Character string form of the switch's MAC address

Usage description

None

Example

The following commands are used to set the configuration name of the switch's STP to **reg-01**.

```
switch(config)# spanning-tree mstp name reg-01
switch(config)#
```

22.1.3 spanning-tree mstp revision

Command description

spanning-tree mstp revision *value*

no spanning-tree mstp revision

Run the **spanning-tree mstp revision *value*** command to generate the revision number of STP. Run the **no spanning-tree mstp revision** to restore the revision number to the default value.

Parameter

Parameter	Description
Value	Revision number: 0 ~65535 Its default value is **0**.

Default

The default value of the revision number is **0**.

Usage description

None

Example

The following commands are used to set the regional revision number of STP to **100**.

```
switch(config)# spanning-tree mstp revision 100
switch(config)#
```

22.1.4 spanning-tree mstp instance

Command description

spanning-tree mstp instance *instance-id* **vlan** *vlan-list*

no spanning-tree mstp instance *instance-id*

Run the command **spanning-tree mstp instance *instance-id* vlan *vlan-list*** to map the VLAN to the MSTI. Run the command **no spanning-tree mstp instance** *instance-id* to re-map the VLAN to the CIST.

Parameter

Parameter	Description
instance-id	Instance number of the STP, meaning an MSTI which ranges from 1 to 15.
vlan-list	VLAN list which is mapped to the STP, ranging from 1 to 4094.

Default

All VLANs are mapped to the CIST (MST00).

Usage description

instance-id is an unique value representing an STP instance.

vlan-list represents a VLAN group, such as “1,2,3”, “1-5” and “1,2,5-10”.

Example

The following commands map VLAN1 to instance 1 of STP, and VLAN5,7,10-20 to instance 2 of STP, and then re-map these VLANs to MST00.

switch(config)# spanning-tree mstp instance 1 vlan 2
switch(config)# spanning-tree mstp instance 2 vlan 5,7,10-20
switch(config)# no spanning-tree mstp instance 2

22.1.5 spanning-tree mstp root

Command description

spanning-tree mstp *instance-id* **root** {**primary** | **secondary**}

[**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mstp root

Configure the specified MSTP instance to the primary/secondary root. Run its negative form to restore the priority of MSTP instance to the default value.

Both the **diameter** command and the **hello-time** command can modify the network diameter and the **HelloTime** parameter of the MSTP when they are setting the root.

Parameter

Parameter	Description
instance-id	MSTP instance, ranging from 0 to 15
Primary	Sets the MSTP instance to the primary root.
Secondary	Sets the MSTP instance to the secondary root.
net-diameter	Network diameter, which is optional When the **instance-id** parameter is **0**, it is effective. It ranges from 2 to 7.
Seconds	Hello time, an optional parameter, which ranges from 1 to 10 seconds

Default

The priority value of all default roots of all MSTP instances are 32768, the network diameter is 7 and the HelloTime is 2 seconds.

Usage description

Both the **diameter** command and the **hello-time** command are valid only when **instanc-id** is **0**.

Generally, after you run the command to set the primary root, the protocol automatically checks the ID of the current network root and then sets the priority field of the root identifier to 24576 if this value gurantees the current switch to be the root of the MSTP instance. If the priority value of the root is smaller than 24576, the protocol will automatically set the MSTP priority of the current root to a value which is 4096 smaller than the root's priority. Here, 4069 is the step of the root priority.

Different from the configuration of the primary root, the protocol directly sets the MSTP priority of the switch to **28672** after the command for configuring the secondary root is run. Thus, the current switch can be the secondary root when the priorities of other switches are the default value **28672**.

Example

The following commands are used to set tbe switch to the primary root in the CIST and recalculate the time parameter of the MSTP through network diameter 3 and HelloTime3, and at last set the switch to the secondary root in the MST01.

```
switch(config)# spanning-tree mstp 0 root primary diameter 3 hello-time 3
switch(config)# spanning-tree mstp 1 root secondary
```

22.1.6 spanning-tree mstp priority

Command description

spanning-tree mstp *instance-id* **priority** *value*

no spanning-tree mstp priority

It is used to configure the bridge priority of the MSTP instance. Its negative form is used to resume the default value of the priority.

Parameter

Parameter	Description
instance-id	MSTP instance number, ranging from 0 to 15
Value	Bridge priority, which can be one of the given values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Default

The default priority of the bridges of all MSTP instances is 32768.

Usage description

Each priority value in the MSTP instance is independent and can be configured independently.

Example

The following commands are used to set the priority of the switch in the CIST and MST01 to 4096 and 8192 respectively.

```
switch(config)# spanning-tree mstp 0 priority 4096
switch(config)# spanning-tree mstp 1 priority 8192
```

22.1.7 spanning-tree mstp hello-time

Command description

spanning-tree mstp hello-time *seconds*

no spanning-tree mstp hello-time

It is used to configure the hello-time of the MSTP, and its negative form is used to resume the default settings of the HelloTime.

Parameter

Parameter	Description
Seconds	It ranges from 1 to 10 seconds. Its default value is 2 seconds.

Default

Two seconds

Usage description

None

Example

The following commands are used to set the HelloTime of the MSTP to **10**.

```
switch(config)# spanning-tree mstp hello-time 10
switch(config)# no spanning-tree mstp hello-time
```

22.1.8 spanning-tree mstp forward-time

Command description

spanning-tree mstp forward-time *seconds*

no spanning-tree mstp forward-time

It is used to configure the Forward Delay of the MTSP. Its negative is used to resume the default settings.

Parameter

Parameter	Description
Seconds	It ranges from 4 to 30 seconds. Its default value is 15 seconds.

Default

15 seconds

Usage description

None

Example

The following commands are used to set the **Forward Delay** parameter of the MTSP to **10**.

```
switch(config)# spanning-tree mstp forward-time 10
switch(config)# no spanning-tree mstp forward-time
```

22.1.9 spanning-tree mstp max-age

Command description

spanning-tree mstp max-age *seconds*

no spanning-tree mstp max-age

It is used to configure the **Max Age** parameter of the MSTP. Its negative is used to resume the default settings.

Parameter

Parameter	Description

Seconds	Range: 6 – 40 seconds The default value is 20 seconds.

Default

20 seconds

Usage description

None

Example

The following commands are used to set the **MaxAge** parameter of the MSTP to **10**.

switch(config)# spanning-tree mstp max-age 10
switch(config)# no spanning-tree mstp max-age

22.1.10 spanning-tree mstp diameter

Command description

spanning-tree mstp diameter *net-diameter*

no spanning-tree mstp diameter

It is used to configure the network diameter of the MSTP. Its negative is used to resume the default settings.

Parameter	Description
net-diameter	Range: 2 – 7 Its default value is 7.

Default

The default network diameter is 7.

Usage description

The **net-diameter** parameter is not saved as an independent settings in the switch. The time parameter that is modified through network diameter configuration can be saved. The **net-diameter** parameter is valid in the CIST. After settings, the three time parameters of the STP can be automatically updated to a relatively advantageous value.

It is recommended to set the time parameters of the STP through root configuration or network diameter configuration. In this way, the reasonability of the time parameters can be assured.

Example

The following first command is to set the bridge diameter of MSTP to 5. The second command is to resume the default value of the bridge diameter.

switch(config)# spanning-tree mstp diameter 5
switch(config)# no spanning-tree mstp diameter

22.1.11 spanning-tree mstp max-hops

Command description

spanning-tree mstp max-hops *hop-count*

no spanning-tree mstp max-hops

The **spanning-tree mstp max-hops** ***hop-count*** command is used to set the maximum number of hops of the MSTP BPDU. Its negative is used to resume the default settings.

Parameter

Parameter	Description
hop-count	Range: 1 -40 Its default value is 20.

Default

The default vaue of the maximum hop counts is 20.

Usage description

None

Example

The first command is to set the maximum hop counts of the MSTP BPDU to 5. The second command is to restore the default value of the maximum hop counts.

switch(config)# spanning-tree mstp max-hops 5
switch(config)# no spanning-tree mstp max-hops

22.1.12 spanning-tree mstp port-priority

Command description

spanning-tree mstp *instance-id* **port-priority** *value*

no spanning-tree *instance-id* **port-priority**

The **spanning-tree mstp *instance-id* port-priority *value*** command is used to the port priority in the specified STP instance. Its negative is used to resume the default settings.

Parameter

Parameter	Description
instance-id	Number of the STP instance, ranging from 0 to 15
Value	Port priority, which is one of the following values: 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240

Default

The default priority value of the port in all STP instances is 128.

Usage description

None

Example

The first command is to set the priority of port F0/1 in the CIST to 16. The second command is to resume the default value.

```
switch(config_f0/1)# spanning-tree mstp 0 port-priority 16
switch(config_f0/1)# no spanning-tree mstp 0 port-priority
```

22.1.13 spanning-tree mstp cost

Command description

spanning-tree mstp *instance-id* **cost** value

no spanning-tree mstp *instance-id* **cost**

The command **spanning-tree mstp *instance-id* cost value** is used to set the path cost of the port in the specified STP instance. Its negative is used to resume the default settings.

Parameter

Parameter	Description
instance-id	Number of the STP instance, ranging from 0 to 15
Value	Path cost of the port, ranging from 1 to 200000000

Default

It depends on the connection rate of the port:

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

Usage description

None

Example

The following commands are used to set the path cost of port F0/1 in the CIST to **200**.

```
switch(config_f0/1)# spanning-tree mstp 0 cost 200
switch(config_f0/1)#
```

22.1.14 spanning-tree mstp point-to-point

Command description

spanning-tree mstp point-to-point { **force-true** | **force-false** | **auto** }

no spanning-tree mstp point-to-point

The command **spanning-tree mstp point-to-point { force-true | force-false | auto }** is used to configure the connection type of the port. Its negative is used to resume the default settings.

Parameter

Parameter	Description
force-true	**Sets the port connection type to** point-to-point**.**
force-false	**Sets the port connection type to** shared**.**
Auto	**Checks the port connection type automatically.**

Default

The MSTP protocol will automatically check the port connection type.

Usage description

None

Example

The following commands are to set the connection type of port F0/1 to **shared**.

```
switch(config_f0/1)# spanning-tree mstp point-to-point force-false
switch(config_f0/1)#
```

22.1.15 spanning-tree mstp mst-compatible

Command description

spanning-tree mstp mst-compatible

no spanning-tree mstp mst-compatible

Activate or shut down the MST-compatible mode.

Parameter

None

Default

The MSTP-compatible mode is not activated.

Usage description

After the MST-compatible mode is enabled, configure other connected switches that are running other MSTP protocols to the roots of CIST, ensuring that the switch can enter the MSTP-compatible mode by receiving the message.

Example

The following command is to activate the MST-compatible mode in global configuration mode:

```
switch(config)#spanning-tree mstp mst-compatible
```

22.1.16 spanning-tree mstp migration-check

Command description

spanning-tree mstp migration-check

Clear the STP information that is checked by the port, and restart the protocol conversion process.

Parameter

None

Default

None

Usage description

The command is valid in global configuration mode and in port configuration mode.

Example

The following commands are used to check the protocol conversion on all ports first, and then check the protocol conversion on port F0/1 again.

```
switch(config)# spanning-tree mstp migration-check
switch(config)# interface f 0/1
switch(config_f0/1)# spanning-tree mstp migration-check
```

22.1.17 show spanning-tree mstp

Command description

show spanning-tree mstp [**instance** *instance-id*]

The command above is used to check the MSTP information. If you run the command **show spanning-tree mstp**, the information about all STP instances is displayed.

Parameter

Parameter	Description
instance-id	**Number of the STP instance, ranging from 0 to 15**

Default

None

Usage description

It is valid in monitoring mode, global configuration mode or port mode.

Example

The following shows how to view all STP instances through the command. Here, **MST00** stands for CIST, and the **Type** field stands for the port connection type.

```
Switch#show spanning-tree mstp

MST00          Vlans Mapped:   1,4-4094
Root         Address   00E0.0F64.8365   Priority   32768 (32768 mst-id 0)
Root           This root is the CIST and regional root
Configured   Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times   Hello Time 2, Forward Delay 15, Max Age 20

Interface           Role Sts Cost         Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
F0/1                Desg FWD 200000       128.1     P2p
F0/3                Back BLK 200000       128.3     P2p
F0/47               Desg FWD 200000       128.47    Edge

MST01          Vlans Mapped:   2
Root         Address   00E0.0F64.8365   Priority   32769 (32768 mst-id 1)
Root           This root for MST01

Interface           Role Sts Cost         Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
F0/1                Desg FWD 200000       128.1     P2p

MST02          Vlans Mapped:   3
Root         Address   00E0.0F64.8365   Priority   32770 (32768 mst-id 2)
Root           This root for MST02

Interface           Role Sts Cost         Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
F0/1                Desg FWD 200000       128.1     P2p
```

22.1.18 show spanning-tree mstp region

Command description

show spanning-tree mstp region

Check the regional configuration information about the MSTP.

Parameter

None

Default

None

Usage description

None

Example

See the following information. **MST Config Table** shows the relation between VLAN and STP instance.

```
switch(config)# show spanning-tree mstp region

MST Region:
  Name:      [reg01]
  Revision:[0]

MST Config Table:
  Instance        VLAN IDs
----------        ----------
         0        1,4-4094
         1        2
         2        3
```

22.1.19 show spanning-tree mstp detail

Command description

show spanning-tree mstp detail

The command above is used to check the detailed information about MSTP.

Parameter

None

Default

None

Usage description

None

Example

The following example shows the detailed STP information after the command is run, including the port connection type and optional characteristics:

```
Switch#show spanning-tree mstp detail

MST00          Vlans Mapped:   1,4-4094
Root           Address   00E0.0F64.8365   Priority   32768 (32768 mst-id 0)
Root           This root is the CIST and regional root
Configured     Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times     Hello Time 2, Forward Delay 15, Max Age 20

FastEthernet0/1 of MST00 is designated forwarding
Port Info                  Port ID 128.1              Priority 128       Cost 200000
Designated Root            Address 00E0.0F64.8365   Priority 32768   Cost 0
CIST Regional Root         Address 00E0.0F64.8365   Priority 32768   Cost 0
Designated Root          Address 00E0.0F64.8365   Priority 32768   Port ID 128.1
Edge Port:      disabled                    Link Type:    point-to-point (auto)
Bpdu Guard:    disabled (default)          Root Guard: disabled (default)
Loop Guard:    disabled (default)
Timers:    message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
Bpdu sent 335, received 5

FastEthernet0/3 of MST00 is backup blocking
Port Info                  Port ID 128.3              Priority 128       Cost 200000
Designated Root            Address 00E0.0F64.8365   Priority 32768   Cost 0
CIST Regional Root         Address 00E0.0F64.8365   Priority 32768   Cost 0
Designated Root          Address 00E0.0F64.8365   Priority 32768   Port ID 128.1
Edge Port:      disabled                    Link Type:    point-to-point (auto)
Bpdu Guard:    disabled (default)          Root Guard: disabled (default)
Loop Guard:    disabled (default)
Timers:    message expires in 5 sec, forward delay 15 sec, up time 662 sec
Number of transitions to forwarding state: 0
Bpdu sent 5, received 335

FastEthernet0/47 of MST00 is designated forwarding
Port Info                  Port ID 128.47             Priority 128       Cost 200000
Designated Root            Address 00E0.0F64.8365   Priority 32768   Cost 0
CIST Regional Root         Address 00E0.0F64.8365   Priority 32768   Cost 0
Designated Root          Address 00E0.0F64.8365   Priority 32768   Port ID 128.47
Edge Port:      enabled (auto)              Link Type:    point-to-point (auto)
Bpdu Guard:    disabled (default)          Root Guard: disabled (default)
Loop Guard:    disabled (default)
Timers:    message expires in 0 sec, forward delay 0 sec, up time 1485 sec
Number of transitions to forwarding state: 1
```

Bpdu sent 744, received 0

MST01 Vlans Mapped: 2
Root Address 00E0.0F64.8365 Priority 32769 (32768 mst-id 1)
Root This root for MST01

FastEthernet0/1 of MST01 is designated forwarding
Port Info Port ID 128.1 Priority 128 Cost 200000
Designated Root Address 00E0.0F64.8365 Priority 32769 Cost 0
Desingated Root Address 00E0.0F64.8365 Priority 32769 Port ID 128.1
Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 335, received 0

MST02 Vlans Mapped: 3
Root Address 00E0.0F64.8365 Priority 32770 (32768 mst-id 2)
Root This root for MST02

FastEthernet0/1 of MST02 is designated forwarding
Port Info Port ID 128.1 Priority 128 Cost 200000
Designated Root Address 00E0.0F64.8365 Priority 32770 Cost 0
Desingated Root Address 00E0.0F64.8365 Priority 32770 Port ID 128.1
Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 335, received 0

22.1.20 show spanning-tree mstp interface

Command description

show spanning-tree mstp interface *interface-id*

The command above is used to check the information about the port which is run under MSTP.

Parameter

Parameter	Description
interface-id	**Port name, such as F0/1 and FastEtnernet0/3**

Default

None

Usage description

None

Example

The following example shows the information about port F0/1 after you run the command **show spanning-tree mstp interface f0/1**:

```
Switch#show spanning-tree mstp interface f0/1

FastEthernet0/1 of MST00 is designated forwarding
Port Info                 Port ID 128.1              Priority 128       Cost 200000
Designated Root           Address 00E0.0F64.8365     Priority 32768     Cost 0
CIST Regional Root        Address 00E0.0F64.8365     Priority 32768     Cost 0
Designated Root           Address 00E0.0F64.8365     Priority 32768     Port ID 128.1
Edge Port:      disabled                             Link Type:    point-to-point (auto)
Bpdu Guard:     disabled (default)                   Root Guard: disabled (default)
Loop Guard:     disabled (default)
Timers:    message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
Bpdu sent 430, received 5

FastEthernet0/1 of MST01 is designated forwarding
Port Info                 Port ID 128.1              Priority 128       Cost 200000
Designated Root           Address 00E0.0F64.8365     Priority 32769     Cost 0
Desingated Root           Address 00E0.0F64.8365     Priority 32769     Port ID 128.1
Timers:    message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 430, received 0

FastEthernet0/1 of MST02 is designated forwarding
Port Info                 Port ID 128.1              Priority 128       Cost 200000
Designated Root           Address 00E0.0F64.8365     Priority 32770     Cost 0
Desingated Root           Address 00E0.0F64.8365     Priority 32770     Port ID 128.1
Timers:    message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 430, received 0

Instance Role Sts Cost          Pri.Nbr Vlans Mapped
-------- ---- --- --------- ------- --------------------
0            Desg FWD 200000      128.1    1,4-4094
1            Desg FWD 200000      128.1    2
2            Desg FWD 200000      128.1    3show spanning-tree mstp protocol-migration
```

Command description

show spanning-tree mstp protocol-migration

The command above is used to check the protocol conversion information when the port is running under MSTP.

Parameter

None

Default

None

Usage description

None

Example

The following example shows the information about protocol conversion after the command **show spanning-tree mstp protocol-migration** is run. Note that port F0/2 has transferred to the 802.1D STP mode.

```
Switch#show spanning-tree mstp protocol-migration

MSTP Port Protocol Migration

Interface            Protocol     Info
---------------- ---------- --------------------------------------------------
F0/2                  802.1D
```

Chapter 23 STP Optional Characteristic Configuration Commands

23.1 STP Optional Characteristic Configuration Commands

23.1.1 spanning-tree portfast

Description

To enable bridge protocol data unit (BPDU) filtering by default on all PortFast ports, use the **spanning-tree portfast** command in global configuration mode. To return to the default settings, use the negative form of this command.

spanning-tree portfast {bpdufilter default | bpduguard default | default}

no spanning-tree portfast {bpdufilter default | bpduguard default | default}

To enable PortFast mode where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the spanning-tree portfast command in interface configuration mode. To return to the default settings, use the negative form of this command.

spanning-tree portfast [disable | trunk]

no spanning-tree portfast

Parameter

Parameter	Description
bpdufilter default	Enables bpdu flter.
bpduguard default	Enables bpdu guard.
default	Specifies the default method.

Default

Disabled

Instruction

In SSTP/PVST mode, the Port Fast characteristic makes a port immediately enter Forwarding state without experiencing any status change process. This configuration is invalid in RSTP/MSTP mode.

After configuring Port Fast, BPDU Guard or BPDU Filter needs to be configured for protection.

Command mode

Global or interface configuration mode

Example

This example shows how to enable PortFast mode globally:

```
Switch(config)# spanning-tree portfast default
Switch(config)#
```

This example shows how to enable PortFast mode on the interface f0/0:

```
Switch(config_f0/0)# spanning-tree portfast
Switch(config_f0/0)#
```

23.1.2 spanning-tree bpduguard

Description

To enable bridge protocol data unit (BPDU) guard on the interface, use the **spanning-tree bpduguard** command in interface configuration mode. To return to the default settings, use the negative form of this command.

spanning-tree bpduguard {**disable** | **enable**}

no spanning-tree bpduguard

Parameter

None

Default

Disabled

Instruction

In SSTP/PVST mode, if a port that configured BPDU Guard and Port Fast receives BPDU, this port will be forced to shutdown. User can restore it by the manual configuration. In RSTP/MSTP mode, if a port that configured BPDU Guard receives BPDU, this port will be configured to Blocking state for a period of time.

Command mode

Interface configuration

Example

This example shows how to enable BPDU guard on this interface:

```
Switch(config_f0/0)# spanning-tree bpduguard enable
Switch(config_f0/0)#
```

23.1.3 spanning-tree bpdufilter

Description

To enable bridge protocol data unit (BPDU) filtering on the interface, use the **spanning-tree bpdufilter** command in interface configuration mode. To return to the default settings, use the **negative form of** this command.

spanning-tree bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

Parameter

None

Default

Disabled

Instruction

In SSTP/PVST mode, if a port that configured BPDU Filter and Port Fast receives BPDU, the BPDU Filter and Port Fast characteristics on that port will be disabled automatically to restore the port to an ordinary port. Then this port must endure the wait from Listening to Learning before entering Forwarding state.

This feature is invalid in RSTP/MSTP mode.

Command mode

Interface configuration

Example

This example shows how to enable BPDU filtering on this interface:

```
Switch(config_f0/0)# spanning-tree bpdufilter enable
```

Switch(config_f0/0)#

23.1.4 spanning-tree uplinkfast

Description

To enable the debugging of the spanning-tree UplinkFast events, use the **debug spanning-tree uplinkfast** command. To disable the debugging output, use the negative form of this command.

spanning-tree uplinkfast [max-update-rate pkts-per-second]

no spanning-tree uplinkfast [*max-update-rate*]

Parameter

None

Default

disabled

Instruction

Uplink Fast characteristic is only valid in SSTP/PVST mode.

Command mode

Global configuration

Example

The following example enables uplinkfast characteristic:

Switch(config)# spanning-tree uplinkfast
Switch(config)#

23.1.5 spanning-tree backbonefast

Description

To enable debugging of the spanning-tree BackboneFast events, use the **debug spanning-tree backbonefast** command. To disable the debugging output, use the negative form of this command.

spanning-tree backbonefast

no spanning-tree backbonefast

Parameter

None

Default

Disabled

Instruction

Backbone Fast characteristic is only valid in SSTP/PVST mode.

Command mode

Global configuration

Example

The following command enables backbonefast characteristic:

```
Switch(config)# spanning-tree backbonefast
Switch(config)#
```

23.1.6 spanning-tree guard

Description

To enable or disable the guard mode, use the **spanning-tree guard** command in interface configuration mode. To return to the default settings, use the negative form of this command.

spanning-tree guard {loop | none | root}

no spanning-tree guard

Parameter

Parameter	Description
loop	Enables the loop-guard mode on the interface. Value is from 1 to 0xfe.
none	Sets the guard mode to none. Value is 48-bit.
root	Enables root-guard mode on the interface.

Default

Disabled

Instruction

Root Guard characteristic can prevent a port from becoming Root port due to receving high priority BPDU.

Loop Guard characteristic can protect a Root Port or a Alternate Port when it becomes the Designated Port. This function can prevent a port from occuring the loop when it cannot continuously receive BPDU.

Command mode

Interface configuration

Example

This example shows how to enable root guard:

```
Switch(config_f0/0)# spanning-tree guard root
Switch(config_f0/0)#
```

23.1.7 spanning-tree loopguard

Description

To enable loop guard as a default on all ports of a given bridge, use the **spanning-tree loopguard default** command in global configuration mode. To disable loop guard, use the **negative form of** this command.

spanning-tree loopguard default

Parameter

None

Default

None

Instruction

None

Command mode

Global configuration

Example

The following command enables loopguard function:

```
Switch(config)# spanning-tree loopguard default
Switch(config)#
```

Chapter 24 Link Aggregation Configuration Commands

24.1 Link Aggregation Configuration Commands

24.1.1 aggregator-group

Description

To configure interface aggregation, use the **aggregator-group** command. Use the negative form of this command to restore the default value.

aggregator-group *id* mode {lacp-negotiation |static }

no aggregator-group

Parameter

Parameter	Description
id	ID number of the logical port. Value range: none.
lacp-negotiation	Uses LACP negotiation. Value range:N/A.
static	Negotiation is not used on an port. Value range:N/A.

Default

Disabled

Instruction

Port link aggregation is to bind several ports with the familiar attrubute to one logical port. LACP negotiation can be used to form binding process. Also the binding process can be forced to be formed without any LACP negotiation .

If the static aggregation is used, please make sure the attribute of the ports to be binded is the same,that is, they are all full-duplex mode and with the same rate. Meantime make sure the connection of the ports to be binded is peer-to-peer connection. Also the remote ports of the peer-to-peer connection are also binded to one logical port.

You can select LACP negotiation mode when configuring port aggregation. Active—Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets. Passive—Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.

Switches of partial models doesn't support dynamic negotiation mode, therefore relevant configuration commands are not provided.

Command mode

Interface configuration mode

Example

Switch(config_f0/24)#aggregator-group 3 mode lacp-negotiation
Creating a port-aggregator interface Port-aggregator3
Switch(config_f0/24)#int f0/23
Switch(config_f0/23)#aggregator-group 3 mode lacp-negotiation

24.1.2 aggregator-group load-balance

Description

To configure the load balance after port aggregation, use the **aggregator-group load-balance** command. Use the negative form of this command to restore the default value.

aggregator-group load-balance { dst-mac| src-mac| both-mac | src-ip | dst-ip | both-ip }

no aggregator-group load-balance

Parameter

parameter	description
dst-mac	Sets destination mac address as standard. Value range: N/A.
src-mac	Sets source mac address as standard. Value range: N/A.
both-mac	Sets source and destination mac address as standard. Value range:N/A.
dst-ip	Sets destination ip address as standard. Value range:N/A.
src-ip	Sets source ip address as standard. Value range:N/A.
both-ip	Sets source and destination ip address as standard. Value range:N/A.

Default

dst-mac

Instruction

To ensure load balance of each physical port after port aggregation, use this command to equably distribute data flow on each physical port.

When dst-mac mode is selected, the distribution of data flow sets destination MAC address of the data packet as standard. The same MAC address is only sent out on a certain physical interface. The src-mac uses source MAC address as standard.

The supporting capability in load balance policy varies according to different models of switches. The command prompt only shows the sharing policy that the switch supports. If the switch doesn't support any sharing polich or just supports one of them, the relevant subcommands will not be displayed.

Command mode

Global configuration mode

Example

The following command modifies load balance of the port-aggregator 3 to src mode:

Switch(config)#**port-aggregator load-balance 3 src-mac**
Switch(config)#

24.1.3 show aggregator-port

Description

To show the concrete information of aggregator-group, use the **show aggregator-port** command.

show aggregator-port [*id*] {detail|brief|summary}

Parameter

parameter	Description
id	Concrete logical port ID

Default

None

Instruction

This command is used to show port aggregation information.

Command mode

EXEC/ All configuration modes

24.1.4 show interface port-aggregator

Description

To show concrete information of the aggregator-group, use the **show interface port-aggregator** command.

show interface port-aggregator *id*

Parameter

Parameter	Description
id	The concrete port ID, in the range from 1 to 16.

Default

none

Instruction

This command is used to show port aggregation information.

Command mode

EXEC/All configuration modes

Example

The following example shows information about port-aggregator 1.

```
Switch#sho int po1
Port-aggregator1 is down, line protocol is down
  Hardware is PortAggregator, Address is 0000.0000.0000(0000.0000.0000)
  MTU 1500 bytes, BW 1000 kbit, DLY 2000 usec
  Encapsulation ARPA, loopback not set
  Members in this Aggregator:
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 multicasts
```

0 input errors, 0 input discards
0 CRC, 0 frame, 0 overrun, 0 ignored
0 packets output, 0 bytes, 0 underruns
Transmited 0 broadcasts, 0 multicasts
0 output errors, , 0 discards
0 output buffer failures, 0 output buffers swapped out

Note: Members in this Aggregator indicates the physical port aggregated to the logical port.

Statistics descriptions are as follows：

Packets input indicates total number of error-free packets received by the system, including unicasts, multicasts and broadcasts.

Bytes indicate total number of in the error-free packets received by the system.

Broadcasts indicate total number of broadcast packets received by the interface.

Multicasts indicate total number of multicast packets received by the interface.

Input errors indicate the received error packets.

Input discards indicate the received packets are discarded, like the received packets when the interface protocol is down.

Packets output indicates total number of messages transmitted by the system, including unicasts, multicasts and broadcasts.

Bytes indicate total number of bytes transmitted by the system.

Broadcasts indicate total number of broadcast packets transmitted by the system.

Multicasts indicate total number of multicast packets transmitted by the system.

Input errors indicate the sending error packets.

Input discards indicate the sending packets are discarded, like the sending packets when the interface protocol is down.

24.1.5 debug lacp errors

Description

To debug LACP errors information, use the **debug lacp errors** command.

debug lacp errors

no debug lacp errors

Parameter

None

Default

None

Instruction

This command is used to debug all errors information during lacp operation to locate the error.

Command mode

EXEC

Example

Switch# debug lacp error
Switch#

24.1.6 debug lacp state

Description

To debug lacp state, use the **debug lacp state** command.

debug lacp state

no debug lacp state

Parameter

None

Default

None

Command mode

EXEC

Example

Switch# debug lacp state
Switch#

24.1.7 debug lacp packet

Description

To debug lacp packet information, use the **debug lacp packet** command.

debug lacp packet

no debug lacp packet

Parameter

None

Default

None

Command mode

EXEC

Example

Switch# debug lacp packet
Switch#

Chapter 25 PDP Configuration Commands

25.1 PDP Configuration Commands

PDP commands are listed below:

- pdp timer
- pdp holdtime
- pdp version
- pdp run
- pdp enable
- show pdp traffic
- show pdp neighbor

25.1.1 pdp timer

Syntax

[no|default] pdp timer seconds

It is used to set the time of the PDP timer.

Parameter

Parameter	Description
seconds	Means the interval for PDP to transmit packets outside, which ranges from 5 seconds to 254 seconds.

Default value

The default settings is 60 seconds.

Explanation

This command is configured in global configuration mode.

Example

The following example shows that a switch transmits PDP packets every 5 seconds.

pdp timer 5

25.1.2 pdp holdtime

Syntax

[no|default] pdp holdtime seconds

It is used to set the PDP holdtime.

Parameter

Parameter	Description
seconds	Means the time needed for deleting the neighbor information, which ranges from 10 to 255 seconds.

Default value

The default settings is 180 seconds.

Explanation

This command is configured in global configuration mode.

Example

The following example shows that the neighbor information is kept for 15 seconds.

pdp holdtime 15

25.1.3 pdp version

Syntax

[no] pdp version <1|2>

It is used to set the PDP version.

Parameter

Parameter	Description
version	Means the PDP version, which is 1 or 2.

Default value

The default version is version 2.

Explanation

This command is configured in global configuration mode.

Example

The following example shows that the PDP version of a switch is version 1.

```
pdp version 1
```

25.1.4 pdp run

Syntax

[no] pdp run

It is used to enable PDP.

Parameter

None

Default value

The PDP protocol is disabled.

Explanation

This command is configured in global configuration mode.

Example

The following example shows to disable PDP.

```
no pdp run
```

25.1.5 pdp enable

Syntax

[no] pdp enable

It is used to enable or disable PDP on a port.

Parameter

N/A

Default value

PDP is enabled by default.

Explanation

This command is set in port configuration mode and takes effect in port or global mode only when PDP is enabled.

Example

The following example shows that PDP is disabled on port f0/1.

```
switch_config_f0/1#no pdp enable
```

25.1.6 show pdp traffic

Syntax

```
show pdp traffic
```

It is used to display the number of received PDP packets.

Parameter

N/A

Default value

N/A

Explanation

It is used to browse the running of PDP.

Example

```
Switch_config#show pdp traffic
Packets output: 253491, Input: 0
Hdr syntax: 0, Chksum error: 0
```

No memory: 0, Invalid packet: 0

25.1.7 show pdp neighbor

Syntax

show pdp neighbor

It is used to display the PDP neighbor.

Parameter

N/A

Default value

N/A

Explanation

It is used to browse the running of PDP neighbor.

Example

Switch_config#show pdp neighbor

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

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

Device-ID	Local-Intf	Hldtme	Port-ID	Platform	Capability
Switch	Fas0/1	169	Gig0/1	, RISC	R S

Chapter 26 LLDP Configuration Commands

26.1 LLDP Commands

26.1.1 lldp run

Description

lldp run

no lldp run

To start up LLDP, run **lldp run**; to shut down LLDP, run **no lldp run**.

Parameter

None

Default

Shut down

Explanation

None

Command mode

Global configuration mode

Example

The following command is used to start up LLDP.

```
Switch_config# lldp run
```

26.1.2 lldp holdtime

Description

lldp holdtime *time*

no lldp holdtime

To configure the ttl value of LLDP, run **lldp holdtime *time***. To resume the default transmission delay, run **no lldp holdtime**.

Parameter

Parameter	Description
time	Storage time of the transmitted message, ranging between zero to 65535 seconds

Default

120s

Explanation

None

Command mode

Global configuration mode

Example

The following example shows how to set the ttl value of LLDP to 100 seconds.

```
Switch_config# lldp holdtime 100
Switch_config#
```

26.1.3 lldp timer

Description

lldp timer *time*

no lldp timer

To configure the transmission delay of LLDP, run **lldp timer time**. To resume the default transmission delay, run **no lldptimer**.

Parameter

Parameter	Description
time	Interval for transmitting the LLDP message, ranging between 5 to 65534 seconds.

Default

30s

Explanation

The transmission interval of the LLDP message must be shorter than its storage time, ensuring multiple updates in the storage time and preventing error which is led by packet loss.

Command mode

Global configuration mode

Example

The following example shows how to configure the transmission interval of LLDP to 24 seconds.

```
Switch_config# lldp  timer  24
Switch_config#
```

26.1.4 lldp reinit

Description

lldp reinit *time*

no lldp reinit

To configure the transmission delay of LLDP, run **lldp reinit time**. To resume the default transmission delay, run **no lldp reinit**.

Parameter

Parameter	Description
time	Transmission delay of LLDP, whose values range from two to five seconds

Default

2 s

Explanation

None

Command mode

Global configuration mode

Example

The following example shows how to set the transmission delay of LLDP to five seconds.

```
Switch_config# lldp reinit 5
Switch_config#
```

26.1.5 lldp tlv-select

Description

lldp tlv-select *tlv-type*

no lldp tlv-select *tlv-type*

To add TLV which is transmitted by the LLDP message, run **lldp tlv-select *tlv-type***. To delete TLV which is transmitted by the LLDP message, run **no lldp tlv-select *tlv-type***.

Parameter

Parameter	Description
tlv-type	TLV that can be sent or not whose values are: macphy-confg ,management-address port-description ,port-vlan ,system-capabilities system-description ,system-name

Default

All TLVs are sent.

Explanation

Three mandatory TLVs must be sent.

Command mode

Global configuration mode

Example

The following example shows how to enable the port description not to be transmitted in the message.

```
Switch_config#no  lldp  tlv-select  port-description
Switch_config#
```

26.1.6 lldp transmit

Description

lldp transmit

no lldp transmit

To set the port to send the LLDP message, run **lldp transmit**. To forbid receiving the LLDP message, run **no lldp transmit**.

Parameter

None

Default

Transmittable LLDP message mode

Explanation

Only after the LLDP module is started can the command be valid.

Command mode

Port configuration mode

Example

The following example shows how to set port f0/0 not to send the LLDP message.

```
Switch_config_f0/0# no lldp  transmit
```

Switch_config_f0/0#

26.1.7 lldp receive

Description

lldp receive

no lldp receive

To set the port to the receivable LLDP message mode, run **lldp receive**. To forbid receiving the LLDP message, run **no lldp receive**.

Parameter

None

Default

Receivable LLDP message mode

Explanation

Only after the LLDP module is started can the configuration be valid.

Command mode

Port configuration mode

Example

The following example shows how to set port f0/0 to the LLDP message mode.

```
Switch_config_f0/0# no lldp receive
Switch_config_f0/0#
```

26.1.8 Show lldp errors

Description

Show lldp errors

It is used to display the error information about the LLDP module.

Parameter

None

Default

None

Explanation

None

Command mode

EXEC/Global configuration mode

Example

The following example shows how to set port f0/0 to the LLDP message mode.

switch_config#show lldp errors

LLDP errors/overflows:

Total memory allocation failures: 0

Total encapsulation failures: 0

Total table overflows: 0

switch_config#

26.1.9 Show lldp interface

Description

Show lldp interface *interface-name*

To check the transmission and reception mode, run **show lldp interface interface name**.

Parameter

Parameter	Description
interface-name	Name of the interface, such as f0/1 and fastethernet0/1

Default

None

Explanation

After LLDP is started, you can check the state of the port.

Command mode

EXEC/global configuration mode

Example

The following example shows how to check the transmission and reception mode of port f0/1.

```
switch_config#show lldp interface f0/1
FastEthernet0/1:
Rx: enabled
Tx: enabled
switch_config#
```

26.1.10 show lldp neighbors

Description

show lldp neighbors

It is used to display the simple information about neighbors.

Parameter

None

Default

None

Explanation

The command is used to display the simple information about neighbors.

Command mode

EXEC / global configuration mode

Example

```
switch_config#show lldp neighbors
Capability Codes:
        (R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone
        (W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID       Local-Intf      Hldtme      Port-ID      Capability
switch          Fas0/2          115         Fas0/32      B
switch          Fas0/32         114         Fas0/2       B

Total entries dispalyed: 2
switch_config#
```

26.1.11 Show lldp neighbors detail

Description

Show lldp neighbors detail

It is used to display the detailed information about the neighbor.

Parameter

None

Default

None

Explanation

None

Command mode

EXEC/global configuration mode

Example

```
switch_config#show lldp neighbors detail

chassis id: 00e0.0f61.ca53
port id: Fas0/32
port description: FastEthernet0/32
system name: switch.

system description: (tm) S3448 Software, Version 2.0.1K
Serial: S35000456
Copyright by Shanghai Baud Data Communication CO. LTD.
Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 98
system capabilities: R B
enabled capabilities: B
Managment Address:
    IP: 192.168.213.62

Auto Negotiation -- supported,enabled
Physical media capabilitise:
    100baseTX(FD)
    100baseTX(HD)
    10baseT(FD)
    10baseT(HD)
Media Attachment Unit type: 16

----------------------------------------

chassis id: 00e0.0f61.ca35
port id: Fas0/2
port description: FastEthernet0/2
system name: switch.

system description: (tm) S3448 Software, Version 2.0.1K
Serial: S35000456
Copyright by Shanghai Baud Data Communication CO. LTD.
```

Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 95
system capabilities: R B
enabled capabilities: B
Managment Address:
IP: 90.0.0.66

Auto Negotiation -- supported,enabled
Physical media capabilitise:
100baseTX(FD)
100baseTX(HD)
10baseT(FD)
10baseT(HD)
Media Attachment Unit type: 16

Total entries dispalyed: 2
switch#

26.1.12 Show lldp traffic

Description

Show lldp traffic

To display all statistics information about LLDP, run **show lldp traffic**.

Parameter

None

Default

None

Explanation

None

Command mode

EXEC/global configuration mode

Example

```
switch_config#show lldp traffic
LLDP traffic statistics:
    Total frames out: 1599
    Total entries aged: 0
    Total frames in: 624
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs unrecognized: 0
switch_config#
```

26.1.13 clear lldp counters

Description

clear lldp counters

To clear the statistics information, run **clear lldp counters**.

Parameter

None

Default

None

Explanation

None

Command mode

EXEC

Example

```
switch#clear lldp counters
switch#
```

26.1.14 clear lldp table

Description

clear lldp table

To remove the neighbor list, run **clear lldp table**.

Parameter

None

Default

None

Explanation

None

Command mode

EXEC

Example

```
switch#clear lldp table
switch#
```

26.1.15 debug lldp errors

Description

debug lldp errors

To report some error information about the LLDP module, run **debug lldp errors**.

Parameter

None

Default

None

Explanation

None

Command mode

EXEC

Example

```
switch#debug lldp errors
debug lldp errors on
switch#show  debug
lldp errors  debugging is on
switch#Nov 14 09:39:04LLDP recive a bad frame on interface FastEthernet0/2
Nov 14 09:49:44LLDP transmit fail on interface FastEthernet0/2
```

26.1.16 debug lldp events

Description

debug lldp events

To report some special events about the LLDP module, run **debug lldp events**.

Parameter

None

Default

None

Explanation

None

Command mode

EXEC

Example

```
switch#debug lldp events
debug lldp events on
switch#show  debug
```

lldp event debugging is on
switch#config
switch_config#int f0/2
switch_config_f0/2#no lldp tr
switch_config_f0/2#Nov 14 09:39:04 LLDP transmit a end packet on interface FastEthernet0/2
Nov 14 09:44:08LLDP recive a unrecognized tlv frame on interface FastEthernet0/2

26.1.17 debug lldp packets

Description

debug lldp packets

To report the message transmission event of the LLDP module, run **debug lldp packets**.

Parameter

None

Default

None

Explanation

None

Command mode

EXEC

Example

switch#debug lldp packets
debug lldp packets on
switch#show debug
lldp packet debugging is on
switch#Nov 13 16:38:20 LLDP advertisement packet TX'd on intf FastEthernet0/2
Nov 13 16:38:20 LLDP advertisement packet RX'd on intf FastEthernet0/32

26.1.18 debug lldp states

Description

debug lldp states

To report the information about the state of the LLDP port, run **debug lldp states**.

Parameter

None

Default

None

Explanation

None

Command mode

EXEC

Example

```
switch#debug lldp states
debug lldp states on
switch#show debug
lldp state debugging is on
switch#Nov 13 16:39:51 LLDP transmit state on FastEthernet0/2 set to TX FRAME
Nov 13 16:39:51 LLDP transmit state on FastEthernet0/2 set to IDLE
Nov 13 16:39:51 LLDP receive state on FastEthernet0/32 set to RX FRAME
Nov 13 16:39:51 LLDP receive state on FastEthernet0/32 set to WAIT FOR FRAME
```

Chapter 27 FlexLinkLite Configuration Commands

27.1 FlexLinkLite Commands

27.1.1 Setting the Backup Port

To set another port as the backup of an existing port, run the following command:

switchport backup interface *backup-intf-name* **as** [**active** | **backup**]

To delete the backup port group, run the following command:

no switchport backup interface

Parameter

Parameter	Description
backup-intf-name	Stands for the name of a backup port, such as G0/1 or F0/10.
active	Stands for the active port, to which **backup-intf-name** corresponds, when the current port is a backup one..
backup	Stands for the backup port, to which **backup-intf-name** corresponds, when the current port is an active one.

Explanation

- A pair of ports, which back up each other, can be two physical ports, or a physical port and an aggregation port, or two aggregation ports.
- The port on which FlexLinkLite is set cannot be used for STP calculation or EAPS settings.
- After **switchport backup interface** is set on an interface, the corresponding settings will automatically generate on the backup port without any manual operations.

Example

The following example shows how to set interface G0/2 to be the backup interface of interface G0/1, which blocks the data from being forwarded.

```
Switch# config
Switch_config# interface gigaEthernet0/1
        Switch_config_g0/1# switchport backup interface g0/2 as backup
```

Related command

To browse the state of the backup port group, run the following command:

show backup interfaces

27.1.2 Setting the Preempt Mode of a Backup Port

switchport backup interface preempt

To set the preempt mode of a backup port, run the following command:

switchport backup interface preempt mode [**none** | **role**]

To set the preempt delay of a backup port, run the following command:

switchport backup interface preempt delay [**immediately** | *time-sec*]

To resume the default value of the preempt delay, run the following command:

no switchport backup interface preempt delay

Parameter

Parameter	Description
none	Sets the preempt mode to be not a preempt mode.
role	Sets the preempt mode to be a role-based one, which is the default configuration.
immediately	Sets the delay time of the preempt to be no delay, that is, immediate preempt.
time-sec	Sets the delay time of preempt, which ranges between 1 and 600 seconds and whose default value is 3 seconds.

Default value

In the default settings, the preempt mode of a backup port is a role-based one and its delay time is 3 seconds.

Command mode

Physical interface configuration mode or aggregation port configuration mode

Explanation

N/A

Example

The following example shows how to set the default role preempt and how to set the delay to 15 seconds.

```
Switch_config_g0/1# switchport backup interface preempt delay 15
```

Related command

To browse the state of the backup port group, run the following command:

show backup interfaces

27.1.3 Setting the Transmission and Reception of TCN Packets

switchport backup interface tcn

To set a port to forward the TCN packets, run the following command:

switchport backup interface tcn transmit

To forbid a port to forward the TCN packets, run the following command:

no switchport backup interface tcn transmit

To allow a port to receive and process the TCN packets, run the following command:

switchport backup interface tcn accept

To forbid a port to receive and process the TCN packets, run the following command:

no switchport backup interface tcn accept

Parameter

N/A

Default value

In the default settings, a port does not receive or transmit the TCN packets.

Command mode

Physical interface configuration mode or aggregation port configuration mode

Explanation

The **transmit** command can be enabled on the device with a configured backup port. When a backup port is switched, it will transmit the TCN packets.

The **accept** command can be enabled on the uplink device. If this command is enabled on a uplink device, it can receive the TCN packets and delete the MAC addresses that are learned by the downlink port.

Example

The following example shows how to make related settings to enable the TCN packets to be transmitted.

```
Switch_config_g0/1# switchport backup interface tcn transmit
```

The following example shows how to make related settings to enable the TCN packets to be received.

```
Switch_config# interface range g0/1 , 2
Switch_config_if_range# switchport backup interface tcn accept
```

Related command

N/A

27.1.4 Browsing the State of the Port Backup Group

show backup interfaces

To browse the state of the backup port group, run the following command:

show backup interfaces

Parameter

N/A

Default value

N/A

Command mode

Monitor mode or global mode

Explanation

N/A

Example

The following example shows how to browse the status of the backup port group:

```
Switch_config# show backup interfaces
Backup interface pairs:
                Active Backup State Preemption
---------- ---------- ------------------------------ ------------
                G0/1 G0/2 Active Up/Backup standby Role/15/0
```

Chapter 28 BackupLink Configuration Commands

28.1 Global Commands

28.1.1 backup-link-group *id*

To set the BackupLink group, run the following command:

backup-link-group *id*

To delete the BackupLink group, run the following command:

no backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group.

Default value

The backuplink group is not configured by default.

Command mode

Global configuration mode

Explanation

N/A.

Example

```
Switch_config#backup-link-group 1
Switch_config#
```

Related command

N/A.

28.1.2 backup-link-group *id* preemption-mode forced {delay *value*}

To set the port-based preemption mode for the backuplink group, run the following command:

backup-link-group *id* **preemption-mode forced** {**delay** *value*}

To delete the port-based preemption mode for the backuplink group, run the following command:

no backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group.
value	Stands for the delay time.

Default value

The backuplink group has not been set with the trait of port-based preemption by default.

Command mode

Global configuration mode

Explanation

The **backup-link-group id preemption-mode forced {delay** value**}** command can be used to create the backuplink group directly.

Example

```
Switch_config#backup-link-group 1 preemption-mode forced delay 5
Switch_config#
```

Related command

backup-link-group id

backup-link-group id preemption-mode bandwidth {delay value}

28.1.3 backup-link-group *id* preemption-mode bandwidth {delay *value*}

To set port bandwidth preemption mode for the backuplink group, run the following command:

backup-link-group *id* **preemption-mode bandwidth** {**delay** *value*}

To delete port bandwidth preemption mode for the backuplink group, run the following command:

no backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group.
value	Stands for the delay time.

Default value

The backuplink group has not been set with the trait of port bandwidth preemption by default.

Command mode

Global configuration mode

Explanation

N/A.

Example

Switch_config#backup-link-group 1 preemption-mode bandwidth delay 5
Switch_config#

Related command

backup-link-group id

backup-link-group id preemption-mode forced {delay value}

28.1.4 monitor-link-group *id*

To set the MonitorLink group, run the following command:

monitor-link-group *id*

To delete the MonitorLink group, run the following command:

no monitor-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the monitorlink group.

Default value

The MonitorLink group is not configured by default.

Command mode

This command is run in global configuration mode.

Explanation

N/A.

Example

Switch _config# monitor-link-group 1
Switch_config#

Related command

N/A.

28.2 Port Configuration Commands

28.2.1 backup-link-group *id* active

To set a port to be an active port, run the following command:

backup-link-group *id* **active**

To cancel the active port, run the following command:

no backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group.

Default value

The primary port is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

If the backuplink group is not established, it will be automatically created when you configure the backuplink group on a port directly.

Example

Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group 1 active
Switch_config_g0/1#exit

Related command

backup-link-group id

backup-link-group id backup

28.2.2 backup-link-group *id* backup

To set a port to be a backup port, run the following command:

backup-link-group *id* **backup**

To cancel the backup port, run the following command:

no backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group.

Default value

The backup port is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

If the backuplink group is not established, it will be automatically created when you configure the backuplink group on a port directly.

Example

Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group 1 backup
Switch_config_g0/1#exit

Related command

backup-link-group id

backup-link-group id active

28.2.3 share-load vlan *vlanmap*

To set VLAN load balance for the backup port, run the following command:

share-load vlan *vlanmap*

To delete VLAN load balance for the backup port, run the following command:

no share-load vlan

Parameter

Parameter	Description
vlanmap	Stands for the VLAN value.

Default value

VLAN load balance is not set for the backup port by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

This command can be set only on the backup port, that is, a port must be set to be a backup port before VLAN load balance is set on the port.

Different BackupLink groups can be set to have the same VLAN group or the overlapped VLAN segments. If there are overlapped VLAN segments, the system will classify these VLANs into different MSTs (STGs) and conduct operations toward a

group of ports, the statuses of these ports in different MSTs vary. So, you'd better rule out those overlapped VLAN groups when configuring load balance for VLANs.

Example

Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1# share-load vlan 100-200
Switch_config_g0/1#exit

Related command

backup-link-group id

backup-link-group id backup

28.2.4 backup-link-group mmu transmit

To set MMU transmission for the ports of the backuplink group, run the following command:

backup-link-group mmu transmit

To delete MMU transmission for the ports of the backuplink group, run the following command:

no backup-link-group mmu

Parameter

N/A.

Default value

The MMU transmission function for the ports of the backuplink group is not set by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

Only the ports of the backuplink group can be set to **transmit**, that is, the ports must be set to **active** or **backup**.

Example

Switch_config#interface gigaEthernet 0/1

```
Switch_config_g0/1#backup-link-group mmu transmit
Switch_config_g0/1#exit
```

Related command

backup-link-group id

28.2.5 backup-link-group mmu receive

To set MMU reception for ports, run the following command:

backup-link-group mmu receive

To delete MMU reception for ports, run the following command:

no backup-link-group mmu

Parameter

N/A.

Default value

The MMU reception function for the ports is not set by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

The ports that are set to **receive** are not necessarily the ports of the backuplink group.

Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group mmu receive
Switch_config_g0/1#exit
```

Related command

N/A.

28.2.6 monitor-link-group *id* uplink

To set a port to be an uplink port, run the following command:

monitor-link-group *id* **uplink**

To cancel the uplink port configuration, run the following command:

no monitor-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the monitorlink group.

Default value

The uplink port is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

If the Monitorlink group is not established, it will be automatically created when you configure the Monitorlink group on a port directly.

Example

Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1# monitor-link-group 1 uplink
Switch_config_g0/1#exit

Related command

monitor-link-group id

monitor-link-group id downlink

28.2.7 monitor-link-group *id* downlink

To set a port to be a downlink port, run the following command:

monitor-link-group *id* **downlink**

To cancel the downlink port configuration, run the following command:

no monitor-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the monitorlink group.

Default value

The downlink port is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

If the Monitorlink group is not established, it will be automatically created when you configure the Monitorlink group on a port directly.

Example

Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1# monitor-link-group 1 downlink
Switch_config_g0/1#exit

Related command

monitor-link-group id

monitor-link-group id uplink

28.3 Show

28.3.1 show backup-link-group *id*

To display the information about the backuplink group, run the following command:

show backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group.

Default value

N/A.

Command mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Explanation

N/A.

Example

Switch_config# show backup-link-group 1

Active Interface	Backup Interface	State	Vlan State
GigaEthernet0/2	GigaEthernet0/4	Forward/Block	Block/Block

Share load vlan: 100-200,port[GigaEthernet0/4] vlan state: Forwarding

Preemption Mode: No Preempt

Preemption Delay: 0 seconds

Related command

N/A.

28.3.2 show monitor-link-group *id*

To display the information about the monitorlink group, run the following command:

show monitor-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the monitorlink group.

Default value

N/A.

Command mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Explanation

N/A.

Example

```
Switch_config#show monitor-link-group 1
  uplink interface: GigaEthernet0/2        Forwarding
  downlink interface:
    GigaEthernet0/1        Forwarding
    GigaEthernet0/3        Forwarding
```

Related command

N/A.

Chapter 29 EAPS Configuration Commands

29.1 Global Commands

29.1.1 ether-ring

To set an instance of ring and enter the node mode, run the following command:

ether-ring *id*

To cancel an instance of ring, run the following command:

no ether-ring *id*

Parameter

Parameter	Description
id	ID of the node

Default value

By default, the ring node is not configured.

Command mode

Global configuration mode

Explanation

STP should not be disabled before the configuration of node instance.

Example

```
S1_config#ether-ring 1
S1_config_ring1#
```

Related command

N/A.

29.1.2 control-vlan

To set the control VLAN of the ring node, run the following command:

control-vlan *vlan-id*

Parameter

Parameter	Description
vlan-id	ID of the control VLAN Value range: 1-4094

Default value

By default, the control VLAN of a node is not configured.

Command mode

Node configuration mode for the Ethernet ring

Explanation

1. Any VLAN can be configured as the control VLAN of the node.

2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the Ethernet ring has already been started.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
```

Related command

ether-ring

master-node

transit-node

29.1.3 master-node

To configure an Ethernet ring as a master node, run the following command:

master-node

Parameter

N/A.

Default value

By default, the node type is not configured.

Command mode

Node configuration mode

Explanation

1. A node can be set to be a master node or a transit node.

2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already been started.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node
```

Related command

control-vlan

transit-node

29.1.4 transit-node

Configures the node type to be a transit node.

transit-node

Parameter

N/A.

Default value

By default, the node type is not configured.

Command mode

Node configuration mode

Explanation

1. A node can be set to be a master node or a transit node.

2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already been started.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#transit-node
```

Related command

control-vlan

master-node

29.1.5 hello-time

To configure the cycle for the master node to transmit the HEALTH packets of the Ethernet ring, run the following command:

hello-time *value*

To resume the default value of the cycle, run the following command:

no hello-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second. The default value is one second. The value ranges between 1 and 10 seconds.

Default value

By default, the hello-time is one second.

Command mode

Node configuration mode for the Ethernet ring

Explanation

1. The hello-time configuration validates only on the master node.

2. By default, the value of the hello-time is smaller than that of the fail-time, which avoids the Ethernet ring protocol from being shocked.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node
S1_config_ring1#hello-time 2
```

Related command

fail-time

29.1.6 fail-time

To configure the time cap of waiting for the HEALTH packets for the secondary port of the master node, run the following command:

fail-time *value*

To resume the default value of the fail-time, run the following command:

no fail-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.

Default value

By default, the fail-time is 3 seconds.

Command mode

Node configuration mode for the Ethernet ring

Explanation

1. The fail-time configuration validates only on the master node.

2. By default, the value of the fail-time is triple of the fail-time, which avoids the Ethernet ring protocol from being shocked.

Example

S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node
S1_config_ring1#hello-time 2
S1_config_ring1#fail-time 6

Related command

hello-time

29.1.7 pre-forward-time

Configures the time of maintaining the pre-forward state on the transit port.

pre-forward-time *value*

To resume the default value of the pre-forward-time, run the following command:

no pre-forward-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.

Default value

By default, the pre-forward-time is 3 seconds.

Command mode

Node configuration mode for the Ethernet ring

Explanation

1. The pre-forward-time configuration validates only on the transit node.

2. By default, the pre-forward-time on the transit node is three times the value of the hello-time on the master node, which avoids the network loop from being occurred after the transmission link recovers from disconnection. After the hello-time of the

master node is modified, the corresponding pre-forward-time on the transit node need be adjusted.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#transit-node
S1_config_ring1#pre-forward-time 8
```

Related command

N/A.

29.2 Port Configuration Commands

29.2.1 ether-ring primary-port

To set a port to be the primary port of a master node, run the following command:

ether-ring *id* **primary-port**

To cancel the primary port configuration of a port, run the following command:

no ether-ring *id* **primary-port**

Parameter

Parameter	Description
id	ID of the node

Default value

The primary port is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

Explanation

The primary port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type is the master node.

Example

S1_config#interface GigaEthernet 0/1
S1_config_g0/1#ether-ring 1 primary-port
S1_config_g0/1#exit

Related command

master-node

ether-ring secondary-port

29.2.2 ether-ring secondary-port

To set a port to be the secondary port of a master node, run the following command:

ether-ring *id* **secondary-port**

To cancel the secondary port configuration, run the following command:

no ether-ring *id* **secondary-port**

Parameter

Parameter	Description
id	ID of the node

Default value

The secondary port on the master node is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

Explanation

The secondary port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type must be the master node.

Example

S1_config#interface GigaEthernet 0/3
S1_config_g0/3#ether-ring 1 secondary-port

S1_config_g0/3#exit

Related command

master-node

ether-ring primary-port

29.2.3 ether-ring transit-port

To set a port to be the transit port of a transit node, run the following command:

ether-ring *id* **transit-port**

To cancel the transit port, run the following command:

no ether-ring *id* **transit-port**

Parameter

Parameter	Description
id	ID of the node

Default value

The transit port on the transit node is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

Explanation

The transit port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type must be the transit node. Two transit ports can be configured on one transit node.

Example

S1_config_ring1#exit
S1_config#interface GigaEthernet 0/1
S1_config_g0/1#ether-ring 1 transit-port
S1_config_g0/1#exit
S1_config#interface GigaEthernet 0/3

```
S1_config_g0/3#ether-ring 1 transit-port
S1_config_g0/3#exit
```

Related command

transit-node

29.3 Show

29.3.1 show ether-ring

To display the summary information about the Ethernet-ring node, run the following command:

show ether-ring *id*

To display the detailed information about the Ethernet-ring node, run the following command:

show ether-ring *id* **detail**

To display the information about the Ethernet-ring port, run the following command:

show ether-ring *id* **interface** *intf-name*

To display the summary information about the Ethernet-ring node, run the following command:

show ether-ring <cr>

Parameter

Parameter	Description
id	ID of the node
intf-name	Name of an interface

Default value

N/A.

Command mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Explanation

N/A.

Example

N/A.

Related command

N/A.

Chapter 30 MEAPS Configuration Commands

30.1 Global Commands

30.1.1 mether-ring *id1* domain *id2*

To set an instance of ring and enter the node mode, run the following command:

mether-ring *id1* **domain** *id2*

To cancel an instance of ring, run the following command:

no mether-ring *id1* **domain** *id2*

Parameter

Parameter	Description
Id1	Stands for the node instance ID, which ranges from 0 to 7.
Id2	Stands for the domain instance ID, which ranges from 0 to 3.

Default value

By default, the ring node is not configured.

Command mode

Global configuration mode

Explanation

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#
```

Related command

N/A.

30.1.2 master-node

To configure an Ethernet ring as a master node, run the following command:

master-node

Parameter

N/A.

Default value

By default, the node type is not configured.

Command mode

Node configuration mode

Explanation

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#
```

Related command

transit-node

edge-node

assistant-node

major-ring

sub-ring

control-vlan

30.1.3 transit-node

Configures the node type to be a transit node.

transit-node

Parameter

N/A.

Default value

By default, the node type is not configured.

Command mode

Node configuration mode

Explanation

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1# transit-node
S1_config_ring1#
```

Related command

master-node

edge-node

assistant-node

major-ring

sub-ring

control-vlan

30.1.4 edge-node

To set the node type to be an edge node, run the following command:

edge-node

Parameter

N/A.

Default value

By default, the node type is not configured.

Command mode

Node configuration mode

Explanation

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1# edge-node
S1_config_ring1#
```

Related command

master-node

transit-node

assistant-node

major-ring

sub-ring

control-vlan

30.1.5 assistant-node

To set the node type to be an assistant edge node, run the following command:

assistant-node

Parameter

N/A.

Default value

By default, the node type is not configured.

Command mode

Node configuration mode

Explanation

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1# assistant-node
S1_config_ring1#
```

Related command

master-node

transit-node

edge-node

major-ring

sub-ring

control-vlan

30.1.6 major-ring

To set the node ring's level to be the major ring node, run the following command:

major-ring

Parameter

N/A.

Default value

By default, the node ring's level is not configured.

Command mode

Node configuration mode

Explanation

1. The node ring's level can only be set to one of the two levels: major-ring or sub-ring.

2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node ring's level can never be modified.

3. The edge node and the assistant node cannot be set to major ring.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1# transit-node
S1_config_ring1#major-ring
S1_config_ring1#
```

Related command

master-node

transit-node

edge-node

assistant-node

sub-ring

control-vlan

30.1.7 sub-ring

To set the node ring's level to be the sub-ring node, run the following command:

sub-ring

Parameter

N/A.

Default value

By default, the node type is not configured.

Command mode

Node configuration mode

Explanation

1. The node ring's level can only be set to one of the two levels: major-ring or sub-ring.

2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node ring's level can never be modified.

3. If the edge node or the assistant node is set, they are regarded as sub-rings by default. Of course, you can set them not to be sub-rings.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#
```

Related command

master-node

transit-node

edge-node

assistant-node

major-ring

control-vlan

30.1.8 control-vlan

To set the control VLAN of the ring node, run the following command:

control-vlan *vlan-id*

Parameter

Parameter	Description
vlan-id	ID of the control VLAN Value range: 1-4094

Default value

By default, the control VLAN of a node is not configured.

Command mode

Node configuration mode for the Ethernet ring

Explanation

1. You can set any VLAN to be the control VLAN of a node and at the same time the system will create the corresponding system VLAN and another control VLAN according to the ring level.

2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the ring control VLAN can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#
```

Related command

master-node

transit-node

edge-node

assistant-node

major-ring

sub-ring

30.1.9 single-subring-mode

To enable the edge node or the assistant edge node to enter the single sub-ring mode, run the following command:

single-subring-mode

Parameter

N/A

Default value

The edge node or the assistant edge node does not enter the single sub-ring mode by default.

Command mode

Node configuration mode for the Ethernet ring

Explanation

1. The single-subring-mode command takes effect only on the edge node or the assistant edge node.

In single sub-ring networking mode, the channel state of sub-ring protocol packet is not checked, and dual-affiliation networking must not exist in the ring.

Example

S1_config#mether-ring 1 domain 2
S1_config_ring1#edge-node
S1_config_ring1#control-vlan 2
S1_config_ring1#single-subring-mode

Related command

N/A

30.1.10 hello-time

To configure the cycle for the master node to transmit the HEALTH packets of the Ethernet ring, run the following command:

hello-time *value*

To resume the default value of the cycle, run the following command:

no hello-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 1 and 10 seconds.

Default value

By default, the hello-time is three seconds.

Command mode

Node configuration mode for the Ethernet ring

Explanation

1. The hello-time configuration validates only on the master node.

2. By default, the value of the hello-time is smaller than that of the fail-time, which avoids the Ethernet ring protocol from being shocked. After the hello-time is modified, the corresponding fail-time need be modified too.

Example

S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#hello-time 4

Related command

fail-time

30.1.11 fail-time

To configure the time cap of waiting for the HEALTH packets for the secondary port of the master node, run the following command:

fail-time *value*

To resume the default value of the fail-time, run the following command:

no fail-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.

Default value

By default, the fail-time is 9 seconds.

Command mode

Node configuration mode for the Ethernet ring

Explanation

1. The fail-time configuration validates only on the master node.

2. By default, the value of the fail-time is triple of the fail-time, which avoids the Ethernet ring protocol from being shocked. After the hello-time is modified, the corresponding fail-time need be modified too.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#hello-time 4
S1_config_ring1#fail-time 12
```

Related command

hello-time

30.1.12 pre-forward-time

Configures the time of maintaining the pre-forward state on the transit port.

pre-forward-time *value*

To resume the default value of the pre-forward-time, run the following command:

no pre-forward-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.

Default value

By default, the pre-forward-time is 9 seconds.

Command mode

Node configuration mode for the Ethernet ring

Explanation

1. The pre-forward-time configuration validates only on the transit node.

2. By default, the pre-forward-time on the transit node is three times the value of the hello-time on the master node, which avoids the network loop from being occurred after the transmission link recovers from disconnection. After the hello-time of the master node is modified, the corresponding pre-forward-time on the transit node need be adjusted.

Example

S1_config#mether-ring 1 domain 2
S1_config_ring1#transit-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#pre-forward-time 12

Related command

N/A.

30.2 Port Configuration Commands

30.2.1 mether-ring *id1* domain *id2* primary-port

To set a port to be the primary port of a master node, run the following command:

mether-ring *id1* **domain** *id2* **primary-port**

To cancel the primary port configuration of a port, run the following command:

no mether-ring *id1* **domain** *id2* **primary-port**

Parameter

Parameter	Description
Id1	ID of the node
Id2	ID of domain instance

Default value

The primary port is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the master node.

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted.

Example

```
S1_config#interface GigaEthernet 0/1
S1_config_g0/1# mether-ring 1 domain 2 primary-port
S1_config_g0/1#exit
```

Related command

master-node

mether-ring id1 domain id2 secondary-port

30.2.2 mether-ring *id1* domain *id2* secondary-port

To set a port to be the secondary port of a master node, run the following command:

mether-ring *id1* **domain** *id2* **secondary-port**

To cancel the secondary port configuration, run the following command:

no mether-ring *id1* **domain** *id2* **secondary-port**

Parameter

Parameter	Description
Id1	ID of the node
Id2	ID of domain instance

Default value

The secondary port on the master node is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

The secondary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the master node.

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted.

Example

S1_config#interface GigaEthernet 0/3
S1_config_g0/3# mether-ring 1 domain 2 secondary-port
S1_config_g0/3#exit

Related command

master-node

mether-ring id1 domain id2 primary-port

30.2.3 mether-ring *id1* domain *id2* transit-port

To set a port to be the transit port of a transit node, run the following command:

mether-ring *id1* **domain** *id2* **transit-port**

To cancel the transit port, run the following command:

no mether-ring *id1* **domain** *id2* **transit-port**

Parameter

Parameter	Description

Id1	ID of the node
Id2	ID of domain instance

Default value

The transit port on the transit node is not configured by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the transit node. Two transit ports can be configured on one transit node.

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted.

Example

S1_config_ring1#exit
S1_config#interface GigaEthernet 0/1
S1_config_g0/1# mether-ring 1 domain 2 transit-port
S1_config_g0/1#exit
S1_config#interface GigaEthernet 0/3
S1_config_g0/3# mether-ring 1 domain 2 transit-port
S1_config_g0/3#exit

Related command

transit-node

30.2.4 mether-ring *id1* domain *id2* common-port

To set a port to be a public port of an edge node (assistant edge node), run the following command:

mether-ring *id1* **domain** *id2* **common-port**

To cancel the public port, run the following command:

no mether-ring *id1* **domain** *id2* **common-port**

Parameter

Parameter	Description

Id1	ID of the node
Id2	ID of domain instance

Default value

By default, there is no configuration of the public port of an edge node.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

The public port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the edge node.

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted.

Example

S1_config_ring1#exit
S1_config#interface GigaEthernet 0/1
S1_config_g0/1# mether-ring 2 domain 2 common-port
S1_config_g0/1#exit

Related command

edge-node

assistant-node

mether-ring id1 domain id2 edge-port

30.2.5 mether-ring *id1* domain *id2* edge-port

To set a port to be an edge port of an edge node (assistant edge node), run the following command:

mether-ring *id1* **domain** *id2* **edge-port**

To cancel the edge port configuration of a port, run the following command:

no mether-ring *id1* **domain** *id2* **edge-port**

Parameter

Parameter	Description

Id1	ID of the node
Id2	ID of domain instance

Default value

By default, there is no configuration of the edge port of an edge node.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

The edge port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the edge node.

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted.

Example

S1_config_ring1#exit
S1_config#interface GigaEthernet 0/3
S1_config_g0/3# mether-ring 2 domain 2 edge-port
S1_config_g0/3#exit

Related command

edge-node

assistant-node

mether-ring id1 domain id2 common-port

30.3 Show

30.3.1 show mether-ring

To display the summary information about the Ethernet-ring node, run the following command:

show mether-ring *id1* **domain** *id2*

To display the detailed information about the Ethernet-ring node, run the following command:

show mether-ring *id1* **domain** *id2* **detail**

To display the information about the Ethernet-ring port, run the following command:

show mether-ring *id1* **domain** *id2* **interface** *intf-name*

To display the summary information about the Ethernet-ring node, run the following command:

show mether-ring

Parameter

Parameter	Description
Id1	ID of the node
Id2	ID of domain instance
intf-name	Name of an interface

Default value

N/A.

Command mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Explanation

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted.

Example

N/A.

Related command

N/A.

Chapter 31 ELPS Configuration Commands

31.1 Global Commands

31.1.1 **elps** *id*

To set an instance of ELPS node and enter the node mode, run the following command:

elps *id*

To cancel an instance of ring, run the following command:

no elps *id*

Parameter

Parameter	Description
id	Stands for the node instance ID, which ranges from 0 to 7.

Default value

By default, the ELPS node instance is not configured.

Command mode

Global configuration mode

Explanation

N/A.

Example

S1_config#elps 1
S1_config_elps1#

Related command

N/A.

31.1.2 **working-vlanmap** *vlanmap*

To set the working vlan map of the ELPS node, run the following command:

working-vlanmap *vlanmap*

Parameter

Parameter	Description
vlanmap	Stands for the VLAN range table (1-4094), which is similar with (1,3,5,7), (1,3-5,7) or (1-7).

Default value

By default, the working vlan map of a node is not configured.

Command mode

EPLS node configuration mode

Explanation

1. Configuring working VLAN does not mean creating this VLAN, so you have to establish the control VLAN manually.。

2. After working-vlanmap, protection-mode, revertive-mode and detect-fault are configured, the ELPS configuration mode exits and the ELPS node is started, the working-vlanmap cannot be modified.

Example

```
S1_config#elps 1
S1_config_elps1#working-vlanmap 1-10
S1_config_elps1#
```

Related command

protection-mode {1plus1-bidirectional | 1plus1-unidirectional | 1to1-bidirectional}

revertive-mode {revertive | nonrevertive}

detect-fault {physical-port-check| continuity-check | both-check}

31.1.3 **protection-mode {1plus1-bidirectional | 1plus1-unidirectional | 1to1-bidirectional}**

To set the protection mode of the ELPS node to be the 1plus1-bidirectional mode, run the following command:

protection-mode 1plus1-bidirectional

To set the protection mode of the ELPS node to be the 1plus1-unidirectional mode, run the following command:

protection-mode 1plus1-unidirectional

To set the protection mode of the ELPS node to be the 1to1-bidirectional mode, run the following command:

protection-mode 1to1-bidirectional

Parameter

N/A.

Default value

By default, the ELPS node's protection mode is not configured.

Command mode

ELPS node configuration mode

Explanation

1. When the ELPS node's protection mode is set to **1plus1-bidirectional** or **1plus1-unidirectional**, the revertive mode of node is **non-revertive** by default; the protection mode is **1to1-bidirectional**, it is **revertive** by default.

2. After working-vlanmap, protection-mode, revertive-mode and detect-fault are configured, the ELPS configuration mode exits and the ELPS node is started, the working-vlanmap cannot be modified.

Example

```
S1_config#elps 1
S1_config_elps1#working-vlanmap 1-10
S1_config_elps1#protection-mode 1plus1-bidirectional
S1_config_elps1#
```

Related command

working-vlanmap vlanmap

revertive-mode {revertive | nonrevertive}

detect-fault {physical-port-check| continuity-check | both-check}

31.1.4 revertive-mode {revertive | nonrevertive}

To set the mode of the ELPS to **revertive**, run the following command:

revertive-mode revertive

To set the mode of the ELPS to **non-revertive**, run the following command:

revertive-mode nonrevertive

Parameter

N/A.

Default value

By default, the ELPS node's mode is not configured.

Command mode

ELPS node configuration mode

Explanation

1. When the ELPS node's protection mode is set to **1plus1-bidirectional** or **1plus1-unidirectional**, the revertive mode of node is **non-revertive** by default; the protection mode is **1to1-bidirectional**, it is **revertive** by default. The two cases change after the configuration of the revertive mode.

2. After working-vlanmap, protection-mode, revertive-mode and detect-fault are configured, the ELPS configuration mode exits and the ELPS node is started, the working-vlanmap cannot be modified.

Example

```
S1_config#elps 1
S1_config_elps1#working-vlanmap 1-10
S1_config_elps1#protection-mode 1plus1-bidirectional
S1_config_elps1#revertive-mode revertive
S1_config_elps1#
```

Related command

working-vlanmap vlanmap

protection-mode {1plus1-bidirectional | 1plus1-unidirectional | 1to1-bidirectional}

detect-fault {physical-port-check| continuity-check | both-check}

31.1.5 detect-fault {physical-port-check| continuity-check | both-check}

To set the trouble monitoring mode of the ELPS node to **physical-port-check**, run the following command:

detect-fault physical-port-check

To set the trouble monitoring mode of the ELPS node to **continuity-check**, run the following command:

detect-fault continuity-check

To set the trouble monitoring mode of the ELPS node to **both-check**, run the following command:

detect-fault both-check

Default value

By default, the ELPS node's trouble monitoring mode is not configured.

Command mode

ELPS node configuration mode

Explanation

1. After working-vlanmap, protection-mode, revertive-mode and detect-fault are configured, the ELPS configuration mode exits and the ELPS node is started, the working-vlanmap cannot be modified.

Example

```
S1_config#elps 1
S1_config_elps1#working-vlanmap 1-10
S1_config_elps1#protection-mode 1plus1-bidirectional
S1_config_elps1#revertive-mode revertive
S1_config_elps1#detect-fault continuity-check
S1_config_elps1#
```

Related command

working-vlanmap vlanmap

protection-mode {1plus1-bidirectional | 1plus1-unidirectional | 1to1-bidirectional}

revertive-mode {revertive | nonrevertive}

31.1.6 WTR-time

To set the WTR time of the ELPS node, run the following command:

WTR-time *value*

To resume the default WTR time of the ELPS node, run the following command:

no WTR-time

Parameter

Parameter	Description
value	Stands for the WTR time, which ranges from 5 to 12 minutes. Its step is 1 minute and its default value is 5 minutes.

Default value

By default, the WTR-time is 5 minutes.

Command mode

ELPS node configuration mode

Explanation

N/A.

Example

S1_config#elps 1
S1_config_elps1#working-vlanmap 1-10
S1_config_elps1#protection-mode 1plus1-bidirectional
S1_config_elps1#revertive-mode revertive
S1_config_elps1#detect-fault continuity-check
S1_config_elps1#WTR-time 6
S1_config_elps1#

Related command

N/A

31.1.7 hold-off-time

To set the hold-off time of the ELPS node, run the following command:

hold-off-time *value*

To resume the default hold-off time of the ELPS node, run the following command:

no hold-off-time

Parameter

Parameter	Description
value	Stands for the hold-off time, which ranges from 1 to 10 seconds. Its step is 100ms and its default value is 1 second.

Default value

By default, the hold-off time is one second.

Command mode

ELPS node configuration mode

Explanation

N/A.

Example

```
S1_config#elps 1
S1_config_elps1#working-vlanmap 1-10
S1_config_elps1#protection-mode 1plus1-bidirectional
S1_config_elps1#revertive-mode revertive
S1_config_elps1#detect-fault continuity-check
S1_config_elps1#hold-off-time 2
S1_config_elps1#
```

Related command

N/A

31.2 Port Configuration Commands

31.2.1 **elps** *id* **{working-transport | protection-transport}**

To set a port where the ELPS working transport entity is located, run the following command:

elps *id* **working-transport**

To delete the ELPS working transport entity configuration on a port, run the following command:

no elps *id* **working-transport**

To set a port where the ELPS protection transport entity is located, run the following command:

elps *id* **protection-transport**

To delete the ELPS protection transport entity configuration on a port, run the following command:

no elps *id* **protection-transport**

Parameter

Parameter	Description
id	ID of the node

Default value

No ELPS configuration exists on ports by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

The port cannot be configured until working-vlanmap, protection-mode, revertive-mode and default-fault are all configured.

Example

S1_config#interface GigaEthernet 0/1
S1_config_g0/1# elps 1 working-transport
S1_config_g0/1#exit

Related command

elps id mep md md-string ma ma-string level level-id local local-id remote remote-id

31.2.2 **elps** *id* **mep md** *md-string* **ma** *ma-string* **level** *level-id* **local** *local-id* **remote** *remote-id*

To set the MEP information about the ELPS port, run the following command:

elps *id* **mep md** *md-string* **ma** *ma-string* **level** *level-id* **local** *local-id* **remote** *remote-id*

To delete the MEP information about the ELPS port, run the following command:

no elps *id* **mep**

Parameter

Parameter	Description
id	ID of the node
md-string	MEP maintenance domain
ma-string	MEP maintenance link
level-id	MEP level
local-id	Local MEP ID
remote-id	Remote MEP ID

Default value

No MEP information exists on ports by default.

Command mode

The physical port configuration mode and the converged port configuration mode

Explanation

The port cannot be configured until working-vlanmap, protection-mode, revertive-mode and default-fault, transport entity of the ELPS port are all configured.

Example

```
S1_config#interface GigaEthernet 0/1
S1_config_g0/1#elps 1 working-transport
S1_config_g0/1#elps 1 mep md x ma x level 1 local 1 remote 2
S1_config_g0/1#exit
```

Related command

elps id {working-transport | protection-transport}

31.3 Control Commands

31.3.1 **elps** *id* **LockOut**

To set the protection lockout of ELPS, run the following command:

elps *id* **LockOut**

Parameter

Parameter	Description
Id	ID of the node

Default value

N/A.

Command mode

Monitoring mode

Explanation

N/A.

Example

N/A.

Related command

elps id ForcedSwitch

elps id ManualSwitch

elps id ManualSwitch-Working

elps id Exercise

elps id CLEAR

31.3.2 elps *id* ForcedSwitch

To set the forced switching operation of ELPS, run the following command:

elps *id* **ForcedSwitch**

Parameter

Parameter	Description
Id	ID of the node

Default value

N/A.

Command mode

Monitoring mode

Explanation

N/A.

Example

N/A.

Related command

elps id LockOut

elps id ManualSwitch

elps id ManualSwitch-Working

elps id Exercise

elps id CLEAR

31.3.3 elps *id* ManualSwitch

To set the manual switching operation of ELPS, run the following command:

elps *id* **ManualSwitch**

Parameter

Parameter	Description
Id	ID of the node

Default value

N/A.

Command mode

Monitoring mode

Explanation

N/A.

Example

N/A.

Related command

elps id LockOut

elps id ForcedSwitch

elps id ManualSwitch-Working

elps id Exercise

elps id CLEAR

31.3.4 **elps** *id* **ManualSwitch-Working**

To switch to the working entity of ELPS manually, run the following command:

elps *id* **ManualSwitch-Working**

Parameter

Parameter	Description
Id	ID of the node

Default value

N/A.

Command mode

Monitoring mode

Explanation

N/A.

Example

N/A.

Related command

elps id LockOut

elps id ForcedSwitch

elps id ManualSwitch

elps id Exercise

elps id CLEAR

31.3.5 **elps** *id* **Exercise**

To set the exercise operation of ELPS, run the following command:

elps *id* **Exercise**

Parameter

Parameter	Description
Id	ID of the node

Default value

N/A.

Command mode

Monitoring mode

Explanation

N/A.

Example

N/A.

Related command

elps id LockOut

elps id ForcedSwitch

elps id ManualSwitch

elps id ManualSwitch-Working

elps id CLEAR

31.3.6 **elps** *id* **CLEAR**

To clear the control command of ELPS, run the following command:

elps *id* **CLEAR**

Parameter

Parameter	Description
Id	ID of the node

Default value

N/A.

Command mode

Monitoring mode

Explanation

N/A.

Example

N/A.

Related command

elps id LockOut

elps id ForcedSwitch

elps id ManualSwitch

elps id ManualSwitch-Working

elps id Exercise

31.4 Show

31.4.1 **show elps**

To display the summary information about the ELPS node, run the following command:

show elps *id*

To display the detailed information about the ELPS node, run the following command:

show elps *id* **detail**

To display the information about the ELPS port, run the following command:

show elps *id* **interface** *intf-name*

To display the summary information about all ELPS nodes, run the following command:

show elps

Parameter

Parameter	Description
id	ID of the node
intf-name	Name of an interface

Default value

N/A.

Command mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Explanation

N/A.

Example

N/A.

Related command

N/A.

Chapter 32 UDLD Configuration Commands

32.1 UDLD Configuration Commands

The UDLD configuration commands are listed below:

- udld enable
- udld aggressive
- udld port
- udld port aggressive
- udld message
- udld reset
- show udld

32.1.1 udld enable

Syntax

udld enable

It is used to enable UDLD globally in **normal** mode.

no udld enable

It is used to disable UDLD globally in **normal** mode.

Parameter

None

Default settings

None

Usage explanation

This command is used to enable UDLD on all interfaces in **normal** mode. In **normal** mode, if UDLD determines that the connection is gone, UDLD will set the state of the port to **undetermined**, not to **down**. If UDLD maintains it is a bidirectional link, the port will be set to **bidirectional**.

Command mode

Global

Example

The following example shows how to enable UDLD in **normal** mode:

```
Switch_config#udld enable
```

32.1.2 udld aggressive

Syntax

udld aggressive

It is used to enable UDLD globally in **aggressive** mode.

no udld aggressive

It is used to disable UDLD globally in **aggressive** mode.

Parameter

None

Default Settings

None

Usage explanation

This command is used to enable UDLD on all interfaces in **aggressive** mode. In **aggressive** mode, if UDLD determines that the link is gone and the link cannot be reconnected, it is thought that interrupted communication is a severe network problem and UDLD will set the state of the protocol to **down** and the port is in **down** state. If UDLD maintains it is a bidirectional link, the port will be set to **bidirectional**.

Command mode

Global

Example

The following example shows how to enable UDLD in **aggressive** mode:

```
Switch_config#udld aggressive
```

32.1.3 udld port

Syntax

udld port

This command is used to enable UDLD on a port in **normal** mode.

no udld port

This command is used to disable UDLD on a port in **normal** mode.

Parameter

None

Default Settings

None

Usage explanation

This command is used to enable UDLD on the local port in **normal** mode. In **normal** mode, if UDLD determines that the connection is gone, UDLD will set the state of the port to **undetermined**, not to **down**. If UDLD maintains it is a bidirectional link, the port will be set to **bidirectional**.

Command mode

Interface configuration mode

Example

The following example shows how to enable UDLD in **normal** mode:

```
Switch_config_f0/1#udld port
```

32.1.4 udld port aggressive

Syntax

udld port aggressive

It is used to enable UDLD on the local interface in **aggressive** mode.

no udld port aggressive

It is used to disable UDLD on the local interface in **aggressive** mode.

Parameter

None

Default Settings

None

Usage explanation

This command is used to enable UDLD on the local interface in **aggressive** mode. In **aggressive** mode, if UDLD determines that the link is gone and the link cannot be reconnected, it is thought that interrupted communication is a severe network problem and UDLD will set the state of the protocol to **down** and the port is in **down** state. If UDLD maintains it is a bidirectional link, the port will be set to **bidirectional**.

Command mode

Interface configuration mode

Example

The following example shows how to enable UDLD in **aggressive** mode:

```
Switch_config_f0/1#udld port aggressive
```

32.1.5 udld message

Syntax

udld message *time*

It is used to set the message interval in **aggressive** mode.

no udld message

It is to resume the default message interval in **aggressive** mode.

Parameter

Parameter	Explanation
time	Stands for the message interval in **aggressive** mode. It ranges

	between 7 and 90 seconds.

Default Settings

15s

Usage explanation

This command is used to set the message interval in **aggressive** mode. After the message is set, you need to reset the **aggressive** mode and then the new message interval takes effect.

Command mode

Global

Example

The following example shows how to set the message interval to 7 seconds in **aggressive** mode, which takes effect after the **aggressive** mode is restarted.

```
Switch_config#udld message 7
```

32.1.6 udld reset

Syntax

udld reset

It is used to reset the interface which is down by UDLD to **up**.

Parameter

None

Default Settings

None

Usage explanation

This command is used to reset the interface which is down by UDLD to **up**.

Command mode

EXEC

Example

The following example shows how to restart the interface which is closed by UDLD.

Switch#udld reset

1 ports shutdown by UDLD were reset.

%%UDLD-2-UDLD_PORT_RESET: UDLD reset interface FastEthernet0/1.

%%PM-4-ERR_RECOVER: Attempting to recover from udld err-disable state on FastEthernet0/1.

32.1.7 show udld

Syntax

show udld [*interface*]

It is used to display the information about UDLD running.

Parameter

Parameter	Explanation
interface	Shows the running of the UDLD module on a specific interface.

Default Settings

None

Usage explanation

This command can display the running of the UDLD module. When the **interface** parameter is not entered, the information about the running of all UDLDs on all interfaces will be displayed; when the **interface** parameter is entered, only the running of the UDLD on this interface will be displayed.

Command mode

EXEC / global

Example

The following commands will display the running states of UDLD modules on all interfaces.

Switch_config#show udld

Interface FastEthernet0/1

Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 15
Time out interval: 1
No neighbor cache information stored

Interface FastEthernet0/2

Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 15
Time out interval: 1
No neighbor cache information stored

Interface FastEthernet0/3

Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 15
Time out interval: 1
No neighbor cache information stored
....
....
....

The following commands will display the running state of the UDLD module on the f0/1 interface.

Switch_config#show udld interface f0/1

Interface FastEthernet0/1

Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 15
Time out interval: 1
No neighbor cache information stored

```
Switch_config#
```

Chapter 33 IGMP-SNOOPING Configuration Commands

IGMP-SNOOPING configuration commands include：

- ip igmp-snooping
- ip igmp-snooping static
- ip igmp-snooping immediate-leave
- ip igmp-snooping dlf-frames
- ip igmp-snooping router age
- ip igmp-snooping response time
- ip igmp-snooping querier
- show ip igmp-snooping
- show ip igmp-snooping timer
- show ip igmp-snooping groups
- show ip igmp-snooping statistics
- debug ip igmp-snooping packet
- debug ip igmp-snooping timer

33.1.1 igmp-snooping

Description

To enable the IGMP-snooping of VLAN, use the ip igmp-snooping command. Use the no form of this command to restore the default.

ip igmp-snooping [vlan *vlan_id* **]**

no ip igmp-snooping [vlan *vlan_id* **]**

Parameter

Parameter	Description
vlan id	VLAN identity。Value is from 1 to 4094。

Default

disabled

Instruction

If not specified the vlan parameter, this command enable or disable all vlans in the system (IGMP-snooping currently can be ran on 16 vlans at most at the same time.)

Example

The following command enables IGMP snooping of vlan 1:

```
switch(config)# ip igmp-snooping vlan 1
switch(config)#
```

33.1.2 igmp-snooping static

Description

ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*

no ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*

Parameter

Parameter	Description
vlan id	VLAN identity。Value is from 1 to 4094。
A.B.C.D	Specifies the IP address of multicast
inft	Specifies the interface

Default

None

Instruction

Use this command to configurethe the static multicast address of vlan. Use the no form of this command to delete the address.

Example

The following command adds the static multicast address at 234.5.6.7 to the fast ethernet interface 5 of vlan 2:

```
switch(config)# ip igmp-snooping vlan 2 static 234.5.6.7 interface FastEthernet0/5
switch(config)#
```

Note:

224.0.0.0-224.0.0.255, as the multicast address which cannot be routed, cannot be registered to each interface.

33.1.3 igmp-snooping immediate-leave

Description

To configure the immediate-leave characteristic of vlan, use the ip igmp-snooping vlan command. Use the no form of this command to restore the default value.

ip igmp-snooping vlan *vlan_id* **immediate-leave**

no ip igmp-snooping vlan *vlan_id* **immediate-leave**

Parameter

Parameter	Description
vlan id	VLAN identity。Value is from 1 to 4094。

Default

disabled

Instruction

None

Example

The following command enables immediate-leave characteristic of vlan 1:

```
switch(config)# ip igmp-snooping vlan 1 immediate-leave
switch(config)#
```

33.1.4 igmp-snooping dlf-frames

Description

ip igmp-snooping dlf-frames *filter*

no ip igmp-snooping dlf-frames

Parameter

Parameter	Description
filter	Filters for the multicast packets of the unregistered address

Default

None

Instruction

Use this command to configure filter mode for the multicast packets of the unregistered destination address. Use the no form of this command to restore the default configuration(broadcasting in vlan)

Example

The following example configures to drop multicast packets of the unregistered destination address in all vlans:

switch(config)# ip igmp-snooping dlf-frames filter
switch(config)#

33.1.5 igmp-snooping router age

Description

ip igmp-snooping timer router-age *timer_value*

no ip igmp-snooping timer router-age *timer_value*

Parameter

Parameter	Description
time value	Query timer time. Value is from 10 to 2147483647。

Default

260 seconds

Instruction

Use this command to configure query timer time. Use the no form of this command to restore the default value.

Example

The following example configures router-age to 300 seconds

switch(config)# ip igmp-snooping timer router-age 300
switch(config)#

33.1.6 igmp-snooping response time

Description

To configure the maximum response time of IGMP-snooping, use IGMP-snooping command. Use the no form of this command to restore the default value.

ip igmp-snooping timer response-time *timer_value*

no ip igmp-snooping timer response-time *timer_value*

Parameter

Parameter	Description
time value	Query timer time 。Value is from 1 to 255。

Default

10 seconds

Instruction

None

Example

The following example configures response-time to 20 seconds:

switch(config)# ip igmp-snooping timer response-time 20
switch(config)#

33.1.7 igmp-snooping querier

Description

To activate IGMP-snooping querier mechanism or configure the source ip address of the spontaneous query packets. Use the no form of this command to restore the default value.

ip igmp-snooping querier [address <*ip_addr*>**]**

no ip igmp-snooping querier [address <*ip_addr*>**]**

Parameter

Parameter	Description
ip_addr	Tthe common unicast IP address

Default

disabled，the default source IP address is 10.0.0.200。

Instruction

None

Example

The following command activates IGMP quirier:

```
switch(config)# ip igmp-snooping querier
switch(config)#
```

33.1.8 show ip igmp-snooping

Description

show ip igmp-snooping

Parameter

None

Default

None

Instruction

Use this command to show configuration information of IGMP-snooping.

Example

The following example shows the vlan information of the running ipmp-snooping:

```
switch(config)# show ip igmp-snooping
igmp-snooping router age:260 s
igmp-snooping response time:10 s
   vlan 1
------------
  running
  Router: 90.0.0.120(F0/2)
switch(config)#
```

33.1.9 show ip igmp-snooping timer

Description

show ip igmp-snooping timer

Parameter

None

Default

None

Instruction

Use this command to show timer information of IGMP.

Example

The following example shows timer information of igmp-snooping:

```
switch(config)# show ip igmp-snooping timer
vlan 1 router age : 246
switch(config)#
```

33.1.10 show ip igmp-snooping groups

Description

show ip igmp-snooping groups

Parameter

None

Default

None

Instruction

Use this command to configure multicast group information of IGMP-snooping.

Example

The following example shows the multicast group information of igmp-snooping:

```
switch(config)# show ip igmp-snooping groups
Vlan Source              Group              Type Port(s)
---- --------------- --------------- ---- ------------------------------------
   1 0.0.0.0          234.5.6.6          IGMP F0/2
   1 0.0.0.0          239.255.255.250 IGMP F0/2
switch(config)#
```

33.1.11 show ip igmp-snooping statistics

Description

show ip igmp-snooping statistics

Parameter

None

Default

None

Instruction

Use this command to show IGMP-snooping statistics.

Example

The following example shows igmp-snooping statistics:

```
switch(config)# show ip igmp-snooping statistics
   vlan 1
------------
     v1_packets:1
     v2_packets:2
```

v3_packets:0
general_query_packets:1
special_query_packets:2
join_packets:0
leave_packets:0
send_query_packets:0
err_packets:0
switch(config)#

33.1.12 debug ip igmp-snooping packet

Description

debug ip igmp-snooping packet

no debug ip igmp-snooping packet

Parameter

None

Default

None

Instruction

Use this command to enable/disable the packet debugging switch of IGMP-snooping.

Example

The followig command enables the packet debugging switch of igmp-snooping:

switch(config)# debug ip igmp-snooping packet
switch(config)#

33.1.13 debug ip igmp-snooping timer

Description

debug ip igmp-snooping timer

no debug ip igmp-snooping timer

Parameter

None

Default

None

Instruction

Use this command to enable/disable the timer debugging switch of IGMP-snooping

Example

The following example enables timer debugging switch of igmp-snooping:

```
switch(config)# debug ip igmp-snooping timer
switch(config)#
```

Chapter 34 IGMP Proxy Commands

IGMP-proxy commands include:

Ip igmp-proxy

ip igmp-proxy agent-vlan client-vlan map

ip igmp-proxy source svlan sport

show ip igmp-proxy mcache

show ip igmp-proxy

debug ip igmp-proxy

34.1 ip igmp-proxy enable

Syntax

ip igmp-proxy enable

no ip igmp-proxy enable

To enable or disable IGMP proxy, run **ip igmp-proxy enable**. To resume the default value, run **no ip igmp-proxy enable**.

Parameter

Parameter	Description
N/A	

Default value

The IGMP proxy is disabled by default.

Remarks

N/A

Example

The following example shows how to enable the IGMP proxy:

switch_config# ip igmp-proxy enable

switch_config#

34.2 ip igmp-proxy agent-vlan client-vlan map

Syntax

ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** c*vlan_map*

no ip igmp-proxy agent-vlan avlan_map **client-vlan map** cvlan_map

Parameter

Parameter	Description
a*vlan_map*	Agent VLAN
c*vlan_map*	Customer VLAN

Default value

N/A

Remarks

1. The represented VLAN cannot be configured before vlan is designated by avlan_map; also, the agent VLAN cannot be configured before cvlan_map.

2. The represented and agent VLANs must accept the control of IGMP-Snooping.

Example

The following example shows how to set vlan2 to be the agent vlan of vlan1.

switch_config# ip igmp-proxy agent-vlan 2 client-vlan map 1
switch_config#

34.3 ip igmp-proxy source svlan sport

Syntax

ip igmp-proxy source multi_ip src_ip **svlan** vlan_id **sport** intf_name

no ip igmp-proxy source multi_ip src_ip **svlan** vlan_id **sport** intf_name

To set the entries of the static multicast source, run the above-mentioned command.

Parameter

Parameter	Description
multi_ip	Multicast IP address
src_ip	Multicast source's IP address
vlan_id	Multicast source VLAN
intf_name	Physical port of the multicast source

Default value

N/A.

Remarks

Only when there are multicast source entries can IGMP-proxy work normally. What is mentioned here is to add static multicast source entries.

Example

The following example shows how to add a multicast source entry with 234.5.6.7 as its static multicast address, 1.2.3.4 as its source address, 2 as its source VLAN and gigabit portg0/1 as its source port.

```
switch_config# ip igmp-proxy source 234.5.6.7 1.2.3.4 svlan 2 sport g0/1
switch_config#
```

Note:

The SVLAN mentioned here is the multicast source VLAN and the vlan ID of SVLAN cannot be that of represented VLAN.

34.4 show ip igmp-proxy mcache

Syntax

show ip igmp-proxy mcache *[delete* | *nonsync* | *sync* | *static]*

Parameter

Parameter	Description
delete	Displays those entries of which hardware caches are deleted but software caches do not time out.
nonsync	Displays those entries that have been processed but not yet synchronized to the hardware cache.

sync	Displays those entries already in the hardware cache.
static	Displays the entries of the IGMP-proxy static multicast cache.

Default value

All entries are to be displayed if no filtration conditions are specified.

Remarks

The multicast source entries of IGMP-proxy are displayed.

Example

The following example shows how to display the information about the IGMP-proxy multicast source.

```
Switch# show ip igmp-proxy mcache
Codes: '+' synchronization, '-' deleted, 'S' static
       '^' unsynchronization

Item 1: Group 225.1.1.2
   +(192.168.213.163, 2, G3/24)
  VLAN 3,4
```

34.5 show ip igmp-proxy

Syntax

show ip igmp-proxy

Parameter

N/A

Default value

N/A

Remarks

This command is used to display the configurations about IGMP proxy.

Example

The following example shows how to display the configurations of IGMP proxy.

```
switch#show ip igmp-proxy
Global IGMP proxy configuration:
---------------------------------
Globally enable     : Enable

Agent: vlan 2, it has been alloced

----------------
      Client static     : vlan 1
      Client auto       : vlan
Agent: vlan 3, it has been alloced

----------------
      Client static     : vlan 1
      Client auto       : vlan

Globally clients list
---------------------
      Client              : vlan 1, it has been alloced

Static Multi-source list
---------------------
      Static Source     : No Static Source
switch#
```

34.6 debug ip igmp-proxy

Syntax

debug ip igmp-proxy *[error | event | packet]*

no debug ip igmp-proxy *[error | event | packet]*

Parameter

Parameter	Description
event	Debugs the IGMP-snooping event.
packet	Debugs the reception and transmission of IGMP-snooping.
error	Debugs the IGMP-snooping errors.

Default value

N/A

Remarks

This command is used to enable or disable the debugging & printing switch of IGMP-proxy.

Chapter 35 MLD Multicast Configuration Commands

The MLD multicast configuration commands include:

- **ipv6 mld-snooping**
- **ipv6 mld-snooping solicitation**
- **ipv6 mld-snooping vlan** *vlan_id* **static** *X:X:X:X::X* **interface** *intf*
- **ipv6 mld-snooping timer router-age** *timer_value*
- **ipv6 mld-snooping timer response-time** *timer_value*
- **ipv6 mld-snooping vlan** *vlan_id* **mrouter interface** *inft_name*
- **ipv6 mld-snooping vlan** *vlan_id* **immediate-leave**
- **show ipv6 mld-snooping**
- **show ipv6 mld-snooping timer**
- **show ipv6 mld-snooping groups**
- **show ipv6 mld-snooping statistics**
- **show ipv6 mld-snooping mac**

35.1 ipv6 mld-snooping {enable | disable}

Syntax

ipv6 mld-snooping

no ipv6 mld-snooping

To enable MLD snooping, run **ipv6 mld-snooping**.

Parameter

None

Default value

This command is used to enable MLD snooping.

Remarks

After MLD snooping is enabled, when DLF occurs on multicast packets (that is, the destination address is not registered in the swap chip through the MLD-snooping), all multicast packets whose destination addresses are not registered on any port will be dropped.

Example

The following example shows how to enable the MLD snooping function:

switch_config# ipv6 mld-snooping

35.2 ipv6 mld-snooping solicitation

Syntax

ipv6 mld-snooping solicitation

no ipv6 mld-snooping solicitation

To enable or disable the hardware forwarding of the multicast group, run **ip mld-snooping solicitation**.To resume the default value, run **no ip mld-snooping solicitation**.

Parameter

None

Default value

This function is shut down.

Remarks

None

Example

The following example shows how to enable the hardware forward of the multicast group.

switch_config#**ipv6 mld-snooping solicitation**

35.3 ipv6 mld-snooping vlan *vlan_id* static *X:X:X:X::X* interface *intf*

Syntax

ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf*

no ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf*

Parameter

Parameter	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094
X:X:X:X::X	IP address of the multicast
inft	An interface

Default value

None

Remarks

This command is used to configure the static multicast address of VLAN. Its negative form is used to cancel the static multicast address.

Example

The following example shows how to add the static multicast address, ff12::5, to interface g1/1.

```
switch_config# ipv6 mld-snooping vlan 1 static ff12::5 interface g1/1
switch_config#
```

35.4 ipv6 mld-snooping timer router-age *timer_value*

Syntax

ipv6 mld-snooping timer router-age *timer_value*

no ipv6 mld-snooping timer router-age

Parameter

Parameter	Description

time value	Queries the time of the timer. Value range: 10-2147483647

Default value

260 seconds

Remarks

This command is used to query the time of the timer of MLD-Snooping. The negative form of this command is used to resume the default value.

Example

The following example shows how to set the query time of the router to 300 seconds.

```
switch_config# ipv6 mld-snooping timer router-age 300
switch_config#
```

35.5 ipv6 mld-snooping timer response-time *timer_value*

Syntax

ipv6 mld-snooping timer response-time *timer_value*

no ipv6 mld-snooping timer response-time

To configure the maximum response time of IGMP snooping, run **ip mld-snooping timer response-time *timer_value***. To resume the default value of IGMP snooping, run **no ip mld-snooping timer response-time *timer_value***.

Parameter

Parameter	Description
time value	Queries the time of the timer. Value range: 1-255

Default value

15 seconds

Remarks

None

Example

The following example shows how to set the query response time of IGMP snooping to 20 seconds.

switch_config# ipv6 mld-snooping timer response-time 20

35.6 ipv6 mld-snooping vlan *vlan_id* mrouter interface *inft_name*

Syntax

ipv6 mld-snooping vlan *vlan_id* **mrouter** interface *inft_name*

no ipv6 mld-snooping vlan *vlan_id* **mrouter** interface *inft_name*

To set the static multicast router's port of MLD snooping, run the first one of the above-mentioned commands.

Parameter

Parameter	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094
X:X:X:X::X	IP address of the multicast
inft_name	Shows the port type, the slot and the port ID.

Default value

15 seconds

Remarks

None

Example

The following example shows how to set interface g1/4 to be the interface of the static multicast router of MLD snooping.

switch_config# ipv6 mld-snooping vlan 1 mrouter interface g1/4

35.7 ipv6 mld-snooping vlan *vlan_id* immediate-leave

Syntax

ipv6 mld-snooping vlan *vlan_id* **immediate-leave**

no ipv6 mld-snooping vlan *vlan_id* **immediate-leave**

Parameter

Parameter	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default value

The immediate-leave functionality is disabled.

Remarks

This command is used to set the immediate-leave functionality.

Example

The following example shows how to enable the immediate-leave functionality on VLAN 1:

```
switch_config# ipv6 mld-snooping vlan 1 immediate-leave
switch_config#
```

35.8 show ipv6 mld-snooping

Syntax

show ipv6 mld-snooping

Parameter

None

Default value

None

Remarks

This command is used to display the information about MLD-snooping configuration.

Example

The following example shows how to display the information about MLD snooping.

```
switch#show ipv6 mld-snooping

Global MLD snooping configuration:
-----------------------------------
Globally enable          : Enabled
Querier                  : Enabled
Querier address          : FE80::3FF:FEFE:FD00:1
Router age               : 260 s
Response time            : 10 s
Handle Solicitation    : Enabled

Vlan 1:
----------
      Running
      Routers: SWITCH(querier);
Vlan 2:
----------
      Running
      Routers: SWITCH(querier);
Switch_config#show ipv6 mld-s g
Vlan Group                Type Port(s)
---- --------------- ---- ---------------------------------------
    1 FF02::1:FF13:647D MLD    G1/23
    1 FF02::1:FF13:394 MLD    G1/23
    2 FF02::1:FF00:2    MLD    G1/22
    1 FF02::1:FF00:12 MLD    G1/23
    1 FF02::1:FF00:2    MLD    G1/23
    2 FF02::1:FF61:9901 MLD    G1/22
switch#
```

35.9 show ipv6 mld-snooping timer

Syntax

show ipv6 mld-snooping timer

Parameter

None

Default value

None

Remarks

This command is used to display the information about the MLD-snooping clock.

Example

The following example shows how to display the information about the MLD-snooping clock.

switch#**show ipv6 mld-snooping timers**

vlan 1 Querier on port 0 : 251
vlan 2 Querier on port 0 : 251
vlan 2 multicast address 3333.0000.0005 response time : 13

switch#

vlan 2 multicast address 3333.0000.0005 response time : This shows the time period from receiving a multicast query packet to the present; if there is no host to respond when the timer times out, the port will be canceled.

35.10 show ipv6 mld-snooping groups

Syntax

show ipv6 mld-snooping groups

Parameter

None

Default value

None

Remarks

This command is used to display the information about the multicast group of MLD-snooping.

Example

The following example shows how to display the information about the multicast group of MLD-snooping.

switch# show ipv6 mld-snooping timer

Vlan Group Type Port(s)

```
---- ---------------- ---- ---------------------------------------
   2 FF02::1:FF00:2    MLD    G2/22
   2 FF02::1:FF61:9901 MLD    G2/22
   1 FF02::1:FF13:394 MLD    G2/23
   1 FF02::1:FF00:2    MLD    G2/23
   1 FF02::1:FF00:12 MLD    G2/23
   1 FF02::1:FF13:647D MLD    G2/23
switch#
```

35.11 show ipv6 mld-snooping statistics

Syntax

show ipv6 mld-snooping statistics

Parameter

None

Default value

None

Remarks

This command is used to display the information about MLD-snooping statistics.

Example

The following example shows how to display the information about MLD-snooping statistics.

```
switch#show ipv6 mld-snooping statistics
v1_packets:0          Quantity of MLD v1 packets
v2_packets:6          Quantity of MLD v2 packets
v3_packets:0          Quantity of MLD v3 packets
general_query_packets:5       Quantity of general query packets
special_query_packets:0       Quantity of special query packets
listener_packets:6       Quantity of Report packets
done_packets:0       Quantity of Leave packets
err_packets:0         Quantity of error packets
```

35.12 show ipv6 mld-snooping mac

Syntax

show ipv6 mld-snooping mac

Parameter

None

Default value

None

Remarks

This command is used to display the multicast MAC of MLD snooping.

Example

The following example shows how to display the multicast MAC of MLD snooping.

```
switch#show ipv6 mld-snooping mac
   Vlan Mac                    Ref Flags
   ---- --------------- ---- ------
       1 3333:0000:0001      1    2
       2 3333:ff61:9901      1    0
             FF02::1:FF61:9901
       1 3333:0000:0002      1    2
       1 3333:ff00:0002      1    0
             FF02::1:FF00:2
       1 3333:ff00:0012      1    0
             FF02::1:FF00:12
       1 3333:ff13:647d      1    0
             FF02::1:FF13:647D
       2 3333:ff00:0002      1    0
             FF02::1:FF00:2
       1 3333:ff13:0394      1    0
             FF02::1:FF13:394
       1 3333:ff00:0001      1    2
       1 3333:ff8e:7000      1    2
switch#
```

Ref means the quantity of referred IPv6 addresses of MAC.

Flags means the debug output information, and 2 means the information need be sent to CPU.

Chapter 36 OAM Configuration Commands

36.1 OAM Configuration Commands

The following are OAM configuration commands:

- ethernet oam
- ethernet oam {max-rate | min-rate | mode | timeout }
- ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action
- ethernet oam remote-loopback {supported | timeout}
- ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high
- ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low
- ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window
- ethernet oam link-monitor high-threshold action
- ethernet oam link-monitor negotiation-supported

36.1.1 ethernet oam

Description

[**no**] **ethernet oam**

To enable or disable the OAM function, run [**no**] **ethernet oam**.

Parameter

None

Default

Ethernet OAM is disabled by default.

Command mode

Port configuration mode

Explanation

None

Example

The following commands are used to enable the OAM function on GigaEthernet 0/2 interface.

Switch#
Switch#config
Switch_config#interface g0/2
Switch_config_g0/2#ethernet oam

36.1.2 ethernet oam {max-rate | min-rate | mode | timeout }

Description

[**no**] **ethernet oam {max-rate** *value1* **| min-rate** *value2* **| mode {active | passive} | timeout** *value3***}**

ethernet oam max-rate *value1* is used to set the fastest transmission rate of the OAM packet.

ethernet oam max-rate *value2* is used to set the slowest transmission rate of the OAM packet.

ethernet oam mode {active | passive} is used to set the OAM mode.

ethernet oam timeout *value3* is used to set the timeout time of the OAM connection.

Parameter

Parameter	Description
value1	Fastest transmission rate, which ranges between 1 and 10. Its unit is packet/second.
value2	Slowest transmission rate, which ranges between 1 and 10. Its unit is second.
value3	Timeout time of the OAM connection, which ranges between 2 and 30 and whose unit is second

Default

The value of **max-rate** is 10.

The value of **min-rate** is 1.

The value of **timeout** is 5.

The value of **mode** is **active**.

Command mode

Port configuration mode

Explanation

This command can be used to configure some optional parameters for establishing the OAM connection.

Example

The following example shows how to set the fastest and slowest connection rates of the OAM on the GigaEthernet 0/2 interface to 5 packets/second, the connection timeout time to 10 seconds and the OAM mode to **passive**.

```
Switch #config
Switch_config#
Switch_config#interface g0/2
Switch_config_g0/2# ethernet oam max-rate 5
Switch_config_g0/2#ethernet oam min-rate 5
Switch_config_g0/2#ethernet oam timeout 10
Switch_config_g0/2#ethernet oam mode passive
```

36.1.3 ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action

Description

ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action error-disable-interface

no ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action

This command is used to configure the trigger action after the remote fault instruction is received.

Parameter

None

Default

No trigger action is conducted after the remote fault instruction is received.

Command mode

Port configuration mode

Explanation

switch cannot generate the LINK FAULT packets and the Critical Event packets. However, these packets will be handled if they are received from the remote terminal. router can transmit and receive the Dying Gasp packet. When the local port enters the **errdisabled** state or is closed by the administrator or the OAM function of the local port is closed by the manager, the Dying Gasp packet will be transmitted to the remote terminal that connects the local port.

Example

The following example shows how to set the GigaEthernet0/2 port as the access port of VLAN10:

Switch(config)#interface f0/1

Switch(config)#vlan10

Switch(config-f0/1)#switchport pvid 10

36.1.4 ethernet oam remote-loopback {supported | timeout}

Description

The command **ethernet oam remote-loopback supported** is used to configure the remote loopback function.

The **ethernet oam remote-loopback timeout *value*** is used to configure the timeout time of the remote loopback.

Parameter

Parameter	Description
value3	Timeout time of the OAM connection, which ranges between 1 and 10 and whose unit is second

Default

Two seconds

Command mode

Port configuration mode

Explanation

The timer is effective only to the loopback master terminal. If the slave terminal does not receive the response from the slave terminal in the regulated timeout time after the master terminal transmits the **start** or **stop** request, the system will exit the loopback mode automatically.

Example

The following example shows how to set the timeout time of loopback on the GigaEthernet 0/2 port to 5 seconds.

```
Switch_config_g0/2#ethernet oam remote-loopback timeout 5
```

36.1.5 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high

Description

[**no**] **ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high {none |** *value***}**

To configure the high threshold for link monitoring, run the previous command.

Parameter

Parameter	Description
Value	Error-signal period event ranges between 1 and 65535, whose unit is signal number. Error-frame event ranges between 1 and 65535, whose unit is frame number. Error-frame event ranges between 1 and 65535, whose unit is frame number. Error-frame second event ranges between 1 and 900, whose unit is second. Error-CRC event ranges between 1 and 65535, whose unit is frame number.

Default

The default value of each general link event is **none**.

Command mode

Port configuration mode

Explanation

After the high threshold of an event and **ethernet oam link-monitor high-threshold action error-disable-interface** are configured, the local port enters the **errdisabled** state when the local port receives the high threshold of the event.

Example

The following example shows how to configure the high threshold of the error-frame event to **10** on interface GigaEthernet0/2.

```
Switch_config_g0/2#ethernet oam link-monitor symbol-period threshold high 10
```

36.1.6 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low

Description

[**no**] **ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low {none |** *value***}**

To configure the low threshold for link monitoring, run the previous command.

Parameter

Parameter	Description
Value	Error-signal period events ranges between 1 and 65535, whose unit is signal number. Error-frame event ranges between 1 and 65535, whose unit is frame number. Error-frame event ranges between 1 and 65535, whose unit is frame number. Error-frame second event ranges between 1 and 900, whose unit is second. Error-CRC event ranges between 1 and 65535, whose unit is frame number.

Default

The default value of the error-signal period event is 1.

The default value of the error-frame event is 1.

The default value of the error-frame period event is 1.

The default value of the error-frame second event is 1.

The default value of the error-CRC event is 10.

Command mode

Port configuration mode

Explanation

After the low threshold of an event is configured and the locally-received event exceeds the low threshold, the Event Notification OAM packet will be transmitted to notify the peer terminal.

Example

The following example shows how to set the low threshold of the error-frame event to **10** on interface GigaEthernet0/2.

Switch_config_g0/2#ethernet oam link-monitor symbol-period threshold low 10

36.1.7 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window

Description

ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window *value*

To configure the size of the round-query window for link monitoring, run the previous command.

Parameter

Parameter	Description
Value	The error-signal period event ranges between 10 and 600 on GigaEthernet and ranges between 1 and 60 on FastEthernet. The unit is 100M signals. The error-frame event ranges between 1 and 60, whose unit is second. The error-frame period event ranges between 100 and 6000 on GigaEthernet and ranges between 10 and 600 on FastEthernet. The unit is 14881 frames. Error-frame second event ranges between 10 and 900, whose unit is second. The error-CRC event ranges between 1 and 180, whose unit is second.

Default

The default value of the error-signal period event is 10 on GigaEthernet and is 1 on FastEthernet.

The default value of the error-frame event is 1.

The default value of the error-frame period event is 100 on GigaEthernet and is 10 on FastEthernet.

The default value of the error-frame second event is 60.

The default value of the error-CRC event is 1.

Command mode

Port configuration mode

Explanation

None

Example

The following example shows how to set the window of the error-frame period event to **50** on interface GigaEthernet0/2.

```
Switch_config_g0/2#ethernet oam link-monitor symbol-period window 50
```

36.1.8 ethernet oam link-monitor high-threshold action

Description

ethernet oam link-monitor high-threshold action error-disable-interface

[**no**] **ethernet oam link-monitor high-threshold action**

To configure the link-monitor trigger event with the high threshold, run **ethernet oam link-monitor high-threshold action error-disable-interface**.

Parameter

None

Default

The high-threshold trigger event does not exist by default.

Command mode

Port configuration mode

Description

After the high threshold of an event and **ethernet oam link-monitor high-threshold action error-disable-interface** are configured, the local port enters the **errdisabled** state when the local port receives the high threshold of the event.

Example

The following example shows how to set the high-threshold trigger event on interface GigaEthernet 0/2 to **error-disable-interface**.

Switch_config_g0/2#ethernet oam link-monitor high-threshold action error-disable-interface

36.1.9 ethernet oam link-monitor negotiation-supported

Description

[**no**] **ethernet oam link-monitor negotiation-supported**

To configure the link-monitor negotiation, run **ethernet oam link-monitor negotiation-supported**.

Parameter

None

Default

Link-monitor negotiation is supported.

Command mode

Port configuration mode

Description

devices support link monitoring. However, if the third-party devices do not support link monitoring, devices automatically do not support link monitoring during OAM Discovery and the OAM connection can be established through the third-party devices in this case. Otherwise, when the link-monitor negotiation is not configured, devices mandatorily support the link-monitor function, but the OAM connection cannot be created if the third-party devices do not support the link-monitor function.

Example

The following example shows that the link-monitor function is not supported on interface GigaEthernet 0/2.

Switch_config_g0/2#no ethernet oam link-monitor negotiation-supported

36.1.10 ethernet oam remote-loopback {start | stop}

Description

ethernet oam remote-loopback {start | stop} interface intf-type intf-id

To start or stop the remote OAM loopback, run the previous command.

Parameter

Parameter	Description
intf-id	Designates an interface.

Default

None

Command mode

Privileged mode

Description

The remote OAM loopback cannot be enabled on the physical interface that belongs to the aggregation interface.

Example

The following example shows how to positively start the remote OAM loopback on interface GigaEthernet 0/2.

Switch#ethernet oam remote-loopback start interface g0/2

36.1.11 clear ethernet oam statistics

Description

clear ethernet oam statistics [interface intf-type intf-id**]**

To clear the OAM statistics information, run the previous command.

Parameter

Parameter	Description
intf-id	Designates an interface. If an interface is not designated, the OAM statistics information on all interfaces will be deleted.

Default

None

Command mode

Privileged mode

Description

After this command is run, the following statistics information (type-classified packet numbering information, link-event statistics information and remote trouble statistics information) is deleted meanwhile.

Example

The following example shows how to clear the OAM statistics information on interface GigaEthernet 0/2.

```
Switch#clear ethernet oam statistics interface g0/2
```

36.1.12 show ethernet oam discovery

Description

show ethernet oam discovery interface [intf-type intf-id]

To display the OAM discovery information on all interfaces or a designated interface, run the previous command.

Parameter

Parameter	Description
intf-id	Displays the Discovery information on the designated interface or on all protocol-up ports and enables the Discovery information on the OAM interface.

Default

None

Description

None

Example

The following example shows how to display the OAM discovery information on interface GigaEthernet 0/2.

```
Switch_config_g0/2#show ethernet oam discovery interface g0/2
GigaEthernet0/2
Local Info TLV
--------------
PDU revision:         1

Loopback status:     LB_DISABLED

OAM configurations field:
   Mode                    : active
   Unidirection          : not supported
   Remote loopback     : supported
   Link Events           : supported
   Variable retrieval: not supported

Mtu size:               1500

OUI:                     00e00f

Remote Info TLV
---------------
MAC address:              001b.0d9c.e703

PDU revision:         0

OAM configurations field:
   Mode                    : active
   Unidirection          : not supported
   Remote loopback     : not supported
   Link Events           : supported
   Variable retrieval: not supported

Mtu size:               1500

OUI:                     00000c
```

36.1.13 show ethernet oam statistics {pdu | link-monitor | remote-failure}

Description

show ethernet oam statistics {pdu | link-monitor | remote-failure} interface [intf-type intf-id]

To display the OAM statistics information on a designated interface or all interfaces, run the previous command.

Parameter

Parameter	Description
intf-id	Displays the statistics information on the designated interface or on all protocol-up ports and enables the statistics information on the OAM interface.

Default

None

Description

None

Example

The following example shows how to display the classified OAM packet numbering information on interface GigaEthernet 0/2.

```
Switch#show ethernet oam statistics pdu interface g0/2
GigaEthernet0/2
Counters:
---------
Information OAMPDU Tx                 : 59
Information OAMPDU Rx                 : 56
Unique Event Notification OAMPDU Tx   : 0
Unique Event Notification OAMPDU Rx   : 0
Duplicate Event Notification OAMPDU TX: 0
Duplicate Event Notification OAMPDU RX: 0
Loopback Control OAMPDU Tx            : 0
Loopback Control OAMPDU Rx            : 0
Variable Request OAMPDU Tx            : 0
Variable Request OAMPDU Rx            : 0
Variable Response OAMPDU Tx           : 0
Variable Response OAMPDU Rx           : 0
```

Organization Specific OAMPDU Tx : 0
Organization Specific OAMPDU Rx : 0
Unsupported OAMPDU Tx : 0
Unsupported OAMPDU Rx : 0
Frames Lost due to OAM : 0

36.1.14 show ethernet oam configuration

Description

show ethernet oam configuration interface [intf-type intf-id]

To display the OAM configuration information on all interfaces or a designated interface, run **show ethernet oam configuration interface [intf-type intf-id]**.

Parameter

Parameter	Description
intf-id	Displays the OAM configuration information on the designated interface or on all protocol-up ports and enables the configuration information on the OAM interface.

Default

None

Description

None

Example

The following example shows how to display the OAM configuration information on interface GigaEthernet 0/2.

Switch#show ethernet oam configuration interface g0/2
GigaEthernet0/2
General

Admin state : enabled
Mode : active
PDU max rate : 10 packets/second
PDU min rate : 1 seconds/packet
Link timeout : 1 seconds
High threshold action: no action

Remote Failure

Link fault action : no action
Dying gasp action : no action
Critical event action: no action

Remote Loopback

Is supported : supported
Loopback timeout : 2

Link Monitoring

Negotiation : supported
Status : on

Errored Symbol Period Event
Window : 10 * 100M symbols
Low threshold : 1 error symbol(s)
High threshold : none

Errored Frame Event
Window : 1 seconds
Low threshold : 1 error frame(s)
High threshold : none

Errored Frame Period Event
Window : 100 * 14881 frames
Low threshold : 1 error frame(s)
High threshold : none

Errored Frame Seconds Summary Event
Window : 60 seconds
Low threshold : 1 error second(s)
High threshold : none

Errored CRC Frames Event
Window : 1 seconds
Low threshold : 10 error frame(s)
High threshold : none

36.1.15 show ethernet oam runtime

Description

show ethernet oam runtime interface [intf-type intf-id]

To display the OAM running information on all interfaces or a designated interface, run the previous command.

Parameter

Parameter	Description
intf-id	Displays the Runtime information on the designated interface or on all protocol-up ports and enables the Runtime information on the OAM interface.

Default

None

Description

None

Example

The following example shows how to display the OAM Runtime information on interface GigaEthernet 0/2.

```
Switch#show ethernet oam runtime interface g0/2
GigaEthernet0/2
Runtime Settings:
-----------------
local_pdu              : NOT_WORKING
local_mux              : FWD
local_par              : FWD
local_link_status : OK
local_satisfied     : FALSE
local_stable          : FALSE
pdu_cnt                 : 10
pdu_timer              : stopped
lost_link_timer     : stopped
remote_state_valid: FALSE
remote_stable        : FALSE
remote_evaluating : FALSE

Discovery State Machine:
------------------------
Last 10 state transition recorded: INACTIVE -> FAULT -> ACTIVE_SEND_LOCAL -> SEN
D_LOCAL_REMOTE -> SEND_LOCAL_REMOTE_OK -> SEND_ANY -> INACTIVE
```

36.1.16 debug ethernet oam remote-loopback

Description

debug ethernet oam remote-loopback

To enable the debugging switch of remote OAM loopback, run the previous command.

Parameter

None

Default

None

Command mode

Privileged mode

Description

When this command is run, the state switchover process of the remote state machine will be displayed.

36.1.17 debug ethernet oam packet {tx | rx}

Description

debug ethernet oam packet [tx | rx]

To enable the debugging switch of the OAM output packet's content, run the previous command.

Parameter

None

Default

None

Command mode

Privileged mode

Description

If **tx** and **rx** are not entered and the **Enter** key is pressed directly, all received and transmitted OAM PDU content will be exported and the remaining length of the frame-header-excluded packet will be displayed. **tx** means to export only the content of the transmitted OAM PDU; **rx** means to export only the content of the received OAM PDU.

Example

omitted

36.1.18 debug ethernet oam discovery-sm

Description

debug ethernet oam discovery-sm

To open the debugging switch of the OAM discovery state machine, run the previous command.

Parameter

None

Default

None

Command mode

Privileged mode

Description

None

Example

omitted

36.1.19 debug ethernet oam error

Description

debug ethernet oam error

To open the error-treated debugging switch of the OAM packet, run the previous command.

Parameter

None

Default

None

Command mode

Privileged mode

Description

None

Example

omitted

Chapter 37 CFM and Y1731 Configuration Commands

37.1 CFM Configuration Commands

37.1.1 Adding the Maintenance Domain and Entering the Maintenance Domain Mode

1. Syntax

ethernet cfm md mdnf *{string}* **mdn** <*char_string*> [**level** <*0-7*> | **creation** <*MHF_creation_type*> | **sit** <*sender_id_type*> | **ip** <*IP_address*>]

2. Function

To add a maintenance domain or enter the already existent maintenance domain, run the above-mentioned command.

3. Parameter

Parameter	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
level	Stands for the level of the maintenance domain, which is optional. If it is not chosen, its default value is 0.
creation	Stands for the creation mode of MIP, which is optional. If it is not chosen, its default value is **none**.
sit	Stands for the type of sender ID, which is optional. If it is not chosen, its default value is **none**.
ip	Stands for IP address of the trouble alarm server, which is optional. If it is not chosen, its default value is 0.0.0.0.

4. Mode

Global configuration mode

5. Example

Switch_config#ethernet cfm md mdnf string mdn customer level 5

6. Related command

N/A

37.1.2 Deleting the Maintenance Domain

1. Syntax

no ethernet cfm md mdnf *{string}* **mdn** <*char_string*>

2. Function

To delete a designated maintenance domain, run the above-mentioned command.

3. Parameter

Parameter	Description
Mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
Mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.

4. Mode

Global configuration mode

5. Example

Switch_config#no ethernet cfm md mdnf string mdn customer

6. Related command

N/A

37.1.3 Browsing the Maintenance Domain

1. Syntax

show ethernet cfm md [mdnf *{string}* **mdn** <*char_string*>**]**

2. Function

To browse all the maintenance domains or the designated maintenance domains of the local device, run the above-mentioned command.

3. Parameter

Parameter	Description
mdnf	Stands for the format of the name of a to-be-browsed designated maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of a to-be-browsed designated maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.

4. Mode

EXEC, global, interface, maintenance domain

5. Example

Switch_config#show ethernet cfm md mdnf string mdn customer

6. Related command

N/A

37.1.4 Adding a Maintenance Association

1. Syntax

ma manf *{string}* **man** <*char_string*> **ci** *{100ms* | *1s* | *10s* | *1min* | *10min}* **meps** <*mepids*> [**vlan** <*1-4094*> | **creation** <*MHF_creation_type*> | **sit** <*sender_id_type*> | **ip** <*IP_address*>]

2. Function

To add a maintenance association, run the above-mentioned command.

3. Parameter

Parameter	Description
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string mode.
ci	Stands for the transmission interval of CCM. The shortest transmission interval which is supported presently is 100ms.
meps	Stands for the MEPID of all MEPs in the local maintenance domain.
vlan	Stands for the identifier of the VLAN where the maintenance association is located, which is optional. If it is not chosen, its default value is 1.
creation	Stands for the creation mode of MIP, which is optional. If it is not chosen, its default value is **none**.
Sit	Stands for the type of sender ID, which is optional. If it is not chosen, its default value is **none**.
ip	Stands for IP address of the trouble alarm server, which is optional. If it is not chosen, its default value is 0.0.0.0.

4. Mode

Maintenance domain mode

5. Example

Switch_config_cfm#ma manf string man customer1 ci 1s meps 1-2,2009 vlan 10

6. Related command

N/A

37.1.5 Deleting the Maintenance Association

1. Syntax

no ma manf *{string}* man <*char_string*>

2. Function

To delete a designated maintenance association, run the above-mentioned command.

3. Parameter

Parameter	Description
Manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
Man	Stands for the name of the maintenance association. It is in character string mode.

4. Mode

Maintenance domain mode

5. Example

Switch_config_cfm#no ma manf string man customer

6. Related command

N/A

37.1.6 Browsing the Maintenance Association

1. Syntax

show ethernet cfm ma mdnf *{string}* **mdn** <*char_string*> [**manf** {string} **man** <char_string>]

2. Function

To browse all or designated maintenance associations in a designated maintenance domain on the local device, run the above-mentioned command.

3. Parameter

Parameter	Description

Mdnf	Stands for the format of the name of the maintenance domain where the to-be-browsed maintenance association is located. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain where the to-be-browsed maintenance association is located. It is a character string with 1 to 43 printable characters, capital sensitive.
Manf	Stands for the format of the name of a to-be-browsed maintenance association. At present only the char-string format is supported.
man	Stands for the name of a to-be-browsed maintenance association. It is in character string mode.

4. Mode

EXEC, global, interface, maintenance domain

5. Example

Switch_config#show ethernet cfm ma mdnf string mdn customer manf string man customer1

6. Related command

N/A

37.1.7 Adding MIP

1. Syntax

ethernet cfm mip add level <*0-7*> [**vlan** <*1-4094*>]

2. Function

To add an MIP of a specific level, which belongs to a designated VLAN, on a specific interface, run the above-mentioned command.

3. Parameter

Parameter	Description
Level	Stands for the level of a maintenance domain.
vlan	Stands for the identifier of the VLAN where the maintenance association is located,

	which is optional. If it is not chosen, its default value is 1.

4. Mode

Physical interface configuration mode

5. Example

Switch_config_g0/1#ethernet cfm mip add level 1 vlan 10

6. Related command

N/A

37.1.8 Deleting MIP

1. Syntax

ethernet cfm mip del vlan *<1-4094>*

2. Function

To delete a designated MIP, run the above-mentioned command.

3. Parameter

Parameter	Description
Vlan	Stands for the identifier of the VLAN where MIP is located.

4. Mode

Interface configuration mode

5. Example

Switch_config_g0/1#ethernet cfm mip del vlan 10

6. Related command

N/A

37.1.9 Browsing MIP

【Method 1】

1. Syntax

show ethernet cfm mip vlan *<1-4094>* **interface** *<interface_name>*

show ethernet cfm mip interface *<interface_name>*

2. Function

To browse all MIPs of a designated interface in the local device or MIPs in a specific VLAN, run the above-mentioned command.

3. Parameter

Parameter	Description
interface	Stands for a to-be-browsed interface.
Vlan	Stands for the identifier of a to-be-browsed VLAN.

4. Mode

EXEC, global, interface, maintenance domain

5. Example

Switch_config#show ethernet cfm mip vlan 1 interface g0/1

6. Related command

N/A

【Method 2】

1. Syntax

ethernet cfm mip display

2. Function

To browse all MIPs on the current interface of the local device, run the above-mentioned command.

3. Parameter

N/A

4. Mode

Physical interface mode

5. Example

Switch_config_g0/1#ethernet cfm mip display

6. Related command

N/A

37.1.10 Adding MEP

1. Syntax

ethernet cfm mep add mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*> [**direction** *{up* | *down}* **| ip** <*ip_address*>]

2. Function

To add an MEP, which belongs to a designated maintenance association, on a specific interface, run the above-mentioned command.

3. Parameter

Parameter	Description
Mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
Mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43

	printable characters, capital sensitive.
Manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
Man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
Mepid	Stands for the MEPID of the to-be-added MEP.
direction	Stands for the direction of the to-be-added MEP. If it is not chosen, its default value is **down**.
ip	Stands for IP address of the trouble alarm server, which is optional. If it is not chosen, its default value is 0.0.0.0.

4. Mode

Physical interface configuration mode

5. Example

Switch_config_g0/1#ethernet cfm mep add mdnf string mdn customer manf string man customer1 mepid 2009 direction up

6. Related command

N/A

37.1.11 Deleting MEP

1. Syntax

ethernet cfm mep del mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*>

2. Function

To delete a designated MEP, run the above-mentioned command.

3. Parameter

Parameter	Description
Mdnf	Stands for the format of the name of the maintenance domain. At present only the

	char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
Manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
Mepid	Stands for the MEPID of the to-be-added MEP.

4. Mode

Physical interface configuration mode

5. Example

Switch_config_g0/1#ethernet cfm mep del mdnf string mdn customer manf string man customer1 mepid 2009

6. Related command

N/A

37.1.12 Browsing MEP

【Method 1】

1. Syntax

show ethernet cfm mep mdnf *{string}* **mdn** *<char_string>* **manf** *{string}* **man** *<char_string>* [**mepid** *<1-8191>*] [**view** *{detail | brief}*]

2. Function

To browse the detailed or brief information about all MEPs in the designated maintenance domain of the local device, or that about a specific MEP, run the above-mentioned command.

3. Parameter

Parameter	Description

mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of the to-be-browsed MEP.
view	Means to browse the detailed information or the brief information. It is the detailed information that will be browsed by default.

4. Mode

EXEC, global, interface, maintenance domain

5. Example

Switch_config#show ethernet cfm mep mdnf string mdn x manf string man x view brief

6. Related command

N/A

【Method 2】

1. Syntax

ethernet cfm mep display

7. Function

To browse all MEPs on the current interface of the local device, run the above-mentioned command.

8. Parameter

N/A

9. Mode

Physical interface mode

10. Example

Switch_config_g0/1#ethernet cfm mep display

11. Related command

N/A

37.2 Y1731 Configuration Commands

2.2.1 Modifying the Transmission Interval of the AIS Frame

Syntax

ethernet y1731 ais-mep timer *time*
To modify the transmission interval of the AIS frame, run the above-mentioned command:
[**no**] **ethernet y1731 ais-mep timer**
To resume the default transmission interval, run the above-mentioned command.

Parameter

Parameter	Description
time	Stands for the transmission interval of the AIS frame. <1> -- 1 frame per second <2> -- 1 frame per minute

Default value

The default transmission interval is one frame every second.

Command mode

Global configuration mode

Explanation

If a current device supports Eth-AIS and have to go through 4094 VLANs, the AIS frames it sends every second may cause tension. Therefore the current device has to support another AIS transmission period based on one minute. The AIS frame exchanges the AIS transmission interval through its period field.

Example

The following example shows how to modify the transmission interval of the AIS frame to 1 minute.

```
Switch#
Switch#config
Switch_config#ethernet y1731 ais-mep timer 2
Switch_config#
```

37.2.2 Performing the Termination Command

Syntax

ethernet y1731 terminate

The above-mentioned command is used to conduct the termination command.

Parameter

N/A

Default value

N/A

Command mode

Global configuration mode

Explanation

This command can be used to terminate the running **delay-measurement** command:

Example

The following example shows how to terminate the operation which is running in global configuration mode:

```
Switch#
Switch#config
Switch_config#ethernet y1731 terminate
Switch_config#
```

37.3 CFM Maintenance Commands

37.3.1 loopback

1. Syntax

ethernet cfm loopback mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*> **mac** <*AA:BB:CC:DD:EE:FF*> [**number** <*1-64*>]

2. Function

To use a designated MEP at the local terminal to conduct loopback towards another designated MEP at the remote terminal, run the above-mentioned command.

3. Parameter

Parameter	Description
Mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
Mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
Manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
Man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of the local MEP.
mac	Stands for the MAC address of the remote MEP.
number	Stands for the loopback times, which is optional. If it is not chosen, its default value is 3.

4. Mode

EXEC

5. Example

Switch#ethernet cfm loopback mdnf string mdn x manf string man x mepid 1 mac 00:15:E9:43:AD:E3 number 3

6. Related command

N/A

37.3.2 linktrace

1. Syntax

ethernet cfm linktrace mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man**

<*char_string*> **mepid** <*1-8191*> **mac** <*AA:BB:CC:DD:EE:FF*> [**ttl** *{1-255}* | **fdb-only** *{yes}*]

2. Function

To use a designated local MEP to conduct linktrace towards a designated remote MEP, run the above-mentioned command.

3. Parameter

Parameter	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of the local MEP.
mac	Stands for the MAC address of the remote MEP.
ttl	Stands for the TTL value, which is optional. If it is not chosen, its default value is 64.
fdb-only	Means whether LTM forwarding is only via MAC address, which is optional. If it is not chosen, its default value is **yes**.

4. Mode

EXEC

5. Example

Switch#ethernet cfm linktrace mdnf s mdn x manf string man x mepid 1 mac 00:15:E9:43:AD:E3 ttl 64

6. Related command

N/A

37.3.3 Deleting the Linktrace Result Table

1. Syntax

clear ethernet cfm linktrace mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> [**mepid** <*1-8191*>]

2. Function

To delete the linktrace result table of a designated MEP, run the above-mentioned command.

3. Parameter

Parameter	Description
Mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
Mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
Manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
Man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
Mepid	Stands for the MEPID of the local MEP.

4. Mode

EXEC

5. Example

Switch#clear ethernet cfm linktrace mdnf string mdn x manf string man x mepid 1

6. Related command

N/A

37.3.4 Setting the Size of the Linktrace Result Table

1. Syntax

ethernet cfm linktrace table-size *<1-16>*

2. Function

To set the size of the linktrace result table (that is, the number of linktraces which can be conducted concurrently), run the above-mentioned command.

3. Parameter

Parameter	Description
table-size	Stands for the size of the linktrace result table.

4. Mode

Global configuration mode

5. Example

Switch_config#ethernet cfm linktrace table-size 1

6. Related command

N/A

37.3.5 Setting the Number of Entries in the Linktrace Result Table

1. Syntax

ethernet cfm linktrace entry-number *<2-4095>*

2. Function

To set the maximum number of entries that are received each time by the linktrace result table, run the above-mentioned command.

3. Parameter

Parameter	Description
entry-number	Stands for the number of the entries in the linktrace result table.

4. Mode

Global configuration mode

5. Example

Switch_config#ethernet cfm linktrace entry-number 2009

6. Related command

N/A

37.3.6 Setting the Aging Time of the Linktrace Result Table

1. Syntax

ethernet cfm linktrace hold-time *<1-29>*

2. Function

It is used to set the saving time of the LTR table after the first Linktrace (unit: minute).

3. Parameter

Parameter	Description
hold-time	Stands for the aging time of the linktrace result table. Unit: minute

4. Mode

Global configuration mode

5. Example

Switch_config#ethernet cfm linktrace hold-time 10

6. Related command

N/A

37.3.7 Deleting the MEP Statistics Data

1. Syntax

ethernet cfm mep clear mdnf *{string}* **mdn** *<char_string>* **manf** *{string}* **man** *<char_string>* **mepid** *<1-8191>*

2. Function

To delete the statistics data of a designated MEP, run the above-mentioned command.

3. Parameter

Parameter	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of a designated MEP.

4. Mode

Physical interface mode

5. Example

Switch_config_g0/1#ethernet cfm mep clear mdnf string mdn x manf string man x mepid 1

6. Related command

N/A

37.3.8 Conducting the Loss Measurement Command

1. Syntax

ethernet cfm lm-start mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*> **mac** <*AA:BB:CC:DD:EE:FF*> [**number** <*1-64*>]

2. Function

To use a designated MEP at the local terminal to conduct the LM operation towards another designated MEP at the remote terminal, run the above-mentioned command.

3. Parameter

Parameter	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of the local MEP.
mac	Stands for the MAC address of the remote MEP.
number	Stands for the LM times, which is optional. If it is not chosen, its default value is 0, which means the LM operation always continues.

4. Mode

EXEC

5. Example

Switch#ethernet cfm lm-start mdnf string mdn x manf string man x mepid 1 mac 00:15:E9:43:AD:E3 number 3

6. Related Command

N/A

37.3.9 Disabling the Loss Measurement Command

1. Syntax

ethernet cfm lm-stop mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*>

2. Function

To stop the LM operation of a designated MEP, run the above-mentioned command.

3. Parameter

Parameter	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of the local MEP.

4. Mode

EXEC

5. Example

Switch#ethernet cfm lm-stop mdnf string mdn x manf string man x mepid 1

6. Related command

N/A

37.3.10 Enabling the Delay Measurement Command

1. Syntax

ethernet cfm dm-start mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*> **mac** <*AA:BB:CC:DD:EE:FF*> [**number** <*1-64*>]

2. Function

To use a designated MEP at the local terminal to conduct the DM operation towards another designated MEP at the remote terminal, run the above-mentioned command.

3. Parameter

Parameter	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of the local MEP.
mac	Stands for the MAC address of the remote MEP.
number	Stands for the DM times, which is optional. If it is not chosen, its default value is 0, which means the LM operation always continues.

4. Mode

EXEC

5. Example

Switch#ethernet cfm dm-start mdnf string mdn x manf string man x mepid 1 mac 00:15:E9:43:AD:E3 number 3

6. Related command

N/A

37.3.11 Disabling the Delay Measurement Command

1. Syntax

ethernet cfm dm-stop mdnf *{string}* **mdn** *<char_string>* **manf** *{string}* **man** *<char_string>* **mepid** *<1-8191>*

2. Function

停止指定的 MEP 的 LM 操作。

3. Parameter

Parameter	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of the local MEP.

4. Mode

EXEC

5. Example

Switch#ethernet cfm dm-stop mdnf string mdn x manf string man x mepid 1

6. Related command

N/A

37.4 CFM Control Commands

37.4.1 CFM Stack Control Command

1. Syntax

ethernet cfm *{enable* | *disable}*

2. Function

To enable or disable the whole CFM protocol stack, run the above-mentioned command.

3. Parameter

N/A

4. Mode

Global configuration mode

5. Example

Switch_config#ethernet cfm enable

6. Related command

N/A

37.4.2 CFM Interface Control Command

1. Syntax

ethernet cfm *{enable* | *disable}*

2. Function

To enable or disable the CFM function of the current interface, run the above-mentioned command.

3. Parameter

N/A

4. Mode

Physical interface mode

5. Example

Switch_config_g0/1#ethernet cfm enable

6. Related command

N/A

37.4.3 MIP Control Command

1. Syntax

ethernet cfm mip *{enable* | *disable}* **vlan** *<1-4094>*

2. Function

To enable or disable the MIP of a designated VLAN on the current interface, run the above-mentioned command.

3. Parameter

N/A

4. Mode

Physical interface mode

5. Example

Switch_config_g0/1#ethernet cfm mip enable vlan 1

6. Related command

N/A

37.4.4 MEP Control Command

1. Syntax

ethernet cfm mep *{enable | disable}* **mdnf** *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*>

2. Function

To enable or disable a designated MEP, run the above-mentioned command.

3. Parameter

N/A

4. Mode

Physical interface mode

5. Example

Switch_config_g0/1#ethernet cfm mep enable mdnf string mdn x manf string man x mepid 1

6. Related command

N/A

37.4.5 CC Control Command

1. Syntax

ethernet cfm mep *{cci-enable | cci-disable}* **mdnf** *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*>

2. Function

To enable or disable the CCM transmission function of a designated MEP, run the above-mentioned command.

3. Parameter

N/A

4. Mode

Physical interface mode

5. Example

Switch_config_g0/1#ethernet cfm mep cci-disable mdnf string mdn x manf string man x mepid 1

6. Related command

N/A

37.5 CFM Query Commands

37.5.1 Browsing the CFM Protocol Stack

1. Syntax

show ethernet cfm stack

2. Function

To browse the CFM protocol stack, run the above-mentioned command.

3. Parameter

N/A

4. Mode

Non-user mode

5. Example

Switch_config#show ethernet cfm stack

6. Related command

N/A

37.5.2 Browsing the CFM Interface

1. Syntax

show ethernet cfm interface [<*interface_name*>]

2. Function

This command can be used to browse the information about a designated CFM interface.

3. Parameter

N/A

4. Mode

Non-user mode

5. Example

Switch_config#show ethernet cfm interface g0/1

6. Related command

N/A

37.5.3 Browsing the Locally Stored Information About the Remote MEP

1. Syntax

show ethernet cfm rmep mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> [**mepid** <*1-8191*>] [**rmepid** <*1-8191*>] [**view** *{detail* | *brief}*]

2. Function

To browse the detailed or brief information about all remote MEPs, which together with a designated local MEP belong to the same maintenance association, or about a designated remote MEP, run the above-mentioned command.

3. Parameter

Para	Description

meter	
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of the local MEP, which together with the to-be-browsed remote MEP belongs to the same maintenance association.
rmepid	Stands for the MEPID of the to-be-browsed remote MEP.
view	Means to browse the detailed information or the brief information. It is the detailed information that will be browsed by default.

4. Mode

Non-user mode

5. Example

Switch_config#show ethernet cfm rmep mdnf string mdn x manf string man x mepid 1 rmepid 2 view brief

6. Related command

N/A

37.5.4 Browsing the LinkTrace Result Table

1. Syntax

show ethernet cfm linktrace mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*> **tid** <*0-4294967295*>

2. Function

To browse the linktrace result table which is carried out by a specified TID of a specific MEP, run the above-mentioned command.

3. Parameter

Parameter	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is a character string with 1 to 43 printable characters, capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is a character string with 1 to 43 printable characters, capital sensitive.
mepid	Stands for the MEPID of the local MEP, which together with the to-be-browsed remote MEP belongs to the same maintenance association.
tid	Stands for the TID that is returned during linktrace.

4. Mode

Non-user mode

5. Example

Switch_config#show ethernet cfm linktrace mdnf string mdn x manf string man x mepid 1 tid 19830719

```
**** [RESULT FOR READING LINKTRACE REPLY] ****

                ================================================
                                ID :0x12E97BF (19830719)【Event ID of the presently running LT】
                                TTL :0x00000004(4)  【TTL value of the presently running LT】
                            TOTAL LTRs:1【LTRs returned by the remote terminal of the result table】
                              MAX LTRs:100【receiving at most 100 LTRs】
                            NEXT ORDER:2【The next expected LTR order ID】

                                【The total information of one Linktrace is shown above】
                ==================== LTRs ====================

                                order:1【Order ID of this LTR】
                                  TTL:3【TTL vlaue in the responsed LTRs】
                                FwdYes:NO【Whether the local node forwards LTM】
                            TerminalMEP:NO【Whether the local node is the terminal MEP】
                          Last Egress ID:0 - 00:E0:0F:DC:02:11【MAC of the previous hop】
                          Next Egress ID:0 - 00:00:00:00:00:00【MAC of the next hop, and if the result is 0 it
means there is no next hop】
                            Relay Action:(1)HIT【Field of the Relay action: HIT means just hitting successively】
                          Ingress Action:OK(1)【state of the ingress port: OK】
                     Ingress MAC Address:00:E0:0F:81:11:1C【MAC of the ingress port】
                  Ingress Port ID format:MAC-ADDRESS(3)【ID format of the ingress port: MAC format】
                   Ingress Port ID (hex):00 E0 0F 81 11 1C【Identifier of the ingress port：00 E0 0F 81 11 1C】
```

6. Related command

N/A

37.5.5 Browsing the Whole Running Status of CFM

1. Syntax

show ethernet cfm running-info

2. Function

To browse the whole running status of CFM, run the above-mentioned command.

3. Parameter

N/A

4. Mode

All modes except the user mode

5. Example

Switch_config#show ethernet cfm running-info

6. Related command

N/A

37.6 Y1731 Show Commands

37.6.1 Displaying the MEPs That Can Transmit AIS Frames

Syntax

show ethernet y1731 ais-mep

The above-mentioned command is used to show the MEPs that can transmit AIS frames.

Parameter

N/A

Default value

N/A

Remarks

N/A

Example

```
Switch_config#show ethernet y1731 ais-mep
AIS MEP:
MEGID          MEPID   Level   VLAN    Port      MAC              Direction
aaa            2       3       1       Fas0/8    00E0.0F5F.745D   UP
```

37.6.2 Displaying the Information About Continuous MEG Detection

Syntax

show ethernet y1731 detect *MEGID* **[***MEPID* **]**

To display the information about continuous MEG detection, run the above-mentioned command.

Parameter

Parameter	Description
MEGID	Displays the detection information about the designated MEG.
MEPID	It is an optional parameter and the identifier of MEP should be known well.

Default value

N/A

Remarks

When MEPID is not entered, the detection information about all local MEPs of MEG will be shown.

Example

The following example shows the fault detection of MEP 111 of MEG aaa.

```
Switch_config#show ethernet y1731 detect bbb 2
Ethernet Continuity Check:
        (F)Fail,stand for defect exist
        (N)Normal,stand for defect inexistence
LocMEP CC-Status   SFAIL LOC   MIS   UMEP   UMEL   UPER   AIS   RDI   LCK
2      Enabled     N     N     N     N      N      N      N     N     N
```

```
LocMEP   PeerMEP RDI      LOC      MAC
2        1           N        N        00E0.0FD2.FE17
```

37.6.3 Displaying MEP and MIP Configurations on a Port

Syntax

show ethernet y1731 interface *interface-name*

The above-mentioned command is used to display the configurations of MEP and MIP on a port.

Parameter

Parameter	Description
interface-name	Name of the interface, such as f0/1 and fastethernet0/1

Default value

N/A

Remarks

N/A

Example

```
Switch_config#show ethernet y1731 interface g0/4
GigaEthernet0/4:
MEP list:
    MEGID            MEPID    Level    Vlanid   MAC                Direction
    bbb              2        3        1        00E0.0F68.7FBA     DOWN
MIP list:
    Type     Level    MAC
    MIP      4        00E0.0F68.7FBE
Switch_config#
```

37.6.4 Displaying the Configuration of all MEG or the Detailed Configuration of a Certain MEG

Syntax

show ethernet y1731 meglist [*MEGID* **]**

The above-mentioned command is used to display the configuration of all MEG or the detailed configuration about a certain MEG.

Parameter

Parameter	Description
MEGID	Displays the detailed information about the designated MEG.

Default value

N/A

Remarks

If MEGID is not entered, the information about all MEGs will be displayed.

Example

```
Switch_config#show ethernet y1731 meglist
MEG list:
    MEGID              Level    Vlan
    aaa                3        1
    bbb                3        1
    ccc                1        1
Total entries displayed: 3
Switch_config#show ethernet y1731 meglist aaa
MEG ID: aaa          Level: 3   Vlan: 1      CC-Status: Enabled
MEP mep: 1-2
Local MEP list:
    MEPID    Port       MAC                Direction
    2        Fas0/8     00E0.0F5F.745D     UP
```

37.6.5 Displaying the Information About All Configured MIPs

Syntax

show ethernet y1731 miplist

The above-mentioned command is used to display the information about all configured MIPs.

Parameter

N/A

Default value

N/A

Remarks

N/A

Example

```
Switch_config#
Switch_config#show ethernet y1731 miplist
MIP list:
Type      Level     Port        MAC
MIP       7         Fas0/4      00E0.0FC1.003A
MIP       5         Fas0/1      00E0.0FC1.0037
```

37.6.6 Displaying the Statistics Information About the Y1731 Module

Syntax

show ethernet y1731 traffic

The above-mentioned command is used to display some statistics information about the Y.1731 module, including statistics of the received and transmitted OAM packets and the system error.

Parameter

N/A

Default value

N/A

Remarks

N/A

Example

```
Switch_config#
Switch_config#show ethernet y1731 traffic
ethernet y1731 traffic/errors:
        Total output CCM frames: 223933
        Total output LBM frames: 67
        Total output LTM frames: 41
        Total output AIS frames: 0
        Total output 1DM frames: 1067
        Total output DMM frames: 60
        Total input CCM frames: 160778
```

Total input LBM frames: 30
Total input LBR frames: 67
Total input LTM frames: 0
Total input LTR frames: 41
Total input AIS frames: 0
Total input 1DM frames: 0
Total input DMM frames: 0
Total input DMR frames: 60
Total memory allocation failures: 0
Total system failures: 0
Switch_config#

37.7 Y1731 Clear Command

37.7.1 Deleting the Transmission Statistics Information About the OAM Packets and the System Error Information

Syntax

clear ethernet y1731 counters
The above-mentioned command is used to delete the transmission statistics information about the OAM packets and the system error information.

Parameter

N/A

Default value

N/A

Explanation

N/A

Command mode

EXEC

Example

The following example shows how to delete the transmission statistics information about the OAM packets and the system error information.
Switch#clear ethernet y1731 counters

Chapter 38 DHCP-Relay Snooping Configuration Commands

The DHCP-relay snooping configuration commands include:

- ip dhcp-relay snooping
- ip dhcp-relay snooping vlan
- ip dhcp-relay snooping database-agent
- ip dhcp-relay snooping db-file
- ip verify source vlan
- ip arp inspection vlan
- ip source binding
- arp inspection trust
- dhcp snooping trust
- ip-source trust
- show ip dhcp-relay snooping
- show ip dhcp-relay snooping binding
- debug ip dhcp-relay snooping
- debug ip dhcp-relay event
- debug ip dhcp-relay binding

38.1.1 dhcp-relay snooping

Command syntax

ip dhcp-relay snooping

no ip dhcp-relay snooping

To enable or disable the DHCP-relay snooping function in a VLAN, run **ip dhcp-relay snooping**. To resume the corresponding default settings, run **no dhcp-relay snooping**.

Parameter

None

Default value

The dhcp-relay snooping function is disabled by default.

Description

None

Example

The following example shows how to enable the DHCP-relay snooping function:

```
switch(config)# ip dhcp-relay snooping
switch(config)#
```

38.1.2 dhcp-relay snooping vlan

Command syntax

ip dhcp-relay snooping vlan *vlan_id*

no ip dhcp-relay snooping vlan *vlan_id*

Parameter

Parameter	Description
vlan id	ID of a VLAN Range: 1-4094

Default value

None

Description

This command is used to configure the VLAN of DHCP snooping.

Example

The following example shows how to conduct the snooping inspection to the DHCP packets in VLAN2.

```
switch(config)# ip dhcp-relay snooping vlan 2
switch(config)#
```

38.1.3 dhcp-relay snooping database-agent

Command syntax

ip dhcp-relay snooping database-agent *A.B.C.D*

no ip dhcp-relay snooping database-agent

To configure the TFTP server for backing up DHCP-snooping binding, run **ip dhcp-relay snooping database-agent *A.B.C.D***.

Parameter

Parameter	Description
A.B.C.D	Stands for the IP address of the TFTP server.

Default value

There is no standby servers by default.

Description

If the address of the TFTP server is not configured, the binding backup is not conducted.

Example

The following example shows how to set the address of a server of backing up DHCP snooping binding to 192.168.1.1.

```
switch(config)# ip dhcp-relay snooping database-agent 192.168.1.1
switch(config)#
```

38.1.4 dhcp-relay snooping db-file

Command syntax

ip dhcp-relay snooping db-file *name*

no ip dhcp-relay snooping db-file

Parameter

Parameter	Description
Name	File name which is saved during DHCP snooping binding backup.

Default value

There is no file.

Description

If the file name is not configured, the binding backup is not conducted.

Example

The following example shows how to set the file name of binding backup to **dhcp_binding.txt**.

```
switch(config)# ip dhcp-relay snooping db-file dhcp_binding.txt
switch(config)#
```

38.1.5 dhcp-relay snooping write

Command syntax

ip dhcp-relay snooping write-time *num*

no ip dhcp-relay snooping write-time

Parameter

Parameter	Description
Num	Stands for the interval of backing up the DHCP snooping binding.

Default value

The default value of the interval is 30 minutes.

Description

The binding update will be checked during interval configuration. If the binding is updated, the binding information need be backed up.

Example

The following example shows how to set the interval of backing up the binding to 60 minutes.

```
switch(config)# ip dhcp-relay snooping write 60
switch(config)#
```

38.1.6 dhcp-relay snooping information option

Command syntax

ip dhcp-relay snooping information option [format snmp-ifindex]

no ip dhcp-relay snooping information option [format snmp-ifindex]

Parameter

Parameter	Description
format snmp-ifindex	Fills in option 82 in **SNMP ifindex** mode (optional).

Default value

Option 82 will not be added to or removed from the report by default.

Description

This command is used to set whether DHCP option82 can be handled when a switch is conducting DHCP snooping. If **format snmp-ifindex** is designated, Use the **SNMP ifindex** mode to fill in option 82; otherwise, fill in option 82 according to RFC3046.

Example

The following example shows how to fill in option 82 in **SNMP ifindex** mode.

Switch_config#ip dhcp-relay snooping information option format snmp-ifindex

38.1.7 ip verify source vlan

Command syntax

ip verify source vlan *vlanid*

no ip verify source vlan *vlanid*

Parameter

Parameter	Description
vlan id	ID of a VLAN Range: 1-4094

Default value

None

Description

This command is used to configure a VLAN for monitoring the source IP address. The “no” form of this command is used to cancel this VLAN.

Example

The following example shows how to conduct source IP address monitoring to the packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
switch(config)# ip verify source vlan 2
switch(config)#
```

38.1.8 ip arp inspection vlan

Command syntax

ip arp inspection vlan *vlanid*

no ip arp inspection vlan *vlanid*

Parameter

Parameter	Description
vlan id	Queries the time of the timer. Range: 1-255

Default value

None

Description

This command is used to configure a VLAN for monitoring the source address of the ARP packet. The “no” form of this command is used to cancel this VLAN.

Example

The following example shows how to conduct source address monitoring to the ARP packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
switch(config)# ip arp inspection vlan 2
switch(config)#
```

38.1.9 ip source binding

Command syntax

ip source binding *xx-xx-xx-xx-xx-xx A.B.C.D* interface *name*

no ip source binding *xx-xx-xx-xx-xx-xx A.B.C.D*

To add MAC-to-IP binding to an interface, run **ip source binding *xx-xx-xx-xx-xx-xx A.B.C.D* interface *name***.

Parameter

Parameter	Description
xx-xx-xx-xx-xx-xx	MAC address.
A.B.C.D	IP address
Name	Name of the interface

Default value

None

Description

None

Example

The following example shows how to bind MAC address **08-00-3e-00-00-01** to IP address **192.168.1.2** on interface **fastEthernet0/0**.

```
switch(config)# ip source binding   08-00-3e-00-00-01 192.168.1.2 interface fastEthernet0/0
switch(config)#
```

38.1.10 arp inspection trust

Command syntax

arp inspection trust

Parameter

None

Default value

The interfaces are distrusted ones by default.

Description

The ARP monitoring is not conducted to the ARP-trusted interface. The “no” form of this command is used to configure the default value of this interface.

Example

The following example shows how to set interface fastEthernet 0/0 to an ARP-trusted interface.

Switch_config_f0/0# arp inspection trust

38.1.11 dhcp snooping trust

Command syntax

dhcp snooping trust

Parameter

None

Default value

The default interface is a distrusted one.

Description

DHCP snooping is not conducted to the DHCP-trusted interface. The “no” form of this command is used to resume the default value of this interface.

Example

The following example shows how to set interface fastEthernet 0/0 to a DHCP-trusted interface.

Switch_config_f0/0# dhcp snooping trust

38.1.12 dhcp snooping deny

Command syntax

dhcp snooping deny

Parameter

None

Default value

DHCP snooping is allowed on the default interface.

Description

After this command is configured, DHCP snooping trust, IP-sourcetrust and ARP inspection trust are automatically enabled. The “no” form of this command is used to configure the default value of this interface.

Example

The following example shows how to disable DHCP snooping on interface fastEthernet0/0.

```
Switch_config_f0/0# dhcp snooping deny
```

38.1.13 ip-source trust

Command syntax

ip-source trust

Parameter

None

Default value

The default interface is a distrusted one.

Description

Source IP address snooping is not conducted to the source-IP-trusted interface. The “no” form of this command is used to resume the default value of this interface.

Example

The following example shows how to set interface fastEthernet 0/0 to a source-ip-trusted interface.

Switch_config_f0/0# ip-source trust

38.1.14 dhcp-relay agent (L2 switch)

Command syntax

ip dhcp-relay agent

no ip dhcp-relay agent

To enable the forwarding of the DHCP packets on L2 switches, run **ip dhcp-relay agent**. This command is invalid on L3 switches.

Parameter

None

Default value

The **dhcp-relay agent** function is disabled by default.

Description

None

Example

The following example shows how to enable the DHCP-relay agent function:

Switch_config#ip dhcp-relay agent
Switch_config#

38.1.15 dhcp-relay snooping helper-address (L2 switch)

Command syntax

ip dhcp-relay helper-address *address* **vlan** *vlan_id*

no ip dhcp-relay helper-address *address* **vlan** *vlan_id*

Parameter

Parameter	Description
address	Stands for the destination IP address of the DHCP-forwarded packets.
vlan id	Stands for the ID of a VLAN.Value range: 1-4094

Default value

None

Description

This command is used to configure the destination address and VLAN of the DHCP-forwarded packets of L2 switch.

Example

The following example shows how to conduct the snooping inspection to the DHCP packets in VLAN2.

```
Switch_config#ip dhcp-relay helper-address 1.1.1.1    vlan 1
Switch_config#
```

38.1.16 show ip dhcp-relay snooping

Command syntax

show ip dhcp-relay snooping

Parameter

None

Default value

None

Description

This command is used to display the information about DHCP-relay snooping configuration.

Example

The following example shows how to display the information about DHCP-relay snooping configuration.

switch(config)# show ip dhcp-relay snooping

38.1.17 show ip dhcp-relay snooping binding

Command syntax

show ip dhcp-relay snooping binding [all]

Parameter

None

Default value

None

Description

This command is used to display the binding information about DHCP-relay snooping.

If the **all** parameter is in the command sentence, all binding information about DHCP-relay snooping will be displayed.

Example

The following example shows how to display the binding information about DHCP-relay snooping.

switch(config)# show ip dhcp-relay snooping binding

38.1.18 debug ip dhcp-relay snooping

Command syntax

debug ip dhcp-relay snooping

no debug ip dhcp-relay snooping

Parameter

None

Default value

None

Description

This command is used to enable or disable the debugging switch of DHCP-relay snooping.

Example

The following example shows how to enable the debugging switch of DHCP-relay snooping.

switch(config)# debug ip dhcp-relay snooping

switch(config)#

38.1.19 debug ip dhcp-relay event

Command syntax

debug ip dhcp-relay eventr

no debug ip dhcp-relay event

Parameter

None

Default value

None

Description

This command is used to enable or disable the event debugging switch of DHCP-relay.

Example

The following example shows how to enable the event debugging switch of DHCP-relay.

switch(config)# debug ip dhcp-relay event

switch(config)#

38.1.20 debug ip dhcp-relay binding

Command syntax

debug ip dhcp-relay binding

no debug ip dhcp-relay binding

Parameter

None

Default value

None

Description

This command is used to enable or disable the binding debugging switch of DHCP-relay snooping.

Example

The following example shows how to enable the binding debugging switch of DHCP-relay snooping.

```
switch(config)# debug ip dhcp-relay binding
switch(config)#
```

Chapter 39 MACFF Configuration Commands

MACFF configuration commands include:

- macff enable
- macff vlan *vlan_id* enable
- macff vlan *vlan_id* enable default-ar *A.B.C.D*
- macff vlan *vlan_id* enable other_ar *A.B.C.D*
- debug macff

39.1.1 macff enable

Syntax

macff enable

no macff enable

To enable global MACFF, run **macff enable**. To resume the default value, run **no macff enable**.

Parameter

N/A

Default value

The MACFF function is disabled by default.

Remarks

N/A.

Example

The following example shows how to enable the MACFF function.

```
Switch_config#macff enable
Switch_config#
```

39.1.2 macff vlan *vlan_id* enable

Syntax

macff vlan *vlan_id* **enable**

no macff vlan *vlan_id* **enable**

Parameter

Parameter	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default value

N/A

Remarks

This command is used to enable MACFF in VLAN.

Example

The following example shows how to enable MACFF in VLAN2 and set its default gateway address to **192.168.1.1**.

Switch_config#arp 192.168.1.1 00:e0:0f:17:92:ed

Switch_config#macff vlan 2 enable

Switch_config#

39.1.3 macff vlan *vlan_id* default-ar *A.B.C.D*

Syntax

macff vlan *vlan_id* **default-ar** *A.B.C.D*

no macff vlan *vlan_id* **default-ar** *A.B.C.D*

To bind DHCP snooping to standby TFTP server, run **macff vlan *vlan_id* default-ar *A.B.C.D***..

Parameter

Parameter	Description
A.B.C.D	Stands for the IP address of default gateway.

Default value

There is no default gateway settings.

Remarks

This command is used when you set the IP address of the client host and the default gateway manually. Of course, you also need to add the DHCP snooping binding table manually.

Example

The following example shows how to set the address of MACFF binding gateway in vlan1 to **192.168.1.1** and the client's address to **192.168.1.10**.

Switch_config#arp 192.168.1.1 00:e0:0f:17:92:ed

Switch_config#ip source binding 6c-62-6d-59-18-b6 192.168.1.10 interface GigaEthernet0/1

Switch_config# macff vlan 1 default-ar 192.168.1.1

Switch_config#

39.1.4 macff vlan *vlan_id* enable other_ar *A.B.C.D*

Syntax

macff vlan *vlan_id* **other_ar** *A.B.C.D*

no macff vlan *vlan_id* **other_ar** *A.B.C.D*

Parameter

Parameter	Description
A.B.C.D	Stands for the IP address of service AR.

Default value

N/A

Remarks

When the network segment where the client host is has other service ARs and these ARs are only accessed by the client directly without the need of gateway to forwarding packets, this command can be used to add these service ARs.

Example

The following example shows how to set an AR with its IP being 192.168.2.254 and its MAC being 00:e0:0f:23:02:fc on port g0/1 in vlan1.

```
Switch_config#arp 192.168.2.254 00:e0:0f:23:02:fc
Switch_config#interface g0/1
Switch_config_g0/1# dhcp snooping trust
Switch_config_g0/1#exit
Switch_config#macff vlan vlan_id enable other_ar A.B.C.D
```

39.1.5 macff disable

Syntax

macff disable

no macff disable

Parameter

N/A

Default value

A specified port is allowed to enable MACFF.

Remarks

Though MACFF is enabled in a VLAN, MACFF can be disabled on one of the ports in this VLAN. The DHCP snooping functionality is not affected on this port after disabled its MACFF functionality.

Example

The following example shows how to disable MACFF on port g0/1.

```
Switch_config_g0/1#macff disable
Switch_config_g0/1#
```

39.1.6 debug macff

Syntax

debug macff

no debug macff

Parameter

N/A

Default value

N/A

Remarks

This command is used to enable or disable the MACFF debugging switch.

Example

The following example shows how to enable the debugging switch of MACFF.

```
Switch_config#debug macff
Switch_config#
```

Chapter 40 IEEE1588 Transparent Clock Configuration Commands

IEEE1588 Transparent Clock Configuration Commands

IEEE1588 transparent clock configuration commands include:

ptp enable (global)

ptp enable (port)

ptp start

ptp delay-mechanism

ptp sync-mechanism

ptp domain

ptp domain-filter

ptp e2e-record-timeout

debug ptp

show ptpt

ptp enable (global)

Syntax

ptp enable

no ptp enable

Parameter

N/A

Default value

N/A

Explanation

This command is used to enable or disable the IEEE1588 transparent clock. The transparent clock is shortened as TC and it can be classified into E2E TC and P2P TC according to the link delay measurement mode. TC can adjust the time introduced by synchronous packets via intermediate device to realize the exquisite synchronization between active and standby clocks.

Command mode

Global configuration mode

Example

The following example shows how to enable the IEEE1588 TC.

```
Switch_config# ptp enable
Switch_config#
```

ptp enable (port)

Syntax

ptp enable

no ptp enable

Parameter

N/A

Default value

N/A

Explanation

This command is used to enable or disable PTP on a L3 port.

Command mode

Port configuration mode

Example

The following example shows how to enable the IEEE1588 TC on interface vlan1.

```
Switch_config# interface vlan 1
Switch_config_v1#ptp enable
Switch_config_v1#
```

ptp start

Syntax

ptp start {**l2**|**l3**}

no ptp start

Parameter

Parameter	Description
L2	Creates a L2 PTP port to run in an Ethernet.
L3	Creates a L3 PTP port to run in IP or UDP.

Default value

N/A

Explanation

Before PTP communication, several PTP ports should be created on TC and connected to the active and standby TCs respectively. You can run **ptp start** to create or delete the PTP ports in port configuration mode. All the ports of a switch support PTP.

After **no ptp enable** is globally configured, all created PTP ports will be deleted automatically.

After you create L2 PTP ports via the **ptp start l2** command, these ports receive and transmit Ethernet-based PTP packets. After you create L3 PTP ports via the **ptp start l3** command, these ports receive and transmit IP/UDP-based PTP packets. You can switch over to **ptp start l2** from **ptp start l3** directly without extra deletion actions.

If you run the **no ptp start** command to delete PTP ports, no extra parameters need to be added to this command.

Command mode

Port configuration mode

Example

The following example shows how to create a L2 PTP port on port G0/24.

```
Switch_config_g0/24# ptp start l2
Switch_config_g0/24#
```

The following example shows how to modify a L2 PTP port to be a L3 PTP port on port G0/24.

```
Switch_config_g0/24# ptp start l3
Switch_config_g0/24#
```

The following example shows how to delete the PTP port on port G0/24.

```
Switch_config_g0/24# no ptp start
Switch_config_g0/24#
```

ptp delay-mechanism

Syntax

ptp delay-mechanism {**e2e**|**p2p**}

Parameter

Parameter	Description
e2e	Sets to the E2E TC mode.
p2p	Sets to the P2P TC mode.

Default value

p2p

Explanation

The IEEE1588 TC can be switched over between two working modes: the E2E mode and the P2P mode. The P2P mode is the default one. In E2E mode, TC can process the **Delay_Req** packets and the **Delay_Resp** packets; In P2P mode, the path-delay mechanism is running on each PTP port, the Pdelay_Req packets are transmitted periodically, and the **Pdelay_Resp** packets and the **Pdelay_Resp_Folllow_Up** packets are responded to. The two modes are incompatible with each other. For example, if it is in P2P mode, the **Delay_Req** packets received from the clock will be dropped.

Command mode

Global configuration mode

Example

The following example shows how to set TC to the P2P mode.

```
Switch_config# ptp delay-mechanism p2p
Switch_config#
```

The following example shows how to set TC to the E2E mode.

```
Switch_config# ptp delay-mechanism e2e
Switch_config#
```

ptp sync-mechanism

Syntax

ptp sync-mechanism { straight-forward | store-forward}

Parameter

Parameter	Description
straight-forward	Sets the proceeding method of **Sync/Follow_Up** packets to **direct forwarding**.
store-forward	Sets the proceeding method of **Sync/Follow_Up** packets to **store-forward**.

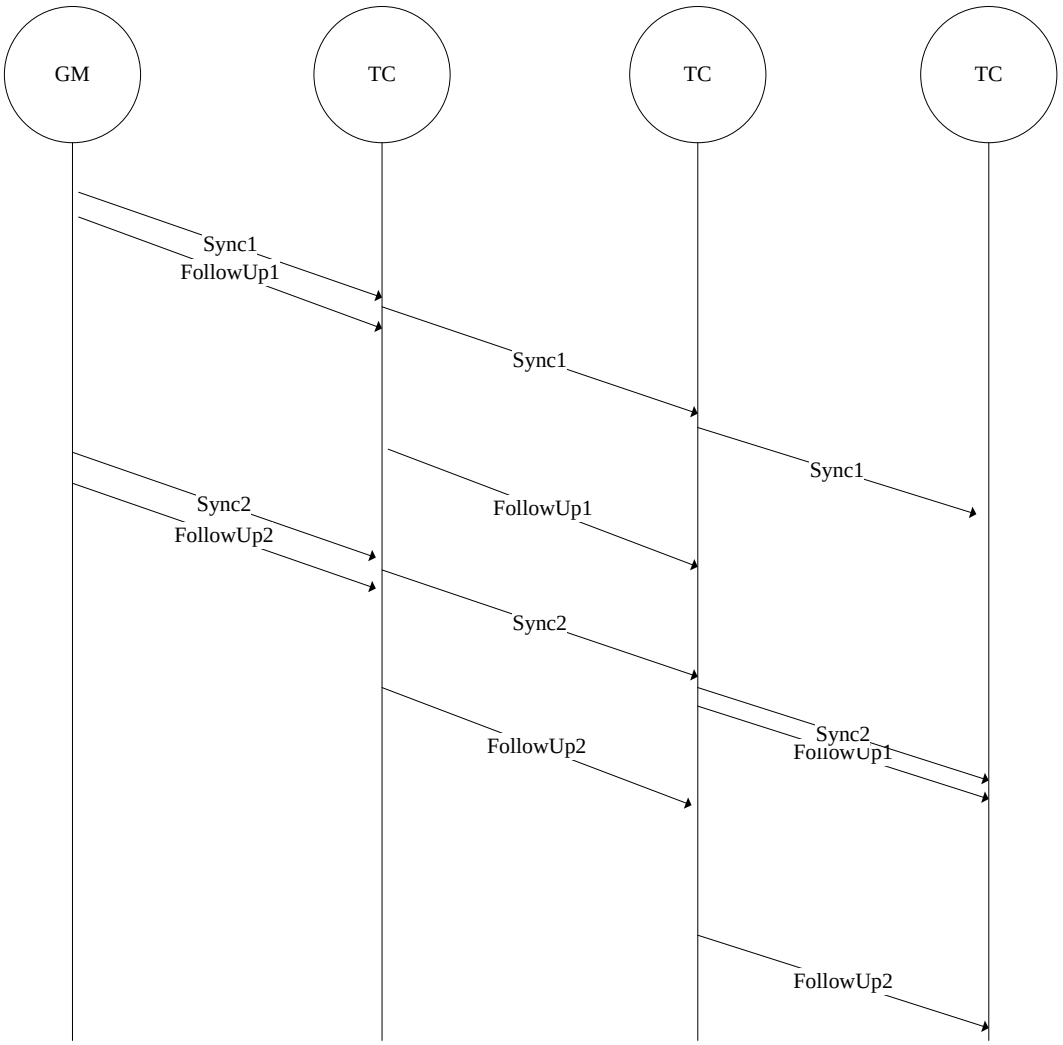
Default value

straight-forward

Explanation

This command is mainly used to set the forwarding mode of Sync/Follow_Up packets to **straight forward** or **store-forward**. The default forwarding mode is straight forwarding, that is, the PTP port immediately forwards after receiving Sync packets, re-encapsulates the Follow_UP packets after receiving them and then forwards them out.

This mode may lead to disorder in multileveled TC cascading, as shown in the following figure:



In straight-forward mode, the time to process the Sync packets is obviously less than that to process the Follow_Up packets. If this process goes through multileveled TC cascading, the clock may have already received Sync2 before Follow_up1. This may lead to the malfunction of the clock.

Hence, we specially design the store-forward mode for our customers in which the PTP port does not forward a received Sync packet until the corresponding Follow_Up packet is received so that the problem of disorder will not arise.

Command mode

Global configuration mode

Example

The following example shows how to set TC to the straight-forward mode.

```
Switch_config#ptp sync-mechanism straight-forward
Switch_config#
```

The following example shows how to set TC to the store-forward mode.

Switch_config#ptp sync-mechanism store-forward
Switch_config#

ptp domain

Syntax

ptp domain *number*

no ptp domain

Parameter

Parameter	Description
number	Stands for the PTP domain ID, which ranges from 0 to 3.

Default value

0

Explanation

This command is used to set the domain to which the PTP port belongs and the default domain of this port is domain0. In IEEE1588 are there four domains defined: domain0, domain1, domain2 and domain3.

Command mode

Port configuration mode

Example

The following example shows how to set the PTP port on interface g0/24 to run in domain1.

Switch_config_g0/24# ptp domain 1
Switch_config_g0/24#

ptp domain-filter

Syntax

ptp domain-filter

no ptp domain-filter

Parameter

N/A

Default value

The PTP domain filter is enabled by default.

Explanation

This command is used to set the domain filtration function, which is enabled by default. You can conduct area management toward PTP equipment through domain segment. PTP equipment in different sub-domains cannot perform time synchronization. After the domain filtration function is enabled, the PTP packets in other domains are dropped; if domain filtration is disabled, TC will not conduct the domain checkup.

Command mode

Global configuration mode

Example

The following example shows how to enable domain filtration:

```
Switch_config#ptp domain-filter
Switch_config#
```

The following example shows how to disable domain filtration:

```
Switch_config#no ptp domain-filter
Switch_config#
```

ptp pdelay-interval

Syntax

ptp pdelay-interval *time*

no ptp pdelay-interval

Parameter

Parameter	Description
time	Stands for the transmission interval of Pdelay_Req packets.

Default value

0 (that is, 1 second)

Explanation

This command is used to set the transmission interval of Pdelay_Req packets. The transmission interval ranges from -4 to 4, and its actual interval is the *n* powers of 2 seconds. For example, it is set to 0, the actual transmission interval is the *0* power of 2 seconds, that is, 1 second.

Command mode

Global configuration mode

Example

The following example shows how to configure the transmission interval of Pdelay_Req packets to 2 seconds.

```
Switch_config#ptp delay-interval 1
Switch_config#
```

ptp e2e-record-timeout

Syntax

ptp e2e-record-timeout *time*

no ptp e2e-record-timeout

Parameter

Parameter	Description
time	Stands for the timeout time of recording Delay_Req packets, which ranges from 0 to 10.

Default value

5 (32s)

Explanation

This command is used to set the timeout time recorded by Delay_Req packets, which ensures that the Delay_Req record can be released even if Delay_Resp message is missing.

Command mode

Global configuration mode

Example

The following example shows how to set the timeout time recorded by Delay_Req packets to 1024 seconds.

Switch_config# ptp e2e-record-timeout *10*

Switch_config#

debug p2p

Syntax

debug ptp {errors|rx-packet|tx-packet |sync|e2e|p2p}

Parameter

Parameter	Description
errors	Browses the PTP error logs.
rx-packet	Browses the received PTP packets.
tx-packet	Browses the transmitted PTP packets.
sync	Browses how TC processes Sync packets.
e2e	Browses how TC processes Delay_Req packets.
p2p	Browses Path_Delay calculation on a PTP port.

Default value

N/A

Explanation

This command is used to export the debugging information generated during the running of TC for you to have an idea of how PTP is going on and incorrect positioning.

show ptp

Syntax

show ptp [interface *intf-id*]

To display the 802.1x configuration information, run the previous command.

Parameter

Parameter	Description
intf-id	Stands for a specific physical interface.

Default value

N/A

Explanation

This command is used to display the configuration information on the IEEE1588 TC.

Command mode

EXEC

Example

```
Switch#show ptp

   IEEE1588 Transparent Clock Default Data Set

clock identity ..... 00-E0-0F-FF-FE-DB-0B-54
number of ports ..... 300
delay mechianism..... E2E
primary domain ..... 0
Pdelay_Req interval... 0

   Domain Control

domain filter          ON
domain number          sync mode          master port
      0                straight_forward   G0/20
      1                straight_forward   (null)
      2                straight_forward   (null)
      3                straight_forward   (null)
```

```
delay-req record timeout 32(s)

  IEEE 1588 on port G0/18 enabled

        Port Data Set
      clock identity ..... 00-E0-0F-FF-FE-DB-0B-66
      port number ..... 1
      log pdelay interval ... 0
      current path delay .... 000000000.000000000
      domain number ..... 0

  Request_Respond Mechanism (E2E) on port G0/18 is ON
    current sequece id 59983

  IEEE 1588 on port G0/20 enabled

        Port Data Set
      clock identity ..... 00-E0-0F-FF-FE-DB-0B-68
      port number ..... 2
      log pdelay interval ... 0
      current path delay .... 000000000.000000000
      domain number ..... 0

  Request_Respond Mechanism (E2E) on port G0/20 is ON
    current sequece id 0

Switch#
```

Chapter 41 Layer 2 Protocol Tunneling Configuration Commands

41.1 Layer 2 Protocol Tunneling Configuration Commands

Layer 2 protocol tunneling configuration commands include：

- l2protocol-tunnel

41.1.1 Layer-2 protocol-tunnel

Description

To configure layer 2 protocol tunneling, use the **l2protocol-tunnel command.**

[no] l2protocol-tunnel [stp]

Parameter

None

Default

Disabled

If you do not specify a protocol, all protocols are tunneled.

Instruction

Currently we only support STP.

Example

This example shows how to enable the stp protocol (including STP/PVST) tunneling feature on interface f0/2:

Switch_config#int f0/2
Switch_config_f0/2#l2protocol-tunnel stp

41.2 Layer 2 Protocol Tunneling Monitor Commands

The layer-2 protocol tunneling monitor command is debug layer-2 protocol tunnel.

41.2.1 debug layer-2 protocol-tunnel

Description

To configure the debugging option of layer 2 protocol tunneling, use the **debug l2protocol-tunnel** command.

[no] debug l2protocol-tunnel [error | packet]

Parameter

None

Default

If you do not specify a debugging optionl, all debugging options are enabled.

Instruction

None

Example

This example shows how to enable the stp protocol (including STP/PVST) tunneling feature on the interface f0/2:

```
Switch_config#int f0/2
Switch_config_f0/2#l2protocol-tunnel stp
```

Chapter 42 Loopback Detection Configuration Commands

42.1 Loopback Detection Configuration Commands

Loopback detection configuration commands include:

- loopback-detection
- loopback-detection enable
- loopback-detection vlan-control
- loopback-detection hello-time
- loopback-detection recovery-time
- loopback-detection control
- loopback-detection dest-mac
- loopback-detection existence
- show loopback-detection
- show loopback-detection interface

42.1.1 loopback-detection

[no] loopback-detection

To enable or disable global loopback detection, run the above-mentioned command.

Parameter

N/A

Default value

Loopback detection is globally disabled by default.

Command mode

Global configuration mode

Explanation

N/A

Example

Switch#config
Switch_config#
Switch_config#loopback-detection

42.1.2 loopback-detection enable

[**no**] **loopback-detection enable**

To enable or disable loopback detection on a port, run the above-mentioned command.

Parameter

N/A

Default value

Loopback detection is disabled on a port by default.

Command mode

Port configuration mode

Explanation

You can run this command to enable or disable loopback detection on a specified port. However, this settings takes effect only after loopback detection is enabled globally.

Example

Switch_config#
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection enable

42.1.3 loopback-detection vlan-control

[**no**] **loopback-detection vlan-control** *vlan-list*

To set a port to perform loopback detection toward a specified VLAN, run the above-mentioned command.

Parameter

Parameter	Description
vlan-list	Stands for a VLAN specified by a port. It ranges from 1 to 4094, and up to 10 VLANs can be specified.

Default value

N/A

Command mode

Port configuration mode

Explanation

After loopback detection is configured on a specified VLAN, the port transmits multiple detection packets of specified VLAN tag regularly and the number of these detection packets transmitted by this port can be up to 10.

Example

```
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection vlan-control 1-5
```

42.1.4 loopback-detection hello-time

[**no**] **loopback-detection hello-time** *hello-time*

To set the transmission period of loopback detection packets, run the above-mentioned command.

Parameter

Parameter	Description
hello-time	Stands for the transmission period of loopback packets, whose unit is second.

Default value

3 seconds

Command mode

Port configuration mode

Explanation

N/A

Example

N/A

42.1.5 loopback-detection recovery-time

[**no**] **loopback-detection recovery-time** *recovery-time*

To set the recovery time of a port after being controlled, run the above-mentioned command.

Parameter

Parameter	Description
recovery-time	Stands for the recovery time of a port after being controlled, whose unit is second.

Default value

10 seconds

Command mode

Port configuration mode

Explanation

N/A

Example

N/A

42.1.6 loopback-detection control

[no] loopback-detection control { block|learning|shutdown}

To set a port to be controlled, run the above-mentioned command.

Parameter

Parameter	Description
block	Sets a port to be blocked.
learning	Sets a port to be learning.
shutdown	Sets a port to be shutdown.

Default value

N/A

Command mode

Port configuration mode

Explanation

When a port detects loopback exists in its network, you can perform corresponding control actions to this port by setting control functions. The controlled states of a port include **block**, **nolearn**, **shutdown** and **trap**. When a controlled state is configured and loopback exists on a port, the trap message be transmitted. It is not configured by default.

After loopback detection is enabled globally, the port on which loopback detection is enabled transmits the loopback detection packets and receives the already transmitted loopback detection packets. Four control actions are conducted on the port:

block : This means to block the port. When loopback is found, this port will be isolated from other ports and the packets going into this port cannot be forwarded to other ports. This port is then in **protocol down** state and its MAC address table ages.

nolearn: This means forbidding this port to learn MAC addresses.Upon the discovery of loopback on a port, this port will not learn MAC addresses and at the same time age its MAC address table.

shutdown: It means to shut down the port. At the discovery of loopback, this port will not only transmit the trap message and age its MAC address but also shut down this port automatically to stop packet reception and transmission until the err-disable-recover time comes.

trap: It means that the port only reports alarms. When loopback is discovered, the port will only report alarms and age its MAC address table.

When a port is blocked, the packets entering into this port cannot be forwarded by this port and this port will go on transmitting loopback detection packets at the same time; when

loopback disappears, the port will recover itself automatically. Loopback disappearance takes place if the port has not received loopback detection packets within 10 seconds.

In block state the port protocol is down, while in shutdown state the port's link is down directly.

Example

```
Switch#config
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection control block
```

42.1.7 loopback-detection dest-mac

[**no**] **loopback-detection dest-mac** *mac-addr*

To set the destination MAC address of loopback detection packets on a port, run the above-mentioned command.

Parameter

Parameter	Description
mac-addr	Stands for the destination MAC address of loopback detection packets.

Default value

The default destination MAC address is **01-80-C2-00-00-0a**.

Command mode

Port configuration mode

Explanation

N/A

Example

```
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection dest-mac 1111.1111.1111
```

42.1.8 loopback-detection existence

[no] loopback-detection existence

To set a standard to judge whether loopback exists on a port when this port is enabled or its link state is UP, run the above-mentioned command.

Parameter

N/A

Default value

Loopback is nonexistent by default.

Command mode

Port configuration mode

Explanation

This command is mainly used to solve the problem that loopback exists on a port or not when this port is up and its loopback detection function takes effect. When the controlled action of this port is set to **shutdown**, it is improper to regard that loopback exists on this port for a shutdown port has already not forwarded packets.

Example

N/A

42.1.9 show loopback-detection

show loopback-detection

To display the configuration details of loopback detection, run the above-mentioned command.

Parameter

N/A

Default value

N/A

Command mode

EXEC, global or interface configuration modes

Explanation

This command is used to display the global or port's loopback detection configurations and port status.

Example

```
Switch#show loopback-detection
Loopback-detection is enable

Interface state information
Port        Status   dest MacAddress Control   VLAN
------------ --------- ---------------------- ----------  ------------------------------
    G0/1       UP   1234.5678.9abc BLOCK     1-5
    G0/2       UP   0180.c200.000a WARNING
    G0/3       UP   0180.c200.000a BLOCK
    G0/4       UP   0180.c200.000a WARNING
    G0/5       UP   0180.c200.000a WARNING
    G0/6       UP   0180.c200.000a WARNING 1-8
    G0/7       UP   0180.c200.000a WARNING
    G0/8       UP   0180.c200.000a WARNING
    G0/9       UP   0180.c200.000a WARNING
   G0/10       UP   0180.c200.000a WARNING
   G0/11       UP   0180.c200.000a WARNING
   G0/12       UP   0180.c200.000a WARNING
   G0/13       UP   0180.c200.000a WARNING
```

```
G0/14       UP   0180.c200.000a WARNING
G0/15       UP   0180.c200.000a WARNING
G0/16       UP   0180.c200.000a WARNING
```

42.1.10 show loopback-detection

show loopback-detection *intf-id*

To display the information about the loopback detection port, run the above-mentioned command.

Parameter

Parameter	Description
Interface *Intf-id*	Displays the designated port.

Default value

N/A

Command mode

EXEC, global or interface configuration modes

Explanation

This command is mainly used to display the status of the loopback detection port.

Example

```
Switch#show loopback-detection interface g0/1
Receive Packets :0
Transmit Packets: 20
Discard Packets:0
HelloTimeOut:10
RecoverTimeOut:26
```

Chapter 43 QoS Service Configuration Commands

43.1 QoS Configuration Commands

- QoS Configuration Commands include:
- cos default
- cos map
- scheduler wrr bandwidth
- scheduler policy
- policy-map
- classify
- action
- qos policy

43.1.1 cos default

Description

cos default *cos*

no cos default

To configure the default value of CoS, use the **cos default** command. To disable the configuration, use the negative form of this command.

Parameter

Parameter	Description
cos	Default cos value. The range is 0-7

Default

0

Instruction

Layer 2 interface configuration mode

Example

Set the CoS value of the no-label frame received from ge0/1 interface to **4**.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# cos default 4
```

43.1.2 cos map

Description

cos map *quid cos1..cosn*

no cos map

To set the CoS priority queues, use the **cos map** command.

Parameter

Parameter	Description
quid	ID of CoS priority queues. The range is 1 to 8
cos1..cosn	CoS value defined by IEEE802.1p. The range is 0 to 7

Default

CoS value	Priority Queue
0, 1	1
2, 3	2
4, 5	3
6,7	4

Instruction

Layer 2 interface configuration mode

Using this command in the global configuration mode will affect all CoS priority queue; while configuring this command in layer 2 interface command will only affect CoS priority queue of the interface.

Example

The following example maps CoS 0-2 to CoS priority queue 1and maps CoS 3 to priority queue 2:

```
Switch(config-if)# cos map 1 0 1 2
Switch(config-if)# cos map 2 3
```

43.1.3 scheduler wrr bandwidth

Description

scheduler wrr bandwidth *weight1...weightn*

no scheduler wrr bandwidth

To configure the bandwidth of the cos priotiry queue, use the **scheduler wrr bandwidth** command.

Parameter

Parameter	Description
weight1…weight8	WRR 8 CoS priority queue metrics the range is 1to 5。

Default

All CoS priority queue metrics must be the same, the eight CoS priority queue metrics are all 12.

Instruction

It works in port configuration mode.

The command validates only when the queue schedule mode of a port is set to **wrr**. It defines the broadband metrics of the CoS priority queue for the **wrr** schedule strategy.

Example

Configure the eight CoS priority queue metrics as 1，2，3，4，5，6，7，8

Switch(config)# scheduler wrr bandwidth 1 , 2 , 3 , 4 , 5 , 6 , 7 , 8

43.1.4 scheduler policy

Description

scheduler policy { **sp** | **wrr** }

no scheduler policy

To set CoS priority queue debug policy, use the **scheduler policy** command.

Parameter

Parameter	Description
sp	Use the **sp** scheduler strategy.
wrr	Use the **wrr** scheduler strategy

Default

use SP

Instruction

Global configuration mode

After configure the command, the interface send debug mode is configured to specified value.

Example

Configure interface send debug mode as wrr.

Switch(config)#scheduler policy wrr

Chapter 44 DoS Attack Prevention Configuration Commands

44.1 DoS-Attack Prevention Configuration Commands

DoS attack prevention configuration commands are shown below:

- dos enable
- show dos

44.1.1 dos enable

Syntax

dos enable {all | icmp *icmp-value* **| ip | ipv4firstfrag | l4port | mac | tcpflags | tcpfrag** *tcpfrag-value***}**

no dos enable {**all | icmp | ip | ipv4firstfrag | l4port | mac | tcpflags | tcpfrag**}

Parameter

Parameter	Description
all	Enables to prevent all kinds of DoS attacks.
icmp *icmp-value*	Prevents the ICMP DoS attacks. Here, the **icmp-value** parameter means the maximum length of ICMP packet, whose default value is 512.
ip	Prevents those DoS attack packets whose source IP addresses are equal to the destination IP addresses.
ipv4firstfrag	Starts to check the first fragment of IP packet.
l4port	Starts to check the L4 packets whose source port is equal to the destination port.
mac	Starts to check those packets whose source MACs are equal to destination MACs.
tcpflags	Starts to check the TCP packets with illegal flags.
tcpfrag *tcpfrag-value*	Starts to check the DoS attack packet of TCP fragment. Here, the ***tcpfrag-value*** parameter means the minimum TCP header, whose default value is 20.

Default value

DoS attack prevention is disabled by default.

Remarks

DoS attack prevention is configured in global mode.

The DoS IP sub-function can drop those IP packets whose source IPs are equal to the destination IPs.

The DoS ICMP sub-function can drop the following two kinds of packets: 1. ICMPv4/v6 ping packets whose size is larger than icmp-value; 2. ICMP packets.

The DoS l4port sun-function can drop those TCP/UDP packets whose source port is equal to the destination port.

The DoS MAC sub-function can drop those packets whose source MACs are equal to destination MACs.

The DoS tcpflags sub-function can drop the following 4 kinds of TCP packets: 1. TCP SYN flag=1 & source port<1024; 2.TCP control flags = 0 & sequence = 0; 3.TCP FIN URG PSH =1 & sequence = 0; 4.TCP FIN SYN =1.

The DoS tcpfrag sub-function can drop the following two kinds of TCP packets: 1. The TCP header is smaller than the first TCP fragment of **tcpfrag-value**; 2. TCP fragments whose offset values are 1.

Example

The following example shows how to set the global DoS attack prevention function to prevent those IP packets whose source IPs are destination IP addresses.

Switch_config#dos enable ip

The following example shows how to set DoS attack prevention in global mode to prevent those packets whose maximum ICMP length is bigger than 255.

Switch_config#dos enable icmp 255

44.1.2 show dos

Syntax

show dos

It is used to show all DoS attack prevention functions that users have set.

Parameter

N/A

Default value

N/A

Remarks

EXEC mode

Example

The following example shows how to display all DoS attack prevention functions.

```
Switch_config#dos enable all
Switch_config#show dos
dos enable ip
dos enable ipv4firstfrag
dos enable tcpflags
dos enable l4port
dos enable mac
dos enable tcpfrag
```

```
dos enable icmp
Switch_config#
```

The following example shows how to set **dos enable icmp** to display the sub-function that users have set.

```
Switch_config#dos enable icmp
Switch_config#show dos
dos enable icmp
```

The following example shows how to set **dos enable icmp 255** to display the sub-function that users have set.

```
Switch_config#dos enable icmp 255
Switch_config#show dos
dos enable icmp 255
```

Chapter 45 Anti-Attack Configuration Commands

45.1 Anti-Attack Configuration Commands

45.1.1 filter period *time*

To configure filter period for attack, use the filter period command.

parameter

parameter	Description
time	The filter period for attack in seconds. It is considered as attack when the attack source sends packets above the specified number in any filter period time.

default

10 seconds

Command mode

Global configuration mode

example

Switch_config#filter period 15

Related commands

filter threshold value

45.1.2 filter threshold *value*

To configure the filter threshold value, use the filter thresholf value command.

parameter

parameter	Description
value	It is considered as attack when the receiving packets excddes the filter threshold value.

default

1000

command mode

global configuration mode

example

Switch_config#filter threshold 1500

Related commands

filter period time

45.1.3 filter block-time *value*

To configure the time to block attack resource, use the filter block-time value command.

parameter

parameter	description
Value	Time to block attack source in seconds.

default

300 seconds

command mode

global configuration mode

example

Switch_config#filter block-time 600

Related commands

filter period time

filter threshold value

45.1.4 filter igmp

To filter IGMP attack, use the filter igmp command.

parameter

none

Command mode

Global configuration mode

example

Switch_config#filter igmp

Related commands

filter enable

45.1.5 filter arp

To fliter ARP attack, use the filter arp command.

parameter

none

Command mode

physical interface configuration mode

example

Switch_config_f0/1#filter arp

Related commands

filter enable

45.1.6 filter enable

To enable filter feature, use the filter enable command.

parameter

none

Command mode

Global configuration mode

example

Switch_config#filter enable

Related commands

filter igmp

filter arp

45.1.7 show filter

To display working state of the anti-attack feature of the current switch, use the show filter command.

parameter

none

command mode

non-user mode

```
Switch#show fil
Filter threshold: 1000 packet in any 10 seconds
Filters blocked:
Address            seconds      source interface
00a0.0c13.647d      27.0        FastEthernet1/2

Filters counting:
Address            seconds      count   source interface
00a0.0c43.647d       1.84       371     FastEthernet1/2
```

Filters blocked: indicates MAC address of the blocked attack source, blocked time and source interface.

Filters counting: indicates MAC address of the attack source, counting time, the number of the receiving packets and the source interface.

Chapter 46 IP Addressing Configuration Commands

46.1 IP Addressing Configuration Commands

IP addressing configuration commands include:

- arp
- arp scan
- arp timeout
- clear arp-cache
- ip address
- ip directed-broadcast
- ip forward-protocol udp
- ip helper-address
- ip host name
- ip proxy-arp
- ip unnumbered
- keepalive
- show arp
- show hosts
- show ip interface

46.1.1 arp

To configure the static ARP which will permanently be stored in the ARP cache, run **arp [vrf *vrf-name*] *ip-address hardware-address* [alias]**. To delete the configured static ARP, run **no arp [vrf *vrf-name*] *ip-address***.

arp [**vrf** *vrf-name*] *ip-address hardware-address* [**alias**]

no arp [**vrf** *vrf-name*] *ip-address*

Parameter

Parameter	Description
Vrf-name	VRF name (for the VRF version)
ip-address	IP address of the local link interface
hardware-address	Physical address of the local link interface
alias	(optional) the router will answer the ARP request from the IP address.

Default

No permanent static ARP mapping exists in the ARP cache.

Command Mode

Global configuration mode

Usage Description

A common host can support the dynamic ARP resolution; hence, you need not specially configure the static ARP mapping for the host. The **vrf** subcommand is used to specify which VRF the ARP item belongs to.

Example

The following command shows that the MAC address of the host with IP address 1.1.1.1 is set to 00:12:34:56:78:90.

```
arp 1.1.1.1 00:12:34:56:78:90
```

Related command

clear arp-cache

46.1.2 arp timeout

To configure the timeout value of the dynamic ARP item in the ARP cache, run **arp timeout seconds**. To resume the default value of the ARP item, run **no arp timeout** or **default arp timeout**.

arp timeout seconds

no arp timeout

default arp timeout

Parameter

Parameter	Description
seconds	Timeout value of the dynamic ARP item in the ARP cache, which means that the ARP cache obtained through dynamic resolution on the port will not be released at the timeout time

Default

180 seconds (3 minutes)

Command Mode

Interface configuration mode

Usage Description

If the timeout value of the dynamic ARP item is configured on the non-arp interface, the configuration is invalid. You can run show interface to display the timeout time of the ARP items on the port. See the following information :

ARP type: ARPA, ARP timeout 00:03:00

Example

The following example shows that the timeout time of the dynamic ARP mapping on interface Ethernet 1/0 is set to 900 seconds, which enables the ARP cache to be refreshed rapidly.

```
!
interface ethernet 1/0
arp timeout 900
!
```

Related command

show interface

46.1.3 clear arp-cache

To delete all dynamic ARP cache, run the following command:

clear arp-cache

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

The following command is used to delete all dynamic ARP cache.

clear arp-cache

Related command

arp

46.1.4 ip address

To configure the IP address of the interface and the network mask simultaneously, run **ip address**. Currently, the IP addresses can not be clearly classified into A type, B type and C type. However, the multicast address and the broadcast address can not be used. Except the Ethernet, multiple interfaces of other types of network can work on the same network segment. The network segment configured by the Ethernet interface cannot be same to that configured by other types of interfaces, unnumbered interfaces excluded. One main address and multiple accessory addresses can be configured on an interface. The accessory address can be configured only after the main address is configured, while the main address can be deleted only after all accessory addresses are deleted. If the upper-layer application does not specify the source address of the system-generated IP packet, the router will adopt the IP address (configured on the transmitter interface and is in the same network segment as the gateway); if the IP address cannot be determined, the main address of the transmitter interface will be adopted. If the IP address of an interface is not configured and the interface is not an unnumbered interface, the IP packets will not be handled on the interface.

To delete an IP address or stop the IP packets from being handled on an interface, run **no ip address**.

ip address *ip-address mask* [**secondary**]

no ip address *ip-address* **mask**

no ip address

Parameter

Parameter	Description
ip-address	IP address
mask	Mask of the IP network
secondary	(optional) specifies an accessory IP address. If the IP address is not specified, it must be a main IP address.

Default

No IP addresses is configured on the interface.

Command Mode

Interface configuration mode

Usage Description

If you configure the accessory IP address on a physical network segment through the router, you must configure the accessory IP address of the same logical network segment for other systems on the same physical network segment; otherwise, the routing loop will be easily generated.

When the OSPF protocol is used, make sure that the accessory address and the main address of an interface must be in the same OSPF area.

Example

The following example shows that the main address on interface Ethernet1/0 is set to 202.0.0.1, network mask is set to 255.255.255.0 and two accessory IP addresses are set to 203.0.0.1 and 204.0.0.1 respectively.

```
interface ethernet1/0
ip address 202.0.0.1 255.255.255.0
ip address 203.0.0.1 255.255.255.0 secondary
ip address 204.0.0.1 255.255.255.0 secondary
```

46.1.5 ip directed-broadcast

To forward the directed IP broadcast and transmit the packets in the physical broadcast form, run **IP directed-broadcast [access-list-namer]**.

ip directed-broadcast [*access-list-namer*]

no ip directed-broadcast

Parameter

Parameter	Description
access-list-name	Name of the access list, which is an optional parameterIf the access list is defined, only broadcast packets permitted by the access list can be forwarded.

Default

The directed IP broadcast will not be forwarded by default.

Command Mode

Interface configuration mode

Example

The following example shows how to configure the directed IP broadcast forwarding on interface Ethernet1/0.

```
!
interface ethernet 1/0
ip directed-broadcast
!
```

46.1.6 ip forward-protocol udp

To specify which UDP packets to be forwarded after IP helper-address is configured on the interface, run **ip forward-protocol udp [*port*]**.

ip forward-protocol udp [*port*]

no ip forward-protocol udp [*port*]

default ip forward-protocol udp

Parameter

Parameter	Description
ISDN(BRI)	(optional) destination port which the to-be-forwarded UDP packets is transmitted to

Default

The NETBIOS Name Service packet is forwarded.

Command Mode

Global configuration mode

Usage Description

The NETBIOS Name Service packet is forwarded by default; to stop forwarding the NETBIOS Name Service packet, run either of the following two commands:

no ip forward-protocol udp netbios-ns

no ip forward-protocol udp 137

To stop forwarding all UDP packets, run the following command:

no ip forward-protocol udp

Example

Router_config#ip forward-protocol udp 137

Related command

ip helper-address

46.1.7 ip helper-address

To forward the directed IP packets to the designated IP helper address (unicast address or broadcast address), run **ip helper-address**. You can configure multiple helper addresses on each interface.**ip helper-address** *address*

no ip helper-address [*address*]

Parameter

Parameter	Description
address	IP helper address

Default

The IP helper address is not configured.

Command Mode

Interface configuration mode

Usage Description

The command is invalid on the X.25 interface, because the router cannot identify physical broadcasts.

Example

The following example shows how to set the IP helper address on interface ethernet1/0 to 1.0.0.1.

!
interface ethernet 1/0
ip helper-address 1.0.0.1
!

Related command

ip forward-protocol udp

46.1.8 ip proxy-arp

To enable the agent ARP on the interface, run **ip proxy-arp**. To disable the agent ARP on the interface, run **no ip proxy-arp**.

ip proxy-arp

no ip proxy-arp

Parameter

The command has no parameters or keywords.

Default

The agent ARP is conducted.

Command Mode

Interface configuration mode

Usage Description

When the router receives the ARP request, if the router has the route to the requested IP address and the routing interface is different from the request-received interface, the router will send the ARP response out through its own MAC address; after then, the actual data packet will be forwarded after it is received. In this way, a host can communicate with the remote host even if the host does not completely learn the network topology or the correct router is not set for the host. The host is in the same physical subnet as a remote host is.

If a host requires the router to provide the service, the host and the router must be in the same IP network, or at least the router takes that the IP address of the host and the router are in the same IP subnet, that is, they use different masks. The router, otherwise, cannot provide the service.

Example

The following example shows how to enable the ARP agent on interface ethernet1/0.

```
!
interface ethernet 1/0
ip proxy-arp
!
```

46.1.9 ip unnumbered

To set an interface to an unnumbered interface to enable the IP process function without configuring the IP address, run **ip unnumbered *type number***. To stop the IP process on the interface, run **no ip unnumbered**.

ip unnumbered *type number*

no ip unnumbered

Parameter

Parameter	Description
type number	Type and number of an interface whose IP address is configured The interface cannot be the unnumbered interface which has adopted the IP address of other interfaces.

Default

The function is disabled.

Command Mode

Interface configuration mode

Usage Description

You need not configure the unique IP address for the point-to-point link interface. You can run the command to directly handle the IP and specify the valid IP address of other interfaces as the source address of the packets transmitted from the interface. The IP address is thus saved. The point-to-point interface can be called as the unnumbered interface. IP packets generated on the unnumbered interface, such as route-refresh packets, will use the valid IP addresses configured on the command-designated interface. The address must be used to determine which routing processes are sending the refresh packets on the interface. However, it has the following limitations:

(1) The command can set serial interfaces/channel interfaces that are encapsulated by HDLC, PPP, LAPB and SLIP to unnumbered interfaces. However, the command cannot be used on the X.25 interface and the SMDS interface.

(2) You cannot check whether the interface works normally through the ping command. However, you can use SNMP to check the state of the interface remotely.

The command realizes its function based on the regulation in RFC 1195 that the valid IP address cannot be configured on the interface.

Pay attention to the serial links (between different networks) that adopt the IP address of other interfaces; any routing protocol running on the serial link cannot broadcast any information about each subnet.

Example

The following example shows how to set interface serial0/0 to an unnumbered interface and adopt the valid IP address, 1.0.0.1, which configured on interface ethernet0/1, as the source address of the packet transmitted from the interface.

```
!
interface ethernet 0/1
ip address 1.0.0.1 255.255.255.0
!
interface serial 0/0
ip unnumbered ethernet 1/0
!
```

46.1.10 keepalive

To test the reachablity of the host and the connectivity of the network, run the following command:

keepalive [**group** *group-id*] [**source** *source-address*] [**interval** interval-time] [**number** *number*] **destination** *destination-address*

Parameter

Parameter	Description
group *group-id*	Multiple **keepalive** commands can be configured and can be identified by the group ID. The default value of the group ID is 0.
source *source-address*	Specifies the source IP address adopted by the packet. Default: the main IP address of the transmitted interface
interval *interval-time*	Interval for transmitting the packet, whose unit is second Default value: 1 second
number *number*	Number of the transmitted packets Its default value is 5.
destination *destination-address*	Destination host

Command Mode

EXEC or global configuration mode

Usage Description

The **keepalive** command supports the broadcast address and the multicast address. If the address is the limited broadcast address or the multicast address, the ICMP response packet will be transmitted on all interfaces supporting broadcasts and multicasts.

The command need not wait for the ICMP response packet, which only transmits the designated number of ICMP packets to the destination address regularly.

Example

The following shows that two **keepalive** commands are configured.

You can make a configuration that 10 ICMP request packets are transmitted from source address 192.168.20.230 to destination address 192.168.20.1 every 10 seconds. The packet-transmitting port is determined through destination address 192.168.20.1 and the routing protocol.

keepalive group 1 destination 192.168.20.1 source 192.168.20.230 interval 10 number 10

You can make a configuration that five ICMP request packets are transmitted from source address 172.16.20.232 to destination address 172.16.20.5 every second. The packet-transmitting port is determined through destination address 172.16.20.2 and the routing protocol.

keepalive group 2 destination 172.16.20.2 source 172.16.20.232

46.1.11 show arp

To display all ARP items, including the ARP mapping of the IP address for the interface, static ARP mapping and dynamic ARP mapping, run the following command:

show arp [**vrf** *vrf-name*]

Parameter

Parameter	Description
Vrf-name	ARP item which specifies which VRF to be displayed

Command Mode

EXEC

Usage Description

The displayed information shows in the following table:

Parameter	Description
Protocol	Protocol type, such as the IP protocol
Address	Address type, such as the IP address
Age	Lifetime, that is, the duration of ARP item from its generation (unit: minute) The fact that the router uses the ARP item does not affect the value.
Hardware Address	Physical address corresponding to the network address, which is null for the unresolved item

Type	Type of packet encapsulation used by the interface, including ARPA and SNAP
Interface	Interface relative with the network address

Example

The following command is used to display the ARP cache.

```
router#show arp
Protocol  IP Address        Age(min)  Hardware Address    Type   Interface
  IP      192.168.20.77        11     00:30:80:d5:37:e0   ARPA   Ethernet1/0
  IP      192.168.20.33         0       Incomplete
  IP      192.168.20.22         -     08:00:3e:33:33:8a   ARPA   Ethernet1/0
  IP      192.168.20.124        0     00:a0:24:9e:53:36   ARPA   Ethernet1/0
  IP      192.168.0.22          -     08:00:3e:33:33:8b   ARPA   Ethernet1/1
```

46.1.12 show ip hosts

To display all items in the hostname-address cache, run the following command:

show ip hosts

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

The following example shows how to display all hostname-address mappings:

```
show ip hosts
```

Related command

clear ip host

46.1.13 show ip interface

To display the IP configuration of the interface, run the following command:

show ip interface [*type number*]

Parameter

Parameter	Description
type	Type of the interface, which is optional
number	Number of the interface, which is optional

Command Mode

EXEC

Usage Description

If the link layer of an interface can effectively transmit and receive the data, the interface is available, whose state is **Protocol Up**. If an IP address is configured on the interface, the router will add an direct-through route to the routing table. If the link-layer protocol is disabled, that is, if the link-layer protocol is Protocol Down, the direct-through route will be deleted. If the interface type and the number of the interface is specified, only the information about the specified interface is displayed. Otherwise, the information about the IP configuration of all interfaces is displayed.

Example

The following example shows that the IP configuration of interface e0/1 is displayed.

Router#show ip interface e0/1
Ethernet1/0 is up, line protocol is up
IP address : 192.168.20.167/24
Broadcast address : 192.168.20.255
Helper address : not set
MTU : 1500(byte)
Forward Directed broadcast : OFF
Multicast reserved groups joined:
224.0.0.9 224.0.0.6 224.0.0.5 224.0.0.2
224.0.0.1
Outgoing ACL : not set
Incoming ACL : not set
IP fast switching : ON
IP fast switching on the same interface : OFF
ICMP unreachables : ON
ICMP mask replies : OFF
ICMP redirects : ON

The following table gives a detailed description to some parameters in the previous example.

Domain	Description
Ethernet1/0 is up	If the hardware of the interface is available, the interface will be identified as **up**. If the interface is available, its hardware and line

	protocols must be in the **up** state.
line protocol is up	If the interface can provide bidirectional communication, the line protocol will be identified as **up**. If the interface is available, its hardware and line protocols of the interface must be in the **up** state.
IP address	IP address of an interface and network mask
Broadcast address	Displays the broadcast address.
MTU	Displays the IP MTU configured on the interface.
Helper address	Displays the IP helper address.
Directed broadcast forwarding	Forwards the directed broadcast packets.
Multicast reserved groups joined	Multicast groups added to the interface
Outgoing ACL	Outgoing access control list used by the interface
Incoming ACL	Incoming access control list used by the interface
IP fast switching	Enables fast switching on the interface by the router.
Proxy ARP	Enables the proxy ARP on the interface.
ICMP redirects	Forwards the ICMP redirect packet on the interface.
ICMP unreachables	Forwards the ICMP-unreachable packet on the interface.
ICMP mask replies	Forwards the ICMP-mask-replies packet on the interface.

Chapter 47 NAT Configuration Commands

47.1 NAT Configuration Commands

NAT configuration commands include:

- ip nat
- ip nat local-service
- ip nat enable-peek
- ip nat inside destination
- ip nat inside source
- ip nat outside source
- ip nat pool
- ip nat translation
- clear ip nat statistics
- clear ip nat translation
- show ip nat statistics
- show ip nat translations
- debug ip nat

47.1.1 ip nat

ip nat {**inside | outside | mss inside | outside | mss** }

no ip nat {**inside | outside | mss *MSS-value***}

Parameter

Parameter	Description
inside	Shows that the interface connects the internal network (NAT is applied on the network).
outside	Shows that the interface connects the exterior network (NAT is applied on the network).
mss *MSS-value*	Sets MSS to **MSS-value** after **ip nat outside** must be configured.

Default

The communication volume transmitted or received by the interface does not obey the NAT regulation.

Command Mode

Interface configuration mode

Usage Description

Only the packets forwarded between interior interfaces and exterior interfaces can be translated. Each boundary router where the NAT function is applied must be specified at least one interior interface and one exterior interface.

You can run IP NAT to specify that the communication volume coming from the interface or transmitted to the interface obeys NAT; to forbid the NAT function on the interface, run **no IP nat**.

Note:

The **ip nat mss** command can be configured only on the interface of **IP NAT outside**. Its function is to modify the maximum segment size (MSS) in the synchronous TCP packets that are transmitted from the interior network. To forbid the interface to modify MSS, run **no ip nat mss**.

Example

The following example shows that the IP address of packets from host 192.168.1.0 or host 192.168.2.0 is translated to the unique IP address of network 171.69.233.208/28 and MSS is modified to 1432.

```
!
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
  ip nat mss 1432
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standard a1
permit 192.168.1.0 255.255.255.0
permit 192.168.2.0 255.255.255.0
!
```

47.1.2 ip nat local-service

ip nat local-service {**icmp** | **udp** | **tcp** } **disable**

no ip nat local-service {**icmp** | **udp** | **tcp** } **disable**

Parameter

Parameter	Description
icmp	Icmp packet
udp	Udp packet
tcp	Tcp packet

Default

None

Command Mode

Interface configuration mode

Usage Description

The command is used to the NAT regulations. By default, all ICMP/UDP/TCP packets to access the local router are permitted on the router's interface which is identified as the NAT exterior port. The command can limitedly prevent exterior network users from viciously attack the router; however, the packets which normally access the router will be dropped.

To forbid the local ICMP/UDP/TCP packets to access the local router through the router's interface which is identified as the NAT exterior port, you need configure the **ip nat local-service** {**icmp** | **udp** | **tcp** } **disable** command. You can use the “no” form of the command to resume the default state.

Note:

The command can be configured only on the router’s interface where the NAT-identified exterior port lies and can be used to disable only the interface to receive the ICMP/UDP/TCP packets.

47.1.3 ip fastaccess

ip fastaccess deny {**tcp** | **udp** | **icmp**} {***port*** *number*}

no ip fastnat deny {**tcp** | **udp** | **icmp**} {***port*** *number*}

Parameter

Parameter	Description
deny	Defines the regulations of the **deny** packets.
tcp	Defines the regulations of the **tcp** packets.
udp	Defines the regulations of the **udp** packets.
icmp	Defines the regulations of the **icmp** packets.
Port number	Number of the TCP/UDP port, ranging between 1 and 10000

Default

None

Command Mode

Interface configuration mode

Usage Description

Because the **ip fastaccess** command is used to limit packet forwarding on the basis of the transmission layer, the general access list will be used if packet forwarding is limited based on the IP address.

Advice: If you want to constrain interior users through general access lists in the premises of using dynamic NAT regulations, you are strongly recommended to use the NAT-adopted access list. This method can greatly improve the performance especially for the access lists which require to define many regulations.

47.1.4 ip fastnat 1to1

ip fastnat 1to1 outside {***interface****-type number*} [**backup-outside** {***interface****-type number*}] **inside** {***interface****-type number*} [**privateservices**] [**extend**]

no ip fastnat

Parameter

Parameter	Description
outside ***interface****-type number*	Designated network interface which is identified as NAT OUTSIDE, which is the exit of the main line
backup-outside ***interface****-type number*	Designated network interface which is identified as NAT INSIDE, which is the exit of the backup line
inside interface type number	Designated network interface which is identified as NAT INSIDE, which is the entrance of the backup

	line
privateservices	(optional) Enables the private service.
extend	(optional) Enables the expanded access list.

Default

None

Command Mode

Global configuration mode

Usage Description

The command has requirements for network environment. For details, see the configuration manual.

If the private service or expanded access control list is not used, do not use the **privateservices** option or the **extend** option.

47.1.5 ip nat inside destination

To enable the NAT of the interior destination address, run **ip nat inside destination**. To delete the dynamic connection with the address pool, run **no ip nat inside destination**.

ip nat inside destination list *access-list-name* **pool** *name*

no ip nat inside destination list *access-list-name*

Parameter

Parameter	Description
list name	Name of the standard IP access control list, which is used to translate the packets with the destination address through the global address in the designated address pool
pool name	Name of the address pool During the dynamic translation, the address pool will distribute interior local IP addresses.

Default

The interior destination address is not translated.

Command Mode

Global configuration mode

Usage Description

The command is used to create the dynamic address translation in the access control list form. For the packets from the address matched with the standard access control list, the global address allocated by the designated address pool will be used to translate. The address pool is specified by the **ip nat pool** command.

Example

The following example shows that the packets from network 171.69.233.208 are translated to the address of the interior host whose destination address lies at network segment 192.168.2.208.

```
!
ip nat pool net-208 192.168.2.208 192.168.2.223 255.255.255.240
ip nat inside destination list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standar a1
 permit 171.69.233.208 255.255.255.240
!
```

47.1.6 ip nat inside source

To enable the NAT of the interior source address, run **ip nat inside source**. To delete the static translation or the dynamic connection with the address pool, run **no ip nat inside source**.

Dynamic NAT:

ip nat inside source {**list** *access-list-name*} {**interface** *type number* | **pool** *pool-name*} [**overload**]

no ip nat inside source {**list** *access-list-name*} {**interface** *type number* | **pool** *pool-name*} [**overload**]

Static NAT for a single address:

ip nat inside source {**static** {*local-ip global-ip*}

no ip nat inside source {**static** {*local-ip global-ip*}

Static port NAT:

ip nat inside source {**static** {**tcp** | **udp** *local-ip local-port* {*global-ip* | **interface** *type number*} *global-port*}

no ip nat inside source {**static** {**tcp** | **udp** *local-ip local-port* {*global-ip* | **interface** *type number*} *global-port*}

Static NAT of the network segment:

ip nat inside source {**static** {**network local-network global-network** *mask*}

no ip nat inside source {**static** {**network local-network global-network** *mask*}

Parameter

Parameter	Description
List access-list-name	Name of the IP access control list The packets whose source addresses matches the access control list will be translated by the global address of the address pool.
pool name	Name of the address pool where the global IP addresses are dynamically distributed
interface type number	Specifies the network interface.
overload	(optional) enables the router to use one global address for multiple local addresses. After the overload parameter is set, multiple sessions of similar hosts or different hosts will be differentiated by TCP numbers or UDP numbers.
static local-ip	Creates an independent static address translation. It is a local IP address which is distributed to the interior hosts. The local IP address can be selected freely or distributed from RFC 1918.
local-port	Sets the local TCP/UDP number, ranging between 1 and 65535.
static global-ip	Creates independent static address translation. That is, it is used to create an IP address through which an exterior network can access uniquely.
global-port	Sets the global TCP/UDP number, ranging between 1 and 65535.
tcp	Sets TCP port translation.
udp	Sets UDP port translation.
network local-network	Sets the translation for the local network segment.
global-network	Sets the translation for the global network segment.
mask	Sets the network mask for the network segment translation.

Default

The NAT of any interior source address does not exist.

Command Mode

Global configuration mode

Usage Description

The command has two modes: dynamic address translation and static address translation. The dynamic translation is created for the access control list form. For the packets from the address matched with the standard access control list, the global address allocated by the designated address pool will be used to translate. The address pool is specified by the **ip nat pool** command.

As a secondary method, the syntax format with keyword STATIC need an independent static address translation to be created.

To enable the static NAT to support the PASV mode of FTP, those commands to match the overload type are required. When a static FTP mapping of NAT is set, the overload type transfer is needed and one of the addresses of the exterior-network interface following the PAT regulations must be the same as the exterior-network address of the static FTP.

Example

The following example shows that the IP address of packets from host 192.168.1.0 or host 192.168.2.0 is translated to the unique IP address of network 171.69.233.208/28.

```
!
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standard a1
 permit 192.168.1.0 255.255.255.0
 permit 192.168.2.0 255.255.255.0
!
```

The following is an example of using the PASV mode of the static FTP.

```
ip nat inside source static tcp 10.1.1.1 21 204.112.1.2 8021
```

ip nat inside source static tcp 10.1.1.1 20 204.112.1.2 8020
ip nat inside source list test1 interface f0/0

47.1.7 ip nat outside source

To enable the NAT of the exterior source address, run **ip nat outside source**. To delete the static items or dynamic connection, run **no ip nat outside source**.

Note： Dynamic NAT regulations and static network-segment NAT regulations cannot be deleted if they are being used.

Dynamic NAT:

ip nat outside source {**list** *access-list-name*} **pool** *pool-name*

no ip nat outside source {**list** *access-list-name*} **pool** *pool-name*

Static NAT for a single address:

ip nat outside source static {*global-ip local-ip*}

no ip nat outside source static {*global-ip local-ip*}

Static port NAT:

ip nat outside source {**static** {**tcp** | **udp** *global-ip global-port local-ip local-port*}

no ip nat outside source {**static** {**tcp** | **udp** *global-ip global-port local-ip local-port*}

Static NAT of the network segment:

ip nat outside source {**static network** *global-network local-network mask*}

no ip nat outside source {**static network** *global-network local-network mask*}

Parameter

Parameter	Description
List access-list-name	Name of the standard IP access control list The packets whose source addresses matches the access control list will be translated by the global address of the address pool.。
pool name	Name of the address pool where the global IP addresses are dynamically distributed
Static global-ip	Creates an independent static address translation. It is a global IP address which is distributed by the hosts creating the exterior network. The address can be distributed in the globally-routing network address space.
global-port	Sets the global TCP/UDP number, ranging between 1 and 65535.
Static local-ip	Creates independent static address translation. That is, it is used to create an local IP address of the exterior host through which an interior network

	can access uniquely. The address can be distributed in the address space which can be routed by the interior network.
local-port	Sets the local TCP/UDP number, ranging between 1 and 65535.
tcp	Sets TCP port translation.
udp	Sets UDP port translation.
network global-network	Sets the translation for the global network segment.
local-network	Sets the translation for the local network segment.
mask	Sets the network mask for the network segment translation.

Default

The translation between the source addresses of the exterior network and the interior network address does not exist.

Command Mode

Global configuration mode

Usage Description

You probably use the illegal and abnormally-distributed IP address. You also probably use the IP address which is normally distributed to other networks. The fact that the IP address is legally used by the exterior network and also illegally used by the interior network is defined as address overlapping. The NAT can be used to translate the interior addresses which are overlapped with the exterior addresses. If the IP address of your single-connection network is same to the legal IP address of another network and you need communicate with these hosts or routers, you can use the function.

The command has two modes: dynamic address translation and static address translation. The dynamic translation is created for the access control list form. For the packets from the address matched with the standard access control list, the local address allocated by the designated address pool will be used to translate. The address pool is specified by the **ip nat pool** command.

As a secondary method, the syntax format with keyword STATIC need an independent static address translation to be created.

Example

The following example shows that the IP address of packets among hosts in network 9.114.11.0 is translated to the unique global IP address of network 171.69.233.208/28.

```
!
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat pool net-10 10.0.1.0 10.0.1.255 255.255.255.0
ip nat inside source list a1 pool net-208
ip nat outside source list a1 pool net-10
```

```
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 9.114.11.39 255.255.255.0
 ip nat inside
!
ip access-list standard a1
 permit 9.114.11.0 255.255.255.0
 !
```

47.1.8 ip nat pool

To define an IP address pool for NAT, run **ip nat pool**. To delete the IP address pool with a designated name, run **no ip nat pool**.

ip nat pool name *start-ip end-ip netmask* [**rotary**]

no ip nat pool *name*

Parameter

Parameter	Description
name	Name of the IP address pool
start-ip	Start IP address for defining the range of the IP address pool
end-ip	End IP address for defining the range of the IP address pool
netmask	Subnet mask showing which bytes belong to the network and subnet and which bytes belong to the host parts; it can be used to specify the subnet mask of the network to which the addresses of the IP address pool belongs.
rotary	Rotary address pool

Default

The IP address pool is not defined.

Command Mode

Global configuration mode

Usage Description

The command is used to define an IP address pool with the start IP address, end IP address and subnet mask.

Note: The rotary regulations of the IP address pool in the PAT regulations are shown in the following: only when all connections of an address are aging, the next address is required. That is, there is only one interior global address at the same time.

Example

The following example shows that the IP address of packets from host 192.168.1.0 or host 192.168.2.0 is translated to the unique IP address of network 171.69.233.208/28.

```
!
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standard a1
 permit 192.168.1.0 255.255.255.0
 permit 192.168.2.0 255.255.255.0
!
```

47.1.9 ip nat service

The command is an entrance function provided for all services that NAT supports. Currently, only three kinds of services are provided. All services are disabled by default.

ip nat service { **h323** | **privateservice** | **peek** }

no ip nat service { **h323** | **privateservice** | **peek** }

Parameter

None

Default

Shut down

Command Mode

Global configuration mode

Usage Description

The command is used to control the NAT support of h323.

Private service is a kind of support that the NAT does to the internal game server of the cyber bar, such as the legend. It can control the NAT support of the private service.

The **peek** parameter realizes the NAT support to the game monitor server in the cyber bar. Through the client soft of , you can monitor internal users' surfing.

The “no” form of the command is used to disable corresponding functions.

Example

ip nat service privateservice
ip nat service peek
ip nat service h323
no ip nat service peek

47.1.10 ip nat translation

You can run **ip nat translation** to do the following:

Modifying the timeout value of the NAT translation. You can run **no ip nat translation** to close the timeout.

ip nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout** } *seconds*

no ip nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout** }

Modifying the values of some parameters for NAT translation items. You can use the “no” form of the command to delete the previous configuration or resume the default values.

ip nat translation max-entries { **host** [*A.B.C.D* | **any]** } *numbers*

no ip nat translation max-entries { **host** [*A.B.C.D* | **any**] }

Parameter

Parameter	Description
Timeout	Specifies the timeout value of the dynamic translations except the overload translation. The default value is 3600 seconds.
udp-timeout	Specifies the timeout value for the UDP port. The default value is 300

	seconds.
dns-timeout	Specifies the timeout value to connect the DNS. The default value is 60 seconds.
tcp-timeout	Specifies the timeout value for the TCP port. The default value is 3600 seconds.
finrst-timeout	Specifies the timeout value of the **finish and reset TCP** message, which is used to terminate a translation item. The default value is 60 seconds.
icmp-timeout	Sets the timeout time of the NAT of ICMP; the default value is 60 seconds.
max-entries	Sets the maximum number of the NAT translation items; the default value is 3000.
syn-timeout	Sets the NAT timeout time of the TCP SYN state; the default value is 60 seconds.
seconds	Specifies the timeout value of the port translation. The default value is the value listed out at the default part.
max-entries host *A.B.C.D*	For the specified internal IP address, you can control the maximum number of the NAT translation items. There is no default value. You can use the “no” form of the command not to control the maximum number of the NAT translation items.
max-entries host any	For all internal IP addresses, the maximum number of the NAT translation items can be controlled by limiting the single IP address. The default value is same to max-entries.

Default

timeout is 3600 seconds (1 hours)

udp-timeout is 300 seconds (5 minutes)

dns-timeout is 60 seconds (1 minute)

tcp-timeout is 3600 seconds (1 hours)

finrst-timeout is 60 seconds (1 minute)

Command Mode

Global configuration mode

Usage Description

After the port translation is configured, you can further control the translation items for each translation item contains more information about the communication volume. The UDP translation of the DNS times out five minutes later, while that of the domain system times out one minute later. If there is no RST or FIN in the data flow, TCP translation times out one hour later; if there is RST or FIN, it will time out one minute later.

Example

Example 1:

The following example shows that the UDP port translation times out 10 minutes later.

ip nat translation udp-timeout 600

Example 2:

The following example shows that the maximum number of the NAT translation items created by IP 192.168.20.1 is set to 100.

ip nat translation max-entries host 192.168.20.1 100

47.1.11 clear ip nat statistics

To delete the NAT statistics information, run **clear ip nat statistics**.

clear ip nat statistics

Parameter

None

Command Mode

EXEC

Usage Description

You can use the command to resume all NAT statistics information to the original state.

Note:

Only the statistics parameter behind the **packets dropped** option can be deleted.

Example

Router#show ip nat statistics

Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:

FastEthernet0/1

Inside interfaces:

FastEthernet0/0

Dynamic mappings:
--Inside Source
access-list nat

pool natp: netmask 255.255.255.0
start 172.16.20.125 end 172.16.20.127
total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
PAT(ICMP=5 UDP=39 TCP=224 / TOTAL=268), Dynamic=6
Packets dropped:
--Protocol:
Out: tcp 123, udp 39, icmp 10, others 6
In: tcp 46, udp 109, icmp 0, others 10
--Configuration:
max entries 0, max entries for host 178
Router#clear ip nat statistics
Router#show ip nat statistic
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
FastEthernet0/1
Inside interfaces:
FastEthernet0/0
Dynamic mappings:
--Inside Source
access-list nat
pool natp: netmask 255.255.255.0
start 172.16.20.125 end 172.16.20.127
total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
PAT(ICMP=5 UDP=39 TCP=224 / TOTAL=268), Dynamic=6
Packets dropped:
--Protocol:
Out: tcp 0, udp 0, icmp 0, others 0
In: tcp 0, udp 0, icmp 0, fragments 0
--Configuration:
max entries 0, max links for host 0

47.1.12 clear ip nat translation

To delete dynamic NAT from the translation item, run the following commands:

clear ip nat translation {***** | [**inside** local-ip global-ip] [**outside** local-ip global-ip]}

clear ip nat translation {**tcp|udp**} **inside** *local-ip local-port global-ip global-port* [**outside** *local-ip global-ip*]

Parameter

Parameter	Description
*	Deletes all dynamic translation items.
Inside	Deletes the internal translation consisting of the global IP address and the local IP address.
global-ip	Specifies the global IP address.
local-ip	Specifies the local IP address.
outside	Deletes the external translation consisting of the designated global IP address and the local IP address.
tcp|udp	Protocol
global-port	Specifies the global port for the corresponding protocol.
local-port	Specifies the local port for the corresponding protocol.

Command Mode

EXEC

Usage Description

You can run the command to delete the dynamic translation items before they time out.

Example

The following example shows that the NAT translation items are displayed first and then the UDP translation items are deleted.

Router# show ip nat translation

Pro Inside global Inside local Outside local Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53 171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23 171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23 171.69.1.161:23
Router# clear ip nat translation udp inside 171.69.233.209 1220 192.168.1.95 1220 171.69.2.132 53 171.69.2.132 53
Router# show ip nat translation
Pro Inside global Inside local Outside local Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23 171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23 171.69.1.161:23

47.1.13 show ip nat statistics

To display the NAT statistics table, run **show ip nat statistics**.

show ip nat statistics

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

The following information is displayed after you run **show ip nat statistics**.

```
Router# show ip nat statistics
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
  FastEthernet0/1
Inside interfaces:
  FastEthernet0/0
Dynamic mappings:
--Inside Source
    access-list nat
    pool natp: netmask 255.255.255.0
    start 172.16.20.125    end 172.16.20.127
    total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
  PAT(ICMP=0 UDP=5 TCP=24 / TOTAL=29), Dynamic=0
Packets dropped:
--Protocol:
  Out: tcp 0, udp 0, icmp 0, others 0
  In: tcp 46, udp 100, icmp 0, others 0
--Configuration:
  max entries 0, max links for host 0
```

The important fields in the output results are listed in table 2-1.

Table 2- 1 Field description of show ip nat statistics

Field	Description
Total active translations:	Number of designated translations activated in the system When an address translation regulation is created, the value increases by 1; when an address translation regulation is deleted or times out, the value decreases by 1.
Outside interfaces:	List of outside interfaces which are identified by the **ip nat**

	outside command.
Inside interfaces:	List of inside interfaces which are identified by the **ip nat inside** command.
Dynamic mappings:	Information about dynamic mapping
Inside Source:	Information about the inside source address translation
Access-list	Number of access lists for address translation
Pool	Name of the address pool
Netmask	IP network mask used by the address pool
Start	Start IP address of the address range
End	End IP address of the address range
Total addresses	Number of addresses in the pool, which can be used for address translation
Misses	Number of addresses which cannot be distributed from the address pool
Inside Destination:	Information about the inside destination address translation
Outside Source:	Information about the outside source address translation
Link items:	Number and type of translation items
PAT	Number of translation items under dynamic port translation regulations, among which **madia** stands for the RTP/RTCP session.
Dynamic	Number of translation items under dynamic address translation regulations including FTP-created translation items translated from static addresses
Packets dropped:	Type, number and reason of the dropped packets
Protocol	Number, protocol type and NAT direction of the dropped packets
Configuration	Number of packets which are dropped for an incorrect reason: **max entries** means that the maximum number of translation items is exceeded; **max links for host** means that the number of translation items permitted by each address or a specific address is exceeded.

47.1.14 show ip nat translations

To display the activated NAT address translation, run **show ip nat translations**.

show ip nat translations [**host *A.B.C.D* | tcp** | **udp** | **icmp** | **verbose**]

Parameter

Parameter	Description
host *A.B.C.D*	(optional) Displays translation items A, B, C and D which have the inside

	local address.
tcp	(optional) Displays translation items which bear the TCP session.
udp	(optional) Displays translation items which bear the TCP session.
icmp	(optional) Displays translation items which bear the ICMP session.
Verbose	(optional) Displays extra information about each translation item, including how long it has been created and how long it times out.

Command Mode

EXEC

Usage Description

Example

The following information is displayed after you run **show ip nat translations**.

Two inside hosts and some outside hosts are switching packets without overload.

```
Router# show ip nat translations
Pro Inside local      Inside global     Outside local     Outside global
--- 192.168.1.95      171.69.233.209    ---               ---
--- 192.168.1.89      171.69.233.210    ---               --
```

(3) The following example shows that, at the overload condition, three address translation items are activated, among which one is for DNS and the other two are for the TELNET session. Note: two different inside hosts can appear with the same outside address.

```
Router# show ip nat translations
Pro Inside local      Inside global       Outside local      Outside global
udp 192.168.1.95:1220 171.69.233.209:1220 171.69.2.132:53    171.69.2.132:53
tcp 192.168.1.89:11012 171.69.233.209:11012 171.69.1.220:23  171.69.1.220:23
tcp 192.168.1.95:1067 171.69.233.209:1067 171.69.1.161:23    171.69.1.161:23
```

The following example shows the information with the **verbose** keyword.

```
Router# show ip nat translations verbose
Pro Inside local      Inside global     Outside local      Outside global
udp 192.168.1.95:1220  171.69.233.209:1220 171.69.2.132:53   171.69.2.132:53
    create time 00:00:02 , left time 00:01:10 ,
tcp 192.168.1.89:11012 171.69.233.209:11012  171.69.1.220:23  171.69.1.220:23
    create time 00:01:13 , left time 00:00:50 ,
tcp 192.168.1.95:1067  171.69.233.209:1067 171.69.1.161:23   171.69.1.161:23
    create time 00:00:02 , left time 00:53:19 ,
```

Table 2- 2 Fields of output results for the **show IP NAT Translations** command

Field	Description

Pro	Defines the port protocol of the address.
Inside global	Legal IP address, standing for one or multiple inside local IP addresses connecting the exterior network
Inside local	IP address which is allocated to the inside host It may not a legal address provided by NIC or SP.
Outside local	IP address of an outside host when it looks like an inside network, which may not be a legal address provided by NIC or SP
Outside global	IP address of the outside host which is distributed by the owner
Create time	Creation time of the translation item (its unit is hour: minute: second)
Left time	Timeout time of the address translation

47.1.15 debug ip nat

To debug NAT, run **debug ip nat**.

debug ip nat {**detail** | **h323**}

no debug ip nat {**detail** | **h323**}

Parameter

None

Command Mode

EXEC

Usage Description

You can **run debug ip nat detail** to export the details about the translation procedure, including the source/destination IP address, port number and the reason of the failed translation.

You also can run **debug ip nat h323** to export the details about the NAT translation of the H323 packets, including the H323 information identified by NAT, the IP address of the message or the translated address for the inside address.

Example

Example 1:

Router# debug ip nat detail

Ethernet1/1 recv ICMP Src 194.4.4.89 Dst 10.10.10.102 no link found

Ethernet1/0 send TCP Src 194.4.4.102:2000 Dst 192.2.2.1:21 no matched rule

Table 2- 3 Fields in the previous example

Field	Description
Ethernet1/0	Type and number of the interface
send/recv	Send/receive
ICMP/TCP/UDP	ICMP/TCP/UDP protocol
Src 194.4.4.102:2000	Source IP address and port number
Dst 192.2.2.1:21	Destination IP address and port number
no link found	Means that the NAT translation item is not matched.
no matched rule	Means that the NAT regulations are not matched.

The first command line shows that the ICMP packets are received by interface Ethernet1/1 and the corresponding NAT translation items are not found.

The second command line shows that the TCP packets are transmitted from interface Ethernet1/0 and the matched NAT regulations are not found.

Example 2:

Router# debug ip nat h323
NAT:H225:[I] processing a Setup message
NAT:H225:[I] found Setup sourceCallSignalling
NAT:H225:[I] fix TransportAddress addr-192.168.122.50:11140
NAT:H225:[I] found Setup fastStart
NAT:H225:[I] Setup fastStart PDU length:18
NAT:H245:[I] processing OpenLogicalChannel message, forward channel 1
NAT:H245:[I] found OLC forward mediaControlChannel
NAT:H245:[I] fix TransportAddress addr-192.168.122.50:16517
NAT:H225:[I] Setup fastStart PDU length:29
NAT:H245:[I] processing OpenLogicalChannel message, forward channel 1
NAT:H245:[I] found OLC reverse mediaChannel
NAT:H245:[I] fix TransportAddress addr-192.168.122.50:16516
NAT:H245:[I] found OLC reverse mediaControlChannel
NAT:H245:[O] fix TransportAddress addr-192.168.122.50:16517
NAT:H225:[O] processing an Alerting message
NAT:H225:[O] found Alerting fastStart
NAT:H225:[O] Alerting fastStart PDU length:25
NAT:H245:[O] processing OpenLogicalChannel message, forward channel 1

The important fields are described in the following table.

Field	Description
NAT	Means the packet has been translated by NAT.
RAS/H255/H245	Protocol type of the packet
O	Transmission direction of the packet: inside to outside

I	Transmission direction of the packet: outside to inside

Chapter 48 DHCP Client Configuration Command

48.1 DHCP Client Configuration Command

DHCP client configuration commands include:

- ip address dhcp
- ip dhcp client
- ip dhcp-server
- show dhcp lease
- show dhcp server
- debug dhcp

48.1.1 ip address dhcp

To obtain an IP address for the Ethernet interface through DHCP, run **ip address dhcp**. To delete the obtained IP address, run **no ip address dhcp**.

ip address dhcp

no ip address dhcp

Parameter

None

Default

None

Command Mode

Interface configuration mode

Usage Description

The **ip address dhcp** command allows the interface to obtain the IP address through the DHCP protocol, which is useful for dynamically connecting the Internet service provider (ISP) through the Ethernet interface. Once the dynamic IP address is obtained, the Ethernet interface can adopt the PAT technology to realize the network address translation (NAT).

If the **ip address dhcp** command is configured on the router, the router will transmit the DHCPDISCOVER message to the DHCP server.

If the **no ip address dhcp** command is configured on the router, the router will transmit the DHCP RELEASE message.

Example

The following example shows that interface Ethernet1/1 obtains its IP address through the DHCP protocol.

```
!
interface Ethernet1/1
ip address dhcp
!
```

Related command

ip dhcp client

ip dhcp-server

show dhcp lease

show dhcp server

48.1.2 ip dhcp client

To configure the parameter about the DHCP client of the local router, run **ip dhcp client**.

ip dhcp client { minlease *seconds* | retransmit *count* | retry_interval | select *seconds* }

no ip dhcp client { minlease | retransmit | retry_interval | select }

Parameter

Parameter	Description
minlease seconds	(optional) the minimum lease time, ranging from 60 to 86400 seconds
retransmit *count*	(optional) retransmit times of the protocol packets, ranging between 1 and 10
retry_interval	(optional) Interval for retriggering the DHCP request, ranging between 1 and 1440 minutes
select *seconds*	(optional) interval for the **select** operation, ranging between 0 and 30

Default

The default value of the **minlease** parameter is 60 seconds.

The default value of the **retransmit** parameter is four times.

The default value of the **retry-interval** parameter is five seconds.

The default value of the **select** parameter is 0 seconds.

Command Mode

Global configuration mode

Usage Description

You can adjust these parameters according to the network structure and the DHCP server's requirements.

If the "no" forms of these commands are configured, the parameters are reset to the default values defined by the system.

Example

The following example shows that the receivable minimum lease time of the DHCP client on the router is set to 100 seconds.

```
ip dhcp client minlease 100
```

The following example shows how to set the retransmission times of the protocol packets on the DHCP client to three times.

```
ip dhcp client retransmit 3
```

The following example shows how to set the interval of retriggering the DHCP request on the DHCP client to 10 minutes.

```
ip dhcp client retry_interval 10
```

The following example shows how to set the interval of selecting on the DHCP client to 10 seconds.

```
ip dhcp client select 10
```

Related command

ip address dhcp

ip dhcp-server

show dhcp lease

show dhcp server

48.1.3 ip dhcp-server

To specify the IP address of the DHCP server, run **ip dhcp-server**.

ip dhcp-server *ip-address*

no ip dhcp-server *ip-address*

Parameter

Parameter	Description
ip-address	IP address of the DHCP server

Default

The default IP address of the DHCP server does not exist.

Command Mode

Global configuration mode

Usage Description

The command can be used to specify the IP address of the DHCP server, while the previously-designated IP address of the DHCP server will not be replaced.

You can use the “no” form of the command to delete the previously-configured IP address of the DHCP server.

Example

The following example shows how to set the server with IP 192.168.20.1 to the DHCP server.

ip dhcp-server 192.168.20.1

Related command

ip address dhcp

ip dhcp client

show dhcp lease

show dhcp server

48.1.4 show dhcp lease

To check the DHCP server distribution information used by the current router, run **show dhcp lease**.

Show dhcp lease

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

The command can be used to check the DHCP server distribution information used by the current router.

Example

The following example shows the DHCP server distribution information used by the router.

```
router#show dhcp lease
Temp IP addr: 192.168.20.3    for peer on Interface: Ethernet1/1
Temp    sub net mask: 255.255.255.0
    DHCP Lease server: 192.168.1.3, state: 4 Rebinding
    DHCP transaction id: 2049
    Lease: 86400 secs,    Renewal: 43200 secs,    Rebind: 75600 secs
Temp default-gateway addr: 192.168.1.2
    Next timer fires after: 02:34:26
    Retry count: 1      Client-ID: router-0030.80bb.e4c0-Et1/1
```

Related command

ip address dhcp

ip dhcp client

ip dhcp-server

show dhcp server

debug dhcp

48.1.5 show dhcp server

To display the known DHCP server information, run **show dhcp server**.

show dhcp server

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

The command is used to display the information about the known DHCP server.

Example

The following example shows the information about the known DHCP server.

```
router#show dhcp sever
DHCP Server 255.255.255.255
  Leases:   0
  Discovers: 62 Requests: 0       Declines: 0       Releases: 0
  Offers:      0   Acks:       0       Naks:       0       Bad:        0
  Subnet: 0.0.0.0,          Domain name:
```

Related command

ip address dhcp

ip dhcp client

ip dhcp-server

show dhcp lease

48.1.6 debug dhcp

To check the treatment condition of the DHCP protocol, run **debug dhcp**.

debug dhcp <detail>

no debug dhcp <detail>

Parameter

Parameter	Description
detail	Displays the content of the DHCP packet.

Default

Relative information will not be displayed by default.

Command Mode

EXEC

Usage Description

The following example shows some important information about DHCP treatment:

router#debug dhcp
router#2000-4-22 10:50:40 DHCP: Move to INIT state, xid: 0x7
2000-4-22 10:50:40 DHCP: SDISCOVER attempt # 1, sending 277 byte DHCP packet
2000-4-22 10:50:40 DHCP: B'cast on Ethernet1/1 interface from 0.0.0.0
2000-4-22 10:50:40 DHCP: Move to SELECTING state, xid: 0x7
2000-4-22 10:50:46 DHCP: SDISCOVER attempt # 2, sending 277 byte DHCPpacket
2000-4-22 10:50:46 DHCP: B'cast on Ethernet1/1 interface from 0.0.0.0
2000-4-22 10:50:54 DHCP: SDISCOVER attempt # 3, sending 277 byte DHCPpacket

Related command

show dhcp lease

Chapter 49 DHCP Server Configuration Commands

49.1 DHCP Server Configuration Commands

DHCP server configuration commands include:

- ip dhcpd ping packet
- ip dhcpd ping timeout
- ip dhcpd write-time
- ip dhcpd database-agent
- ip dhcpd pool
- ip dhcpd enable
- ip dhcpd disable

49.1.1 ip dhcpd ping packet

ip dhcpd ping packet *pkgs*

Parameter

Parameter	Description
pkgs	A parameter used by the DHCP server to check whether the address has distributed the number of the transmitted ICMP packets.

Default

2

Command Mode

Global configuration mode

Usage Description

You can run the following command to configure whether the DHCP server has transmitted **n** ICMP packets when it check whether the address is distributed.

ip dhcpd ping packets *n*

Example

You can run the following command to configure whether the DHCP server has transmitted **n** ICMP packets when it check whether the address is distributed.

ip dhcpd ping packets 1

49.1.2 ip dhcpd ping timeout

Parameter

Parameter	Description
timeout	Timeout time for waiting the ICMP echo message when the DHCP server is used to check whether the address is distributed

Default

5

Command Mode

Global configuration mode

Usage Description

You can run the following command to set the timeout time for waiting the ICMP echo packet to **n*100ms** when it check whether the address is distributed.

ip dhcpd ping timeout *n*

Example

You can run the following command to set the timeout time for waiting the ICMP echo packet to **300ms** when it check whether the address is distributed.

ip dhcpd ping timeout 3

49.1.3 ip dhcpd write-time

Parameter

Parameter	Description
time	Interval for the DHCP server to save the address distribution information to the database (unit: minute)

Default

0

Command Mode

Global configuration mode

Usage Description

The following command can be used to set the DHCP server to write the address distribution information to the database every **n** minutes.

ip dhcpd write-time *n*

Example

The following example shows that the DHCP server is set to write the address distribution information to the database every two days.

ip dhcpd write-time 1440

49.1.4 ip dhcpd database-agent

Parameter

Parameter	Description
Ip address	IP address of the address distribution information after the DHCP server is saved on PC

Default

None

Command Mode

Global configuration mode

Usage Description

You can run the following command to configure the address of PC where the address distribution information of the DHCP server is stored:

ip dhcpd database-agent X . X . X . X

If the address is not configured, the address distribution information will be stored in the flash.

Note: To store the address distribution information, you need start the TFTP server on PC and at the same time the PC and the DHCP server must correctly connect.

Example

ip dhcpd database-agent 192.168.1.1

49.1.5 ip dhcp snooping arp

Parameter

None

Default

None

Command Mode

Global configuration mode

Usage Description

To enable the ARP mapping protection mechanism, run **ip dhcp snooping arp**. After the command is configured, the DHCP server will create an ARP mapping between the MAC address of the DHCP server and the distributed IP address and protect the ARP mapping.

Example

ip dhcp snooping arp

49.1.6 ip dhcpd pool

Parameter

Parameter	Description
name	Name of the DHCP address pool

Default

None

Command Mode

Global configuration mode

Usage Description

You can run the following command to add the **name** DHCP address pool and enter the DHCP address pool configuration mode.

ip dhcpd pool *name*

Example

The following command in the example is used to add a **test** DHCP address pool and enter the DHCP address pool configuration mode.

ip dhcpd pool test

49.1.7 ip dhcpd enable

Parameter

None

Default

The DHCP service is disabled by default.

Command Mode

Global configuration mode

Usage Description

You can run the following command to enable the DHCP service. After the DHCP service is enabled, the DHCP server supports the relay operation; for those address requests that cannot be distributed by themselves, the DHCP requests will be forwarded on the port where the ip-helper-address is configured.

ip dhcpd pool *name*

Example

The following command is used to open the DHCP service.

ip dhcpd enable

49.2 DHCP Address Pool Configuration Commands

DHCP address pool configuration commands include the following:

- network
- range
- default-router
- dns-server
- domain-name
- lease
- netbios-name-server
- ip-bind

49.2.1 network

network *ip-addr netmask*

Parameter

Parameter	Description
ip-addr	Network address of the address pool for automatic distribution
netmask	Subnet mask

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can use the command to configure the network address of the address pool for automatic distribution.

Before the command is configured, make sure that the network number of the IP address for a port on the interface receiving the DHCP packet must be same to the network.

Example

The following example shows how to set the network address of the DHCP address pool to 192.168.20.0 and the subnet mask to 255.255.255.0.

network 192.168.20.0 255.255.255.0

49.2.2 range

range *low-addr high-addr*

Parameter

Parameter	Description
low-addr	Start address of the automatic address distribution range
hogh-addr	End address of the automatic address distribution range

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can use the command to configure the automatic address distribution range. You can configure up to eight ranges for each address pool, while each range must be in the network. The command is used only for the automatic distribution mode.

Example

The following example shows how to configure the address distribution range of the DHCP address pool to 192.168.20.210~192.168.20.219.

range 192.168.20.210 192.168.20.219

49.2.3 default-router

default-router *ip-addr*

Parameter

Parameter	Description
ip-addr	Default route which is distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the default route which is distributed to the client; up to four default routes can be configured which are separated through space.

Example

The following example shows how to configure the default route of the DHCP client to 192.168.20.1.

default-router 192.168.20.1

49.2.4 dns-server

dns-server *ip-addr* …

Parameter

Parameter	Description
ip-addr	DNS server address distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the address of the DNS server which is distributed to the client; up to four DNS servers can be configured which are separated through space.

Example

The following example shows how to configure the address of the DNS server distributed to the client to 192.168.1.3.

dns-server 192.168.1.3

49.2.5 domain-name

domain-name *name*

Parameter

Parameter	Description
name	Domain name distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the domain name which is distributed to the client.

Example

The following example shows how to configure the domain name to **test.domain**.

domain-name test.domain

49.2.6 lease

lease {**days** [*hours*][*minutes*] | **infinite**}

Parameter

Parameter	Description
days	Days distributed by the address
hours	Hours distributed by the address
minutes	Minutes distributed by the address
infinite	Means that the addresses will be distributed permanently.

Default

one day

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the time limitation of the address which is distributed to the client.

Example

The following example shows how to configure the time limitation of the address which is distributed to the client to 12 hours and two days.

Lease 2 12

49.2.7 netbios-name-server

netbios-name-server *ip-addr*

Parameter

Parameter	Description
ip-addr	Address of the netbios name server distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the address of the netbios name server which is distributed to the client; up to four netbios name servers can be configured which are separated through space.

Example

The following example shows how to configure the address of the DNS server distributed to the client to 192.168.1.10.

netbios-name-server 192.168.1.10

49.2.8 ip-bind

ip-bind *ip-addr* [**hardware-address**] [**identifier**] [**host-name**]

Parameter

Parameter	Description
ip-addr	Host address used for manual distribution
hardware-address	Binds the IP address to the hardware address. The hardware address is in the hex format: 00-12-3F-28-AE-35.
identifier	Binds the IP address to the identifier of the host which is in the hex format or in the format of the inverted command and character string.
host-name	Binds the IP address to the host name which is in the character string format.

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can use the command to configure the host's address of the address pool for automatic distribution.

Example

The following command is used to bind the manually-distributed address 192.168.20.200 to the hardware address 00-12-3F-28-AE-35.

Ip-bind 192.168.20.200 hardware-address 00-12-3F-28-AE-35

The following command is used to bind the manually-distributed address 192.168.20.200 to the host's name **-315**.

Ip-bind 192.168.20.200 host-name -315

ip-bind *ip-addr* hardware-address

ip-bind *ip-addr* **hardware-address** *hardware-address*{ **type**}

Parameter

Parameter	Description

hardware-address	Matches the hardware address of the client.
type	Means the type of the hardware address.

Default value

The default value of the “type” parameter is 1, standing for Ethernet.

Command mode

DHCP address pool configuration mode

Instruction

This command can be used to configure the hardware address, which is used to match the hardware address. The format of the hardware address is like **ab:cd:ef:gh**. This command is used only in manual distribution mode.

Example

The following example shows how to set the hardware address of the manual-DHCP-distribution address pool to **10:a0:0c:13:64:7d**.

ip-bind *ip-addr* hardware-address 10:a0:0c:13:64:7d

49.2.9 ip-bind *ip-addr* client-identifier

ip-bind *ip-addr* **client-identifier** *unique-identifier*

Parameter

Parameter	Description
unique-identifier	Matches the ID of the client.

Default value

None

Command mode

DHCP address pool configuration mode

Instruction

This command is used to configure the client ID which is used to match the client. The format of the client ID is like **ab.cd.ef.gh**. This command is used only in manual distribution mode.

Example

The following example shows how to set the client ID of the manual-DHCP-distribution address pool to **10:a0:0c:13:64:7d**.

ip-bind *ip-addr* client-identifier 01.10.a0.0c.13.64.7d

49.2.10 ip-bind *ip-addr* client-name

ip-bind *ip-addr* **client-name** *name*

Parameter

Parameter	Description
name	Means the name of the client.

Default value

None

Command mode

DHCP address pool configuration mode

Instruction

This command is used to configure the host name which is distributed to the client. This command is used only in manual distribution mode.

Example

The following example shows how to set the name of the client to **test**.

ip-bind *ip-addr* client-name test

49.3 DHCP Debugging Commands

DHCP debugging commands include:

- debug ip dhcpd packet
- debug ip dhcpd event

49.3.1 debug ip dhcpd packet

debug ip dhcpd packet

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

You can run the command to open the debugging switch of the DHCPD packet.

Example

The following command is used to enable the debugging switch of the DHCPD packet.

debug ip dhcpd packet

49.3.2 debug ip dhcpd event

debug ip dhcpd event

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

You can run the command to open the debugging switch of the DHCPD event.

Example

The following command is used to enable the debugging switch of the DHCPD event.

debug ip dhcpd event

DHCPD management commands

DHCP management commands include:

- show ip dhcpd statistic
- show ip dhcpd binding
- clear ip dhcpd statistic
- clear ip dhcpd binding

49.3.3 show ip dhcpd statistic

Parameter

None

Default

None

Command Mode

All modes except the user mode

Usage Description

You can run the command to display the DHCPD statistics information, including the number of all types of packets and the number of automatically- or manually-distributed addresses.

Example

The following command is used to display the DHCPD statistics information.

Show ip dhcpd statistic

49.3.4 show ip dhcpd binding

show ip dhcpd binding {*ip-addr*}

Parameter

Parameter	Description

ip-addr	Address whose binding information requires to be displayed

Default

The binding information of all addresses is displayed.

Command Mode

All modes except the user mode

Usage Description

You can run the following command to display the binding information, IP address, hardware address, binding type and timeout time about the DHCPD.

Example

The following command is used to display the DHCPD binding information.

Show ip dhcpd binding

49.3.5 show ip dhcpd pool

Parameter

None

Default

None

Command Mode

All modes except the user mode

Usage Description

You can run the command to display the information about the DHCPD address pool, including the network number of the address pool, address range, number of the distributed addresses, number of the temporarily-deserted addresses, number of the addresses that can be distributed, manually-distributed IP address and hardware address.

Example

The following command is used to display the statistics information about the DHCPD address pool.

show ip dhcpd pool

49.3.6 clear ip dhcpd statistic

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

You can run the command to delete the statistics information about the number of the packets.

Example

The following command is used to delete the statistics information about the number of the packets.

Clear ip dhcpd statistic

49.3.7 clear ip dhcpd binding

clear ip dhcpd binding {*ip-addr*|*}

Parameter

Parameter	Description
ip-addr	Address whose binding information requires to be deleted
*	Deletes all binding information.

Default

The designated address binding information is deleted.

Command Mode

EXEC

Usage Description

You can run the command to delete the binding information about the designated address.

Example

The following command is used to delete the binding information about address 192.168.20.210.

clear ip dhcpd binding 192.168.20.210

The following command is used to delete the binding information about address 192.168.20.210 and address 192.168.20.211.

clear ip dhcpd binding 192.168.20.210 192168.20.211

The following command is used to delete all binding information.

clear ip dhcpd binding *

49.3.8 clear ip dhcpd abandoned

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

You can run the command to delete the **abandon** identifier.

Example

The following example shows how to delete the **abandon** identifier.

Clear ip dhcpd abandoned

Chapter 50 IP Configuration Commands

50.1 IP Server Configuration Commands

IP server configuration commands include:

- clear tcp
- clear tcp statistics
- debug arp
- debug ip icmp
- debug ip packet
- debug ip raw
- debug ip rtp
- debug ip tcp packet
- debug ip tcp transactions
- debug ip udp
- ip mask-reply
- ip mtu
- ip redirects
- ip route-cache
- ip source-route
- ip tcp synwait-time
- ip tcp window-size
- ip unreachables
- show ip cache
- show ip irdp
- show ip sockets
- show ip traffic
- show tcp

- show tcp brief
- show tcp statistics
- show tcp tcb

50.1.1 clear tcp

To delete a TCP connection, run the following command:

clear tcp {***local*** *host-name port* **remote** *host-name port* | **tcb** ***address***}

Parameter

Parameter	Description
local host-name port	IP address and TCP port of the local host
remote host-name port	IP address and TCP port of the remote host
tcb address	Address of the transmission control block (TCB) for the to-be-deleted TCP connection TCB is an internal identifier of the TCP connection, which can be obtained through the **show tcp brief** command.

Command Mode

EXEC

Usage Description

The **clear tcp** command is mainly used to delete the terminated TCP connection. Sometimes, because of communication line faults, TCP connection or the peer host is restarted and the TCP connection is actually closed. The TCP connection has no communication, so the system does not know that the TCP connection is already closed. In this case, the **clear tcp** command is used to close the invalid TCP connection. The **clear tcp local *host-name port* remote *host-name port*** command is used to close the TCP connection between the IP address or port of the local host and the IP address or port of the remote host. The **clear tcp tcb address** command is used to close the TCP connection identified by the designated TCB address.

Example

The following example shows that the TCP connection between 192.168.20.22:23 (local) and 192.168.20.120:4420 (remote). The **show tcp brief** command is used to display the information of the local and remote hosts of the current TCP connection.

```
Router#show tcp brief
TCB          Local Address          Foreign Address        State
0xE85AC8     192.168.20.22:23       192.168.20.120:4420    ESTABLISHED
```

```
0xEA38C8      192.168.20.22:23        192.168.20.125:1583     ESTABLISHED
Router#clear tcp local 192.168.20.22 23 remote 192.168.20.120 4420
Router#show tcp brief
TCB           Local Address           Foreign Address         State
0xEA38C8      192.168.20.22:23        192.168.20.125:1583     ESTABLISHED
```

The following example shows how to clear the TCP connection whose TCB address is 0xea38c8. The **show tcp brief** command displays the TCB address of the TCP connection.

```
Router#show tcp brief
TCB           Local Address           Foreign Address         State
0xEA38C8      192.168.20.22:23        192.168.20.125:1583     ESTABLISHED
Router#clear tcp tcb 0xea38c8
Router#show tcp brief
TCB           Local Address           Foreign Address         State
```

Related command

show tcp

show tcp brief

show tcp tcb

50.1.2 clear tcp statistics

To clear the statistics data about TCP, run the following command:

clear tcp statistics

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

The following example shows how to delete the TCP statistics information:

```
Router#clear tcp statistics
```

Related command

show tcp statistics

50.1.3 debug arp

To display the ARP interaction information, such as ARP request transmitting, ARP response receiving, ARP request receiving and ARP response transmitting, run **debug arp**. When the router and host cannot communicate with each other, you can run the command to analyze the ARP interaction information. You can run **no debug arp** to stop displaying the ARP interaction information.

debug arp

no debug arp

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#debug arp

Router#IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, Ethernet1/0

IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:

00:00:00:00:00, wrong cable, Ethernet1/1

IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, Ethernet1/0

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, Ethernet1/0

The first information line shows that the router receives an ARP request from Ethernet 1/0. The ARP is sent from a host whose IP address is 192.168.20.116 and MAC address is 00:90:27:a7:a9:c2 and received by a host whose IP address is 192.168.20.111. The ARP request requires the MAC address of the destination host.

IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, Ethernet1/0

The second information line shows that the router receives an ARP address request with IP 192.168.20.139 from interface Etherner 1/1. However, according to the interface configuration of the router, the interface is not in the network claimed by the host. The reason may lie in the incorrect host configuration. If the router creates an ARP cache according to the information, it cannot communicate with a host having the same address though the host connects an interface normally.

IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:

00:00:00:00:00, wrong cable, Ethernet1/1

The third line shows that, before the router resolves the MAC address of host 192.168.20.77, an incomplete ARP item must be created in the ARP cache for the host; after the ARP response is received, the MAC address is entered. According to the configuration of the router, the host connects interface Ethernet1/0.

IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0

The fourth information shows that the router transmits the ARP request from interface Ethernet 1/0, the IP address of the router is 192.168.20.22, the MAC address of the interface is 08:00:3e:33:33:8a and the IP address of the requested host is 192.168.20.77. The four information line has connection with the third information line.

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, Ethernet1/0

The fifth information line shows the router receives the ARP response which is transferred from host 192.168.20.77 to the router's interface 192.168.20.22 on interface Ethernet 1/0, telling that the MAC address is 00:30:80:d5:37:e0. The fifth information line has connection with the third and fourth information lines.

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, Ethernet1/0

50.1.4 debug ip icmp

To display the interaction information of ICMP, run **debug ip icmp**. To close the debugging output, run **no debug ip icmp**.

debug ip icmp

no debug ip icmp

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Usage Description

The command is used to display the received and transmitted ICMP packets, helping to resolve the end-to-end connection problem. To understand the detailed meaning of the **debug ip icmp** command, see RFC 792, "Internal Control Message Protocol".

Example

Router#debug ip icmp

Router#ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48

ICMP: rcvd echo from 192.168.20.125, len 40

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36

ICMP: sent dst (192.168.20.22) protocol unreachable to 192.168.20.124, len 36

ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36

ICMP: rcvd dst (22.0.0.3) host unreachable from 192.168.20.26, len 36

ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36

ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

The first information line is explained as follows:

ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48

Domain	Description
ICMP:	Displays the information about ICMP.
Sent	Transmits the ICMP packets.
pointer indicating	Type of the ICMP packet, which shows the original IP packet is incorrect and specifies the incorrect domain Other types of ICMP packet include: echo reply dst unreachable，including: ---net unreachable ---host unreachable ---protocol unreachable ---port unreachable ---fragmentation needed and DF set ---source route failed ---net unknown ---destination host unknown ---source host isolated ---net prohibited ---host prohibited ---net tos unreachable ---host tos unreachable source quench redirect, including: ---net redirect ---host redirect ---net tos redirect ---host tos redirect echo router advertisement router solicitation time exceeded，including： ---ttl exceeded

	---reassembly timeout parameter problem,including: ---pointer indicating ---option missed ---bad length timestamp timestamp reply information request information reply mask request mask reply If it is the unknown ICMP type, the system will display the ICMP type and its code.
to 192.168.20.124	The destination address of the ICMP packet is 192.168.20.124, which is also the source address of the original packet triggering the ICMP packet.
(dst was 192.168.20.22)	The destination address of the original packet leading to the ICMP packet is 192.168.20.22.
len 48	The length of the ICMP packet is 48 bytes, the length of IP header excluded.

The second information line is explained as follows:

ICMP: rcvd echo from 192.168.20.125, len 40

Domain	Description
rcvd	Receives the ICMP packet.
echo	Request response packet
from 192.168.20.125	The source address of the ICMP packet is 192.168.20.125.

The third information line is explained as follows:

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

Domain	Command
src 192.168.20.22	Means the source address of the ICMP packet is 192.168.20.22.
dst 192.168.20.125	Means the destination address of the ICMP packet is 192.168.20.125.

Different types of ICMP packets have different formats when the ICMP packet is generated.

For example, the ICMP redirect packet adopts the following format:

ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36

ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36

The first information line shows that the redirect ICMP packet from host 192.168.20.77 is received and gateway 192.168.20.26 is recommended to forward the packet to destination host 22.0.0.3; the length of the ICMP packet is 36 bytes.

The second information line shows the redirect ICMP packet is sent to host 192.168.20.124. The redirect ICMP packet notifies the host of using gateway 192.168.20.77 to send packets to host 22.0.0.5. The length of the ICMP packet is 36 bytes.

For the DST unreachable ICMP packet, the following format is adopted for printing:

ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36

ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

The first information line shows that, because the router cannot route a certain IP packet, the destination-unreachable ICMP packet will be sent to source host 192.168.20.124. The length of the ICMP packet is 36 bytes.

The second information line shows that the router receives an ICMP packet from host 192.168.20.26, notifying that the destination host 2.2.2.2 cannot be reached. The length of the ICMP packet is 36 bytes.

50.1.5 debug ip packet

To display the IP interaction information, run **debug ip packet**. You can run **no debug ip packet** to stop displaying the IP interaction information.

debug ip packet [**detail**] [*ip-access-list-name*]

no debug ip packet

Parameter

Parameter	Description
detail	(optional) exports the protocol information encapsulated in the IP packet, including protocol number, UDP, number of the TCP port and type of the ICMP packet.
ip-access-list-name	(optional) name of the IP access list for filtering and exporting information Only the information about the IP packet which meets the requirement of the designated IP access list can be exported.
access-group	(optional) name of the IP access list for filtering and exporting information Only the information about the IP packet which meets the requirement of the designated IP access list can be exported.
interface	(optional) name of the port for filtering and exporting information Only the information about the IP packet which meets the requirement of the designated port can be exported.

Command Mode

EXEC

Usage Description

The command helps you to know the final direction of each received or locally-generated IP packet flow and detect the reason of communication problems.

The following are potential reasons:

- Forwarded
- Forwarded as the broadcast or multicast packet
- Failed addressing when the IP packet is forwarded
- Forwarding the redirect packet
- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route
- Locally-transmitted packets need fragmentation, while the DF bit is reset.
- Receiving the packets
- Receiving IP fragments
- Transmitting packets
- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented
- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the router at a relatively free time, or the system's performance may be badly affected. Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

Command Mode

EXEC

Example

router#debug ip packet

router#IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, redirected

IP: s=192.168.20.22 (local), d=192.168.20.120 (Ethernet1/0), g=192.168.20.120, len=56, sending

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, forward

IP: s=192.168.20.81 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=56, rcvd

Domain	Description
IP	Means that the information is about the IP packet.
s=192.168.20.120 (Ethernet1/0)	Source address of the IP packet and the name of the interface receiving the packet
d=19.0.0.9 (Ethernet1/0)	Destination address of the IP packet and the name of the interface transmitting the packet (if the routing succeeds)
g=192.168.20.1	Destination address of the next hop of the IP packet, which may be the gateway address or the destination address
len	Length of the IP packet
redirected	Means the router will send the ICMP redirected packet to the source host of the ICMP packet. The following are other cases: Forward—the packet is forwarded. forward directed broadcast---Packets are forwarded as the directed broadcast and packets will be transformed as the physical broadcast on the transmission interface unroutable---The addressing of the packet fails and and the packet will be dropped. source route---Source route rejected source route---Because the system does not support the source route, the packets with the IP source route are rejected. Bad options—the IP option is incorrect and the packet will be dropped. need frag but DF set---The local packet need be fragmented; however, the DF is reset. rcvd---the packet is received by the local host. rcvd fragment---The fragment of the packet is received. sending---The locally-generated packet is being sent. sending broad/multicast---The locally-generated broadcast/multicast packet is being sent. sending fragment---The locally-fragmented IP packet is being sent. denied by in acl---The packet is denied by the ACL of the receiver interface. denied by out acl---The packet is denied by the transmitter interface.

	unknown protocol---unknown protocol encapsulation failed---the protocol encapsulation fails in the Ethernet. When the to-be-transmitted packet is dropped on the Ethernet interface becase of ARP resolution failure, the information appears.

The first information line shows that the router has received an IP packet; its source address is 192.168.20.120 and destination address is 19.0.0.9; it is from the network segment connected by interface Ethernet 1/0; the transmitter interface determined by the routing table is interface Ethernet1/0; the gateway's address is 192.168.20.1 and the length of the packet is 60 bytes. The gateway and the source host which transmits the IP packet are connected on the same network, that is, the network connected by interface Ethernet 1/0 of the router. Hence, the router transmits the ICMP redirect packet.

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, redirected

The second information line describes the transmission of the ICMP redirect packet. The source address is the local address 192.168.20.22 and the destination address is the source addresss of the previous packet, that is, 192.168.20.120. The ICMP redirect packet is transmitted from interface Ethernet1/0 to the destination directly, so the address of the gateway is the destination address 192.168.20.120. The length of the ICMP redirect packet is 56 bytes.

IP: s=192.168.20.22 (local), d=192.168.20.120 (Ethernet1/0), g=192.168.20.120, len=56, sending

The third information line shows that the IP layer receives an IP packet. The source address of the packet is 192.168.20.120; the transmitter interface is interface Ethernet1/0; the destination address of the packet is 19.0.0.9. Through the routing table, the packet is found to forward to interface Ethernet1/0; the address of the gateway is 192.168.20.77 and the length of the packet is 60 bytes.

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.77, len=60, forward

The fourth information line shows that the IP layer receives an IP packet. The source address is 192.168.20.81 and the receiver interface is Ethernet1/0; the destination address is 192.168.20.22, which is an IP address configured on interface Ethernet1/0 of the router; the length of the packet is 56 bytes.

IP: s=192.168.20.81 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=56, rcvd

The output of the **debug ip packet detail** command is described in the following. Only newly-added parts are described.

router#debug ip packet detail

router#IP: s=192.168.12.8 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), len=328, rcvd, UDP: src=68, dst=67

IP: s=192.168.20.26 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), len=68, rcvd, proto=89

IP: s=192.168.20.125 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=84, rcvd, ICMP: type=0, code = 0

IP: s=192.168.20.22 (local), d=192.168.20.124 (Ethernet1/0), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

Domain	Description
UDP	Protocol name, such as UDP, ICMP or TCPOther protocols are presented with the protocol number.
type, code	Type and code of the ICMP packet

src, dst	Source port and destination port of the UDP/TCP packet
seq	Sequence number of the TCP packet
ack	Acknowledge number of the TCP packet
win	Windows value of the TCP packet
ACK	ACK in the control bit of the TCP packet is reset, indicating that the acknowledge number is valid. Other control bits include SYN, URG, FIN, PSH and RST.

The first information line shows that the UDP packet is received. The source port is 68 and the destination port is 67.

IP: s=192.168.12.8 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), len=328, rcvd, UDP: src=68, dst=67

The second information line shows that the protocol number of the received packet is 89.

IP: s=192.168.20.26 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), len=68, rcvd, proto=89

The third information line shows that the ICMP packet is received. Both the packet type and the code are 0.

IP: s=192.168.20.125 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=84, rcvd, ICMP: type=0, code = 0

The fourth information line shows that the TCP packet is transmitted. The source port is 1024, the destination port is 23, the sequence number is 75098622, the acknowledge number is 161000466, the size of the receiver window is 17520 and the ACK bit is reset. For the meanings of these domains, see *RFC 793— TRANSMISSION CONTROL PROTOCOL*.

IP: s=192.168.20.22 (local), d=192.168.20.124 (Ethernet1/0), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

The following describes how to use the ACL. For example, to display the information about the packet whose source address is 192.168.20.125, you need to define the abc ACL and then allow the IP packets whose source address is 192.168.20.125. At last, you can use the ACL through the **debug ip packet** command.

Router#**config**

Router_config#**ip access-list standard abc**

Router_config_std_nacl#**permit 192.168.20.125**

Router_config_std_nacl#**exit**

Router_config#**exit**

Router#**debug ip packet abc**

Router#IP: s=192.168.20.125 (Ethernet0/1), d=192.168.20.22 (Ethernet0/1), len=48, rcvd

In the previous commands, the standard ACL is used. However, the expanded ACL can also be used.

Related command

debug ip tcp packet

50.1.6 debug ip raw

To display the information about IP interaction, run **debug ip raw** [**detail**] [***access-list-group***] [***interface***]. To stop displaying information about IP interaction, run **no debug ip raw**.

debug ip raw [**detail**] [***access-list-group***] [***interface***]

no debug ip raw

Parameter

Parameter	Description
detail	(optional) exports the protocol information encapsulated by the IP packet, such as the protocol number, number of the UDP port and the TCP port, and type of the TCP packet.
access-group	(optional) name of the IP ACL which is used to filter the output information Only the information about the IP packets that comply with the designated IP ACL can be exported.
interface	(optional) interface name which is used to filter the output information Only the information about the IP packets that comply with the designated port can be exported.

Command Mode

EXEC

Usage Description

The command helps you to know the final destination of each received or locally-generated IP flows and to find the reason of the communication problem.

The following are potential cases:

- Forwarded
- Forwarded as the broadcast/multicast packet
- Addressing failed when the IP packet is forwarded
- Forwarding the redirect packet
- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route

- Locally-transmitted packets need fragmentation, while the DF bit is reset.
- Receiving the packets.
- Receiving IP fragments
- Transmitting the packet
- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented
- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the router at a relatively free time, or the system's performance may be badly affected. Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

Example

The example is the same to that of the **debug ip packet** command.

Related command

debug ip tcp packet

50.1.7 debug ip rtp

To display the information about the header compression, run **debug ip rtp** {**header-compression|packets |rtcp**}. You can run **no debug ip rtp** {**header-compression|packets |rtcp**} to stop displaying the information about the header compression.

debug ip rtp {**header-compression|packets |rtcp**}

no debug ip rtp {**header-compression|packets |rtcp**}

Parameter

Parameter	Description
header-compress	RTP/UDP/IP header compression
packets	Packets about data interaction of the RTP/UDP/IP header

	compression
rtcp	Packets about data interaction of the TCP/IP header compression

Command Mode

EXEC

Usage Description

The command helps you to understand the whole process of header compression and interaction.

If you use the command, lots of output information will appear; you had better run the router at a relatively free time, or the system's performance may be badly affected.

Example

router # debug ip rtp header-compress

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: new connection, conn 0,

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7078, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7079, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7080, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7081, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7082, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7083, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7084, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7085, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7086, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4024, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7087, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4025, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4026, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7088, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7089, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4027, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7090, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4028, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7091, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4029, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7092, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4030, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7093, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7094, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4032, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7095, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4033, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7096, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4034, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7097, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7098, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4036, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7099, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4037, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7100, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4038, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7101, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: tossing error packet

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7102, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4040, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7103, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4041, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7104, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4042, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7105, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7106, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4044, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7107, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4045, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7108, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4046, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7109, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7110, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4048, Gen = 0

no deb all

50.1.8 debug ip tcp packet

To display the information about receiving and transmitting the TCP packet, run **debug ip tcp packet**. To stop displaying relative information, run **no debug ip tcp packet**.

debug ip tcp packet

no debug ip tcp packet

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#debug ip tcp packet

Router#tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659460

DATA 1 ACK 3130379810 PSH WIN 4380

tcp: I ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 3130379810

DATA 2 ACK 50659460 PSH WIN 16372

tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659461

DATA 50 ACK 3130379812 PSH WIN 4380

tcp: O FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 50659511

ACK 3130379812 FIN WIN 4380

tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812

ACK 50659511 WIN 16321

tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812

ACK 50659512 WIN 16321

tcp: I FIN_WAIT_2 192.168.20.22:23 192.168.20.125:3828 seq 3130379812

ACK 50659512 FIN WIN 16321

tcp: O TIME_WAIT 192.168.20.22:23 192.168.20.125:3828 seq 50659512

ACK 3130379813 WIN 4380

tcp: I LISTEN 0.0.0.0:23 0.0.0.0:0 seq 3813109318

DATA 2 ACK 8057944 PSH WIN 17440

tcp: O LISTEN 0.0.0.0:23 0.0.0.0:0 seq 8057944

RST

Domain	Description
tcp:	Information about the TCP packets
O	Transmits the TCP packets.
ESTABLISHED	Current state of the TCP connectionFor the description of the TCP connection's state, see the description of the **debug ip tcp transactions** command.
192.168.20.22:23	The source address of the packet is 192.168.20.22 and the source port is 23.
192.168.20.125:3828	The destination address of the packet is 192.168.20.125 and the destination port is 3828.
seq 50659460	The sequence number of the packet is 50659460.
DATA 1	Means that the packet contains only one effective byte.
ACK 3130379810	The acknowledgement number of the packet is 3130379810.
PSH	PSH is reset in the control bit of the packet. Other control bits include ACK, FIN, SYN, URG and RST.
WIN 4380	Window domain of the packet used to notify the peer end to receive the cache size, which is 4380 bytes currently
I	Receives the TCP packet.

If a domain of the previous domains does not appear, the domain has no effective value in the TCP packet.

Related command

debug ip tcp transactions

50.1.9 debug ip tcp transactions

To display the important interaction information about TCP, such as the state change of the TCP connection, run **debug ip tcp transactions**. To stop displaying relative information, run **no debug ip tcp transactions**.

debug ip tcp transactions

no debug ip tcp transactions

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#debug ip tcp transactions

Router#TCP: rcvd connection attempt to port 23

TCP: TCB 0xE88AC8 created

TCP: state was LISTEN -> SYN_RCVD [23 -> 192.168.20.125:3828]

TCP: sending SYN, seq 50658312, ack 3130379657 [23 -> 192.168.20.125:3828]

TCP: state was SYN_RCVD -> ESTABLISHED [23 -> 192.168.20.125:3828]

TCP: connection closed by user, state was LISTEN [23 -> 0.0.0.0:0]

TCP: state was TIME_WAIT -> CLOSED [23 -> 192.168.20.125:3827]

TCP: TCB 0xE923C8 deleted

TCP: TCB 0xE7DBC8 created

TCP: connection to 192.168.20.124:513 from 192.168.20.22:1022, state was CLOSED to SYN_SENT

TCP: sending SYN, seq 52188680, ack 0 [1022 -> 192.168.20.124:513]

TCP: state was SYN_SENT -> ESTABLISHED [1022 -> 192.168.20.124:513]

TCP: rcvd FIN, state was ESTABLISHED -> CLOSE_WAIT [1022 -> 192.168.20.124:513]

TCP: connection closed by user, state was CLOSE_WAIT [1022 -> 192.168.20.124:513]

TCP: sending FIN [1022 -> 192.168.20.124:513]

TCP: connection closed by user, state was LAST_ACK [1022 -> 192.168.20.124:513]

TCP: state was LAST_ACK -> CLOSED [1022 -> 192.168.20.124:513]

TCP: TCB 0xE7DBC8 deleted

Domain	Description
TCP:	Displays the TCP interaction information.
rcvd connection attempt to port 23	Receives the connection request from the peer port 23, that is, the TELNET port.
TCB 0xE88AC8 created	Generates a new control block for the TCP connection, which is identified as 0xE88AC8.
state was LISTEN -> SYN_RCVD	Means that the TCP state machine changes from LISTEN to SYN_RCVD. The states of the TCP include: LISTEN—waiting for the TCP connection request from any remote host SYN_SENT—Sending out the connection request to trigger the TCP connection negotiation and then waiting for the peer's response SYN_RCVD—receiving the connection request from the peer, sending out the acknowledgement response and also sending out its connection

	request, and waiting for the connection request acknowledgement from the peer ESTABLISHED—means that the connection is created; the connection is in the data transmission phase; the data of the upper-layer application can be received and transmitted. FIN_WAIT_1—Means that the connection termination request has been transmitted and the response and connection termination request from the peer are being waited. FIN_WAIT_1—Means that the connection termination request has been transmitted and the response from the peer has been received, while the connection termination request from the peer is being waited. CLOSE_WAIT—Means the connection termination request of the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires closing the connection, the system will send the connection termination request. CLOSING—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request. LAST_ACK—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited. TIME_WAIT—Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of the peer's connection termination request and the connection packet still being transmitted in the network is waited to be sent to the destination or be dropped. CLOSED—Means that there is no connection or the connection has been completed shut down. For more detailed information, see *RFC 793, TRANSMISSION CONTROL PROTOCOL*.
[23 -> 192.168.20.125:3828]	The content in the bracket is explained as follows: The first domain (23) stands for the local TCP port. The second domain (192.168.20.125) stands for the remote IP address. The third domain (3828) stands for the remote TCP port.
sending SYN	Transmits a connection request out (the SYN of the control bit in the TCP header is reset). Other TCP control bits include SYN, ACK, FIN, PSH, RST and URG..
seq 50658312	The sequence number of the transmitted packet is 50658312.
ack 3130379657	The acknowledgement number of the transmitted packet is 3130379657.
rcvd FIN	Means that the connection termination request is received (FIN in the control bit of the TCP header is reset).
connection closed	Means that the upper-layer application requires closing the TCP

by user	connection.
connection timed out	Means that the connection is closed because it times out.

Related command

debug ip tcp packet

50.1.10 debug ip udp

To display the information about UDP interaction, run **debug ip udp**. To stop displaying the information about UDP interaction, run **no debug ip udp**.

debug ip udp

no debug ip udp

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#debug ip udp

Router#UDP: rcvd src 192.168.20.99(520), dst 192.168.20.255(520), len = 32

UDP: sent src 192.168.20.22(20001), dst 192.168.20.43(1001), len = 1008

Domain	Description
UDP:	Means that the information is about the UDP packet.
rcvd	Means that the packet is received.
sent	Means that the packet is transmitted.
src	Stands for the source IP address and UDP port of the UDP packet.
dst	Stands for the destination IP address and UDP port of the UDP packet.
len	Stands for the length of the message.

The first information shows that the UDP packet is received. Its source address is 192.168.20.99 and its source port is port 520; its destination address is 192.168.20.255 and its destination port is port 520; the length of the packet is 32 bytes.

The second information shows that the UDP packet is transmitted. Its source address is 192.168.20.22 and its source port is port 20001; its destination address is

192.168.20.43 and its destination port is port 1001; the length of the packet is 1008 bytes.

50.1.11 ip mask-reply

To enable the router to answer the request of the IP mask on the designated interface, run **ip mask-reply**. To disable this function, run **no ip mask-reply**.

ip mask-reply

no ip mask-reply

default ip mask-reply

Parameter

The command has no parameters or keywords.

Default

The IP mask request is not answered.

Command Mode

Interface configuration mode

Example

```
!
interface ethernet 1/1
 ip mask-reply
!
```

50.1.12 ip mtu

To set the MTU of the IP packet transmitted from an interface, run **ip mtu *bytes***. To reuse the default value of MTU, run **no ip mtu**.

ip mtu *bytes*

no ip mtu

Parameter

Parameter	Description
bytes	Maximum IP transmission length which is counted with bytes

Default

The physical media of the interfaces are different, while the MTU on the interfaces are same. Sixty-eight bytes is the minimum MTU.

Command Mode

Interface configuration mode

Usage Description

If the length of the IP packet exceeds the IP MTU configured on the interface, the router will fragment the packet. Devices on the same physical media can communicate with each other only when they are configured with the same MTU. The MTU value will affect the value of the IP MTU. If the value of IP MTU and that of MTU are same, the value of IP MTU will automatically change to the new value of MTU when the MTU value changes. However, the value of MTU will not change if the value of IP MTU changes.

The minimum value of the IP MTU is 68 bytes, and its maximum value cannot exceed the MTU value configured on the interface.

Example

The following example shows how to set the IP MTU of the interface to 200:

```
!
interface serial0/0
ip mtu 200
!
```

Related command

mtu

50.1.13 ip redirects

To transmit the IP ICMP redirect packet, run **ip redirects**. To stop transmitting the IP ICMP redirect packet, run **no ip redirects**.

ip redirects

no ip redirects

Parameter

The command has no parameters or keywords.

Default

In general, the IP redirect packet is transmitted by default. However, the function that the IP redirect packet can be transmitted will be automatically disabled if the hot-standby router protocol is configured on the interface. If the configuration of the hot-standby router protocol is cancelled later, the function cannot be automatically enabled.

Command Mode

Interface configuration mode

Usage Description

When the router detects that the forwarding interface of the gateway is the same as that of the received packet during the transmission of packets and if the packet-transmitting host directly connects the logic network of the interface, the router can transmit an ICMP redirect packet according to the protocol, notifying the source host of directly taking that router as the gateway for the destination address of the packet without packet forwarding through this router.

If the hot-standby router protocol is configured on an interface, the transmission of IP redirect packet may cause the loss of the packet.

Example

The following example shows how to enable the function of transmitting the ICMP redirect passage on interface ethernet1/0:

```
!
interface ethernet 1/0
 ip redirects
!
```

50.1.14 ip route-cache

To enable the route cache on an interface to forward the IP packet, run **ip route-cache**. To forbid the route cache on an interface, run **no ip route-cache**.

ip route-cache

no ip route-cache

ip route-cache same-interface

no ip route-cache same-interface

Parameter

Parameter	Description

same-interface	Allows the IP packet to be rapidly forwarded from the received interface.

Default

Fast switching is allowed on an interface, while fast switching is forbidden on the same interface.

Command Mode

Interface configuration mode

Usage Description

The route cache can conduct the load balance to the forwarded packets based on the source/destination address.

If the route cache is enabled, the packet forwarding rate of the router will be improved. However, the route cache should be forbidden on the low-speed line (64k or even less than 64k).

You can run **ip route-cache same-interface** to allow rapid IP switching on the same interface, that is, the receiver interface is same to the transmitter interface. In general, the function is not recommended to be enabled because the function conflicts with the redirect function of the router. If you has a incompletely-connected network, such as a frame-relay network, you can enable the function on the frame-relay interface. For example, in a frame-relay network consisting of routers A, B and C, there are only links from A to B and from B to C, the communication between router A and router C must be forwarded through router B. In this case, router B receives a packet from router A through a DLCI of an interface, and then transmits the packet to router C through another DLCI of the same interface.

Example

The following command is used to allow fast switching on the same interface.

```
ip route-cache same-interface
```

The following command is used to forbid fast switching even on the same interface.

```
no ip route-cache
```

The following command is used to forbid fast switching only on the same interface.

```
no ip route-cache same-interface
```

The following command is used to enable the default setting (allowing fast switching, the same interface excluded).

```
ip route-cache
```

Related command

show ip cache

50.1.15 ip source-route

To enable the router to handle the IP packet with the source IP route option, run **ip source-route**. To enable the router to drop the IP packet with the source IP route option, run **no ip source-route**.

ip source-route

no ip source-route

Parameter

The command has no parameters or keywords.

Default

The IP packet with the source IP route option is handled.

Command Mode

Global configuration mode

Example

The following example shows how to enable the router to handle the IP packet with the source IP route option.

ip source-route

Related command

ping

50.1.16 ip tcp synwait-time

To set the timeout time for the router to wait for the successful TCP connection, run **ip tcp synwait-time *seconds***. To resume the default timeout time, run **no ip tcp synwait-time**.

ip tcp synwait-time *seconds*

no ip tcp synwait-time

Parameter

Parameter	Description
seconds	Time for the TCP connection, whose unit is second The valid vale ranges between 5 and 300 seconds. The default value is 75.

Default

75 seconds

Command Mode

Global configuration mode

Usage Description

When the router triggers the TCP connection and if the TCP connection is not established in the designated wait time, the router views that the connection fails and then sends the result to the upper-layer program. You can set the wait time for creation of the TCP connection. The default value of the wait time is 75 seconds. The option has no relation with the TCP connection packet which is forwarded through the router, but has relation with the TCP connection of the router itself.

To know the current value, you can run **ip tcp synwait-time?**. The value in the square bracket is the current value.

Example

The following example shows how to set the wait time of creating TCP connection to 30 seconds:

```
Router_config#ip tcp synwait-time 30
Router_config#ip tcp synwait-time ?
  <5-300>[30] seconds        -- wait time
```

50.1.17 ip tcp window-size

To set the size of the TCP window, run **ip tcp window-size *bytes***. To resume the default size of the TCP window, run **no ip tcp window-size**.

ip tcp window-size *bytes*

no ip tcp window-size

Parameter

Parameter	Description
bytes	Size of the windowThe maximum window size is 65535 bytes. The default window size is 2000 bytes.

Default

2000 bytes

Command Mode

Global configuration mode

Usage Description

Do not change the window size at will unless you have a definite purpose. To know the current value, you can run **ip tcp synwait-time ?**. The value in the square bracket is the current value.

Example

The following example shows how to set the size of the TCP window to 6000 bytes.

```
Router_config#ip tcp window-size 6000
Router_config#ip tcp window-size ?
  <1-65535>[6000] bytes        -- Window size
```

50.1.18 ip unreachables

To enable the router to transmit the ICMP unreachable packet, run **ip unreachable**. To enable the router to stop transmitting this packet, run **no ip unreachable**.

ip unreachable

no ip unreachable

Parameter

The command has no parameters or keywords.

Default

The ICMP unreachable packet is transmitted.

Command Mode

Interface configuration mode

Usage Description

When the router forwards the IP packet, the packet may be dropped because there is no relative route in the routing table. In this case, the router can send the ICMP unreachable packet to the source host, notifying the source host and enabling it to detect the host timely and correct the fault rapidly.

Example

The following example shows how to enable the ICMP unreachable packet to be transmitted on interface Ethernet 1/0:

```
!
interface ethernet 1/0
 ip unreachables
!
```

50.1.19 show ip cache

To display the route cache which is used for fast IP switching, run **show ip cache [*prefix mask*] [*type number*]**.

show ip cache [*prefix mask*] [*type number*]

Parameter

Parameter	Description
prefix mask	Displays the items whose destination addresses match up the designated prefixes/masks users enter. It is optional.
type number	Displays the items whose transmitter interfaces match up the designated interface types/numbers users enter. It is optional.
rsvp	Displays RSVP-relative items. It is optional.

Command Mode

EXEC

Example

The following example shows that the route cache is displayed:

Router#show ip cache

Source	Destination	Interface	Next Hop
192.168.20.125	2.0.0.124	Serial1/0	2.0.0.124
192.168.20.124	192.168.30.124	Serial1/0	2.0.0.124
2.0.0.124	192.168.20.125	Ethernet1/1	192.168.20.125

Domain	Description
Source	Source address
Destination	Destination address
Interface	Type and number of the transmitted interface
Next Hop	Gateway's address

The following example shows the route cache whose destination address matches up the designated prefix/mask.

```
Router#show ip cache 192.168.20.0 255.255.255.0
Source          Destination      Interface        Next Hop
2.0.0.124       192.168.20.125   Ethernet0/1      192.168.20.125
```

The following example shows the route cache whose transmitter interface matches up the designated interface type/mask.

```
Router#show ip cache s1/0
Source          Destination      Interface        Next Hop
192.168.20.125  2.0.0.124        Serial1/0        2.0.0.124
192.168.20.124  192.168.30.124   Serial1/0        2.0.0.124
```

50.1.20 show ip irdp

To display the **irdp protocol** information, run **show ip irdp**.

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

```
xuhao_config_e1/0# show ip irdp
Async0/0 ICMP router discovery protocol(IRDP) : OFF

Ethernet1/0 ICMP router discovery protocol(IRDP) : ON

  Advertisements occur between every 450 and 600 seconds
  Advertisements are sent as broadcasts
  Advertisements valid in 1800 seconds
  Default preference : 0

Ethernet1/1 ICMP router discovery protocol(IRDP) : OFF

Null0 ICMP router discovery protocol(IRDP) : OFF

Loopback7 ICMP router discovery protocol(IRDP) : OFF

Loopback10 ICMP router discovery protocol(IRDP) : OFF
```

50.1.21 show ip sockets

To display the socket information, run **show ip sockets**.

show ip sockets

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#show ip sockets

Proto	Local	Port	Remote	Port	In	Out
17	0.0.0.0	0	0.0.0.0	0	161	0
6	0.0.0.0	0	0.0.0.0	0	513	0
17	0.0.0.0	0	0.0.0.0	0	1698	0
17	0.0.0.0	0	0.0.0.0	0	69	0
6	0.0.0.0	0	0.0.0.0	0	23	0
17	0.0.0.0	0	0.0.0.0	0	137	122590

Domain	Description
Proto	Number of the IP protocol If the value is 17, it means the UDP protocol; if the value is 6, it means the TCP protocol.
Remote	Remote address
Port	Remote port
Local	Local address
Port	Local port
In	Total number of the received bytes
Out	Total number of the transmitted bytes

50.1.22 show ip traffic

To display the flow statistics information, run the following command:

show ip traffic

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

```
Router#show ip traffic
IP statistics:
Rcvd:  0 total, 0 local destination, 0 delivered
       0 format errors, 0 checksum errors, 0 bad ttl count
       0 bad destination address, 0 unknown protocol, 0 discarded
       0 filtered , 0 bad options, 0 with options
  Opts:  0 loose source route, 0 record route, 0 strict source route
       0 timestamp, 0 router alert, 0 others
  Frags: 0 fragments, 0 reassembled, 0 dropped
       0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 0 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  230 generated, 0 forwarded
       0 filtered, 0 no route, 0 discarded
ICMP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors
0 redirect, 0 unreachable, 0 source quench
0 echos, 0 echo replies, 0 mask requests, 0 mask replies
0 parameter problem, 0 timestamps, 0 timestamp replies
0 time exceeded, 0 router solicitations, 0 router advertisements
Sent: 0 total, 0 errors
0 redirects, 0 unreachable, 0 source quench
0 echos, 0 echo replies, 0 mask requests, 0 mask replies
0 parameter problem, 0 timestamps, 0 timestamp replies
0 time exceeded, 0 router solicitations, 0 router advertisements

UDP statistics:
Rcvd: 28 total, 0 checksum errors, 22 no port, 0 full sock
Sent: 0 total
```

TCP statistics:

Rcvd: 0 total, 0 checksum errors, 0 no port

Sent: 3 total

IGMP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors
0 host queries, 0 host reports
Sent: 0 host reports

ARP statistics:

Rcvd: 8 total, 7 requests, 1 replies, 0 reverse, 0 other

Sent: 5 total, 5 requests, 0 replies (0 proxy), 0 reverse

Domain	Description
format errors	Error of the packet's format, such as incorrect IP header length
bad hop count	If the router finds that the TTL value of the packet decreases to zero when it forwards the packet, the packet will be dropped.
no route	Means that the router has no corresponding route.

50.1.23 show tcp

To display the states of all TCP connections, run the following command:

show tcp

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#show tcp

TCB 0xE9ADC8

Connection state is ESTABLISHED, unread input bytes: 934
Local host: 192.168.20.22, Local port: 1023
Foreign host: 192.168.20.124, Foreign port: 513

Enqueued bytes for transmit: 0, input: 934 mis-ordered: 0 (0 packets)

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520
irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):

Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396

Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

Domain	Description
TCB 0xE77FC8	Internal identifier of the control block for the TCP connection
Connection state is ESTABLISHED	Current state of the TCP connection The TCP connection may be in one of the following states: LISTEN---Means the TCP connection request from any remote host is being waited. SYN_SENT---Means that the response from the peer is being waited after the connection request is transmitted to the peer. SYN_RCVD---Means that the connection request acknowledgement from the peer is being waited after the local machine receives the peer's connection request, transmits its acknowledgement and also its own connection request. ESTABLISHED---Means that the connection has been established and is now in the data transmission phase in which the upper-layer application can be received or transmitted. FIN_WAIT_1---Means that the peer's acknowledgement and connection termination request is being waited after the local machine transmits the connection termination request to the peer. FIN_WAIT_2---Means that the peer's connection termination request is being waited after the local machine transmits connection termination request to the peer and receives the peer's acknowledgement. CLOSE_WAIT—Means the connection termination request of the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires to close the connection, the system will send the connection termination request. CLOSING—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received

	and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request. LAST_ACK—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited. Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of its connection termination request. CLOSED—Means that there is no connection or the connection has been completely shut down. For more detailed information, see *RFC 793, TRANSMISSION CONTROL PROTOCOL*.
unread input bytes:	Data that is submitted to but not yet received by the upper-layer application after the lower-layer TCP handles
Local host:	Local IP address
Local port:	Local TCP port
Foreign host:	Remote IP address
Foreign port:	Remote TCP port
Enqueued bytes for transmit:	Bytes in the transmission queue, including the transmitted but unacknowledged data bytes and not-yet-transmitted data bytes
input:	Data in the receiver queue which is waiting for being received by the upper-layer application after sorting
mis-ordered:	Number of bytes and number of packets in the mis-ordered queue These data can enter the receiver queue in order and be received by the upper-layer application after other data is received. For example, if packets 1, 2, 3, 4, 5 and 6 are received, packets 1 and 2 can enter the receiver queue, while packets 4, 5 and 6 have to enter the mis-ordered queue to wait for the arrival of packet 3.

The information about the currently-displayed timer will then be displayed, including start-up times, timeout times and next timeout time. Each connection has its independent timers. The timeout times of the timer are generally less than the start-up times of the timer because the timer may be reset when it is running. For example, if the system receives the peer's acknowledgement of all transmitted data when the re-sending timer runs, the re-sending timer will stop running.

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

Domain	Description
Timer	Name of the timer
Starts	Start-up times of the timer
Wakeups	Timeout times of the timer

Next(ms)	Time before next timeout occurs (unit: millisecond) 0 means that the timer is not running.
Retrans	Retransmission timer which is used to retransmit the data The timer is restarted after the data is transmitted. If the data is not acknowledged by the peer during the timeout time, the data will be resent.
TimeWait	Time-wait timer which is used to ensure that the peer receives the acknowledgement of the connection termination request.
SendWnd	Timer of the transmission timer, used to ensure that the receiver window resumes the normal size after the TCP acknowledgement is lost.
KeepAlive	KeepAlive timer used to ensure that the communication link is normal and the peer is still in the connection state It will trigger the transmission of the test packet to detect the state of the communication link and the peer's state.

The sequence number of the TCP connection will then be displayed. The reliable and ordered data transmission is guaranteed through the sequence number. The local/remote host conducts flow control and transmission acknowledgement through the sequence number.

iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520
irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

Domain	Description
iss:	Initial transmission sequence number
snduna:	Transmission sequence number of the first byte in the data which has been transmitted but the peer's acknowledgement is not received
sndnxt:	Transmission sequence number of the first byte in the data which will be transmitted next time
sndwnd:	Size of the TCP window of the remote host
irs:	Initial reception sequence number, that is, initial transmission sequence number of the remote host
rcvnxt:	Recently-acknowledged acceptation sequence number
rcvwnd:	Size of the TCP window of the local host

The transmission time recorded by the local host is then displayed. The system can adapt to different networks according to the data.

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Domain	Description
SRTT:	Round-trip time after smooth handlement
RXT:	Retransmission timeout time
RTV:	Change value of the round-trip time
MinRXT:	Allowable minimum retransmission timeout
MaxRXT:	Allowable maximum retransmission timeout

ACK hold:	Maximum latency time for delaying the acknowledgement and enabling it to be transmitted together with the data

Datagrams (max data segment is 1460 bytes):

Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396

Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

Domain	Description
max data segment is	Maximum data-segment length allowed by a connection
Rcvd:	Number of packets received by the local host through the connection and the number of mis-ordered packets
with data:	Number of packets which contains valid data
total data bytes:	Total data bytes contained in the packet
Sent:	Total number of packets transmitted by the local host during the connection and the number of resent packets

Related command

show tcp brief

show tcp tcb

50.1.24 show tcp brief

To display the brief information about the TCP connection, run the following command:

show tcp brief [**all**]

Parameter

Parameter	Description
all	(optional) Displays all ports. If the keyword is not entered, the system will not display the port in listening mode.

Command Mode

EXEC

Example

Router#show tcp brief

TCB	Local Address	Foreign Address	State
0xE9ADC8	192.168.20.22:1023	192.168.20.124:513	ESTABLISHED
0xEA34C8	192.168.20.22:23	192.168.20.125:1472	ESTABLISHED

Domain	Description

TCB	Internal identifier of the TCP connection
Local Address	Local address and local TCP port
Foreign Address	Remote address and remote TCP port
State	State of the connectionFor details, see the **show tcp** command.

Related command

show tcp

show tcp tcb

50.1.25 show tcp statistics

To display the statistics data about TCP, run the following command:

show tcp statistics

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

```
Router#show tcp statistics
Rcvd: 148 Total, 0 no port
0 checksum error, 0 bad offset, 0 too short
131 packets (6974 bytes) in sequence
0 dup packets (0 bytes)
0 partially dup packets (0 bytes)
0 out-of-order packets (0 bytes)
0 packets (0 bytes) with data after window
0 packets after close
0 window probe packets, 0 window update packets
0 dup ack packets, 0 ack packets with unsend data
127 ack packets (247 bytes)
Sent: 239 Total, 0 urgent packets
6 control packets
123 data packets (245 bytes)
0 data packets (0 bytes) retransmitted
110 ack only packets (101 delayed)
0 window probe packets, 0 window update packets
```

4 Connections initiated, 0 connections accepted, 2 connections established

3 Connections closed (including 0 dropped, 1 embryonic dropped)

5 Total rxmt timeout, 0 connections dropped in rxmt timeout

1 Keepalive timeout, 0 keepalive probe, 1 Connections dropped in keepalive

Domain	Description
Rcvd:	Statistics data of the packets received by the router
Total	Total number of the received packets
no port	Number of received packets which have no destination ports
checksum error	Number of received packets which have checksum error
bad offset	Number of received packets which have offset error
too short	Number of received packets whose length is less than the valid effective length
packets in sequence	Number of packets received in order
dup packets	Number of received duplicate packets
partially dup packets	Number of some duplicate packets received
out-of-order packets	Number of packets received out of order
packets with data after window	Number of received packets whose data exceeds the received window of the router
packets after close	Number of packets received after the connection is closed
window probe packets	Number of received packets about window detection
window update packets	Number of received packets about window update
dup ack packets	Number of packets which are re-acknowledged after received
ack packets with unsent data	Number of packets which are received but not sent
ack packets	Number of acknowledgement packets
Sent	Statistics data of the packets transmitted by the router
Total	Total number of the transmitted packets
urgent packets	Number of transmitted urgent packets
control packets	Total number of control packets (SYN, FIN or RST) which have been transmitted

data packets	Number of transmitted urgent packets
data packets retransmitted	Number of resent data packets
ack only packets	Number of transmitted acknowledgement packets
window probe packets	Number of transmitted packets about window detection
window update packets	Number of transmitted packets about window update
Connections initiated	Number of locally-initiated connections
connections accepted	Number of locally-accepted connections
connections established	Number of locally-established connections
Connections closed	Number of locally-closed connections
Total rxmt timeout	Total number of re-transmission timeouts
Connections dropped in rxmit timeout	Number of disconnected connections because of re-transmission timeout
Keepalive timeout	Number of keepalive timeouts
keepalive probe	Number of transmitted packets about keepalive detection
Connections dropped in keepalive	Number of connections which are disconnected because of Keepalive

Related command

clear tcp statistics

50.1.26 show tcp tcb

To display the state of a TCP connection, run the following command:

show tcp tcb *address*

Parameter

Parameter	Description
address	Address of the transmission control block (TCB) for the to-be-displayed TCP connection TCB is an internal identifier of the TCP connection, which can be obtained through the **show tcp brief** command.

Command Mode

EXEC

Example

The following information is displayed after the **show tcp** command is run:

Router_config#show tcp tcb 0xea38c8

TCB 0xEA38C8

Connection state is ESTABLISHED, unread input bytes: 0
Local host: 192.168.20.22, Local port: 23
Foreign host: 192.168.20.125, Foreign port: 1583

Enqueued bytes for transmit: 0, input: 0 mis-ordered: 0 (0 packets)

Timer	Starts	Wakeups	Next(ms)
Retrans	4	0	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	+5	0	6633000

iss: 10431492 snduna: 10431573 sndnxt: 10431573 sndwnd: 17440
irs: 915717885 rcvnxt: 915717889 rcvwnd: 4380

SRTT: 2812 ms, RXT: 18500 ms, RTV: 4000 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):

Rcvd: 5 (out of order: 0), with data: 1, total data bytes: 3

Sent: 4 (retransmit: 0), with data: 3, total data bytes: 80

Related command

show tcp

show tcp brief

50.2 ACL Configuration Commands

ACL configuration commands include:

- deny
- ip access-group
- ip access-list
- permit

- show ip access-list

50.2.1 deny

To configure the deny rules in IP ACL configuration mode, run **deny *source* [*source-mask*] [log]**; to remote the deny rules from the IP access control list, run **no deny *source* [*source-mask*] [log]**.

deny *source* [*source-mask***] [log]**

no deny *source* [*source-mask***] [log]**

deny src_range source-begin source-end [log]

no deny src_range source-begin source-end [log]

deny *protocol source* *source-mask* ***destination*** *destination-mask* [**precedence** *precedence*] [**tos *tos***] [**log**]

no deny *protocol source* *source-mask* ***destination*** *destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

deny protocol src_range source-begin source-end dst_range destination-begin destination-end [**precedence** *precedence*] [**tos *tos***] [**log**]

no deny protocol src_range source-begin source-end dst_range destination-begin destination-end [**precedence** *precedence*] [**tos *tos***] [**log**]

The following syntax can also be applied to ICMP:

deny icmp *source* *source-mask* ***destination*** *destination-mask* [***icmp-type***] [**precedence** *precedence*] [**tos** *tos*] [**log**]

deny icmp src_range source-begin source-end dst_range destination-begin destination-end [***icmp-type***] [**precedence** *precedence*] [**tos *tos***] [**log**]

The following syntax can be used for IGMP:

deny igmp *source* *source-mask* ***destination*** *destination-mask* [***igmp-type***] [**precedence** *precedence*] [**tos** *tos*] [**log**]

deny igmp src_range source-begin source-end dst_range destination-begin destination-end [***igmp-type***] [**precedence** *precedence*] [**tos *tos***] [**log**]

For TCP, you can use the following syntax:

deny tcp *source* *source-mask* [***operator port***] ***destination*** *destination-mask* [***operator port***] [**established**] [**precedence** *precedence*] [**tos** *tos]* [**log**]

deny tcp src_range source-begin source-end [***src_portrange port-begin port-end***] **dst_range destination-begin destination-end** [***dst_portrange port-begin port-end***] [**established**] [**precedence** *precedence*] [**tos *tos***] [**log**]

For UDP, you can use the following syntax:

deny udp *source* *source-mask* [***operator port***] ***destination*** *destination-mask* [***operator*** *port*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

deny udp src_range source-begin source-end [***src_portrange port-begin port-end***] **dst_range destination-begin destination-end** [***dst_portrange port-begin port-end***] [**precedence** *precedence*] [**tos *tos***] [**log**]

Parameter

Parameter	Description
protocol	Protocol name or IP protocol number It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the **ip** keyword. Some protocol can be further limited, which can be further described.
source	Source network or host numberTwo methods can be used to designate the source: 32-byte binary-system numbers and decimal-system numbers which are separated by four points. The **any** keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.0.
source-mask	Mask of the source address The **any** keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.0.
destination	Source network or host number, which can designated by the decimal numbers or the binary numbers The **any** keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.0.
destination-mask	Mask of the destination network The **any** keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.0.
precedence precedence	Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7. This parameter is optional.
tos tos	An optional parameter, meaning that the packets can be filtered at the service layer It is designated by any number between 0 and 15.
icmp-type	An optional parameter, which means that the ICMP packet can be filtered based on the type of the ICMP packetThe type of the ICMP packet can be designated by a number between 0 and 255.
igmp-type	An optional parameter, which means that the IGMP packets can be filtered based on the type and name of the IGMP packet The type of the IGMP packet can be designated by a number between 0 and 15.
operator	Compares the source or destination ports. It is an optional parameter. The operations include **lt**, **gt**, **eq** and **neq**. If the operator symbol is behind **source** and **source-mask**, it must match up the source port. If the operator symbol is behind **destination** and **destination-mask**, it must match up the destination port.

ISDN(BRI) interface	Decimal number or name of the TCP/UDP port, which is optional The port number ranges between 0 and 65535. The name of the TCP port is listed in the **Usage Explanation** part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the **Usage Explanation** part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.
established	An optional parameter for the TCP protocol, representing an established connection If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
log	An optional parameter, meaning the logs can be recorded
Source-begin	Enables the source address.
Source-end	Terminates the source address.
Destination-begin	Starts the destination address.
Destination-end	Terminates the destination address.
Port-begin	Starts the port.
Port-end	Terminates the port.

Command Mode

ARP Access List Configuration

Usage Description

You can control the packet transmission on an interface, virtual terminal line access and routing choice update through the access control list. After the match-up is conducted, you shall stop checking the expanded access control list.The segmented IP

packet, not the initial segment, will be immediately accepted by any expanded IP access control list. The expanded ACL is used to control the access of the virtual terminal line or limit the content of the routing choice update without matching up the source TCP port, the type of the service value or the packet's priority.

Note:

After an access control list is initially created, any content added later (or entered through the terminal) will be placed at the end of the list.

The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

- bgp
- ftp
- ftp-data

- login
- pop2
- pop3
- smtp
- telnet
- www

The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

- domain
- snmp
- syslog
- tftp

Example

The following example shows that network segment 192.168.5.0 is being forbidden.

```
!
ip access-list standard filter
deny 192.168.5.0 255.255.255.0
!
```

Note:

The IP access control list ends with an implicit deny rule.

Related command

ip access-group

ip access-list

permit

show ip access-list

50.2.2 ip access-group

To control and access an interface, run **ip access-group** {***access-list-name***}{**in** | **out**}. To delete the designated access group, run **no ip access-group** {***access-list-name***}{**in** | **out**}.

ip access-group {*access-list-name*}{**in** | **out**}

no ip access-group {*access-list-name*}{**in | out**}

Parameter

Parameter	Description
access-list-name	Name of the access control list, which is a string with up to 20 characters
in	Uses the access control list on the incoming interface.
out	Uses the access control list on the outgoing interface.

Command Mode

Interface configuration mode

Usage Description

The access control list can be used on the incoming or outgoing interface. For the standard incoming access control list, the source address of the packet will be checked according to the access control list after the packet is received. For the expanded access control list, the router will check the destination address. If the access is the address, the software continues to handle the packet. If the access control list forbids the address, the software drops the packet and returns an ICMP unreachable packet.

For the standard access control list, after a packet is received and routed to a control interface, the software checks the source address of the packet according to the access control list. For the expanded access control list, the router will also check the access control list at the receiver terminal. If the access control list at the receiver terminal permits the packet, the software will then forward the packet. If the access control list forbids the address, the software drops the packet and returns an ICMP unreachable packet.

If the designated access control list does not exist, all packets will be allowed.

Example

The following example shows how to apply the **filter** application list on interface Ethernet 0.

```
!
interface ethernet 0
  ip access-group filter out
!
```

Related command

ip access-list

show ip access-list

50.2.3 ip access-list

To add the IP access control list, run **ip access-list** {**standard | extended**} ***name***.

To delete an IP access control list, run **no ip access-list** {**standard | extended**} ***name***.

ip access-list {**standard | extended**} *name*

no ip access-list {**standard | extended**} *name*

Parameter

Parameter	Description
standard	Specifies the standard access control list.
extended	Specifies the expanded access control list.
name	Name of the access control list, which is a string with up to 20 characters

Default

No IP access control list is defined.

Command Mode

Global configuration mode

Usage Description

After the command is run, the system enters the IP access control list mode. You then can run **permit** or **deny** to configure the access rules.

Example

The following example shows that a standard access control list is configured.

```
!
ip access-list standard filter
deny 192.168.1.0 255.255.255.0
permit any
!
```

Related command

deny

ip access-group

permit

show ip access-list

50.2.4 permit

To configure the **permit** rules in IP ACL configuration mode, run **permit *source* [*source-mask*] [log]**; to remote the **permit** rules from the IP access control list, run **no permit *source* [*source-mask*] [log]**.

permit *source* [*source-mask*] **[log]**

no permit *source* [*source-mask*] **[log]**

permit src_range source-begin source-end [log]

no permit src_range source-begin source-end [log]

permit *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

no permit *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

permit protocol src_range source-begin source-end dst_range destination-begin destination-end [**precedence** *precedence*] [**tos *tos***] [**log**]

no permit protocol src_range source-begin source-end dst_range destination-begin destination-end [**precedence** *precedence*] [**tos *tos***] [**log**]

The following syntax can also be applied to ICMP:

permit icmp *source source-mask destination destination-mask* [***icmp-type***] [**precedence** *precedence*] [**tos** *tos*] [**log**]

permit icmp src_range source-begin source-end dst_range destination-begin destination-end [***icmp-type***] [**precedence** *precedence*] [**tos *tos***] [**log**]

The following syntax can be used for IGMP:

permit igmp *source source-mask destination destination-mask* [***igmp-type***] [**precedence** *precedence*] [**tos** *tos*] [**log**]

permit igmp src_range source-begin source-end dst_range destination-begin destination-end [***igmp-type***] [**precedence** *precedence*] [**tos *tos***] [**log**]

For TCP, you can use the following syntax:

permit tcp *source source-mask* [*operator port*] *destination destination-mask* [***operator*** *port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

permit tcp src_range source-begin source-end [***src_portrange port-begin port-end***] **dst_range destination-begin destination-end** [***dst_portrange port-begin port-end***] [**established**] [**precedence** *precedence*] [**tos *tos***] [**log**]

For UDP, you can use the following syntax:

permit udp *source source-mask* [***operator*** *port* [*port*]] ***destination destination-mask*** [***operator*** *port*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

permit udp src_range source-begin source-end [***src_portrange port-begin port-end***] **dst_range destination-begin destination-end** [***dst_portrange port-begin port-end***] [**precedence** *precedence*] [**tos *tos***] [**log**]

Parameter

Parameter	Description
protocol	Protocol name or IP protocol number It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the **ip** keyword. Some protocol can be further limited, which can be further described.
source	Source network or host number Two methods can be used to designate the source: 32-byte binary-system numbers and decimal-system numbers which are separated by four points. The **any** keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.0.
source-mask	Mask of the source address The **any** keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.0.
destination	Source network or host number, which can designated by the decimal numbers or the binary numbers There are two methods to express the destination network or the host's number: the binary system and decimal system The **any** keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.0.
destination-mask	Mask of the destination network The **any** keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.0.
precedence precedence	Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7. This parameter is optional.
tos tos	An optional parameter, meaning that the packets can be filter at the service layer It is designated by any number between 0 and 15.
icmp-type	An optional packet, which means that the ICMP packet can be filtered based on the type of the ICMP packetThe type of the ICMP packet can be designated by a number between 0 and 255.
igmp-type	An optional parameter, which means that the IGMP packets can be filtered based on the type and name of the IGMP packet The type of the IGMP packet can be designated by a number between 0 and 15.
operator	Compares the source or destination ports. It is an optional parameter. The operations include **lt**, **gt**, **eq** and **neq**. If the operator is behind **source** and **source-mask**, it must match up the source port. If the operator symbol is behind **destination** and **destination-mask**, it must match up the

	destination port.
ISDN(BRI)	Decimal number or name of the TCP/UDP port, which is optional The port number ranges between 0 and 65535. The name of the TCP port is listed in the **Usage Guide** part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the **Usage Explanation** part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.
established	An optional parameter for the TCP protocol, representing an established connection If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
log	An optional parameter, meaning the logs can be recorded
Source-begin	Enables the source address.
Source-end	Terminates the source address.
Destination-begin	Start the destination address.
Destination-end	Terminates the destination address.
Port-begin	Starts the port.
Port-end	Terminates the port.

Command Mode

IP access list configuration mode

Usage Description

You can control the packet transmission on an interface, virtual terminal line access and routing choice update through the access control list. After the match-up is conducted, you shall stop checking the expanded access control list.

The segmented IP packet, not the initial segment, will be immediately accepted by any expanded IP access control list. The expanded ACL is used to control the access of the virtual terminal line or limit the content of the routing choice update without matching up the source TCP port, the type of the service value or the packet's priority.

Note:

After an access control list is initially created, any content added later (or entered through the terminal) will be placed at the end of the list.

The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the command.

- bgp
- ftp

- ftp-data
- login
- pop2
- pop3
- smtp
- telnet
- www

The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the command.

- domain
- snmp
- syslog
- tftp

Example

The following example shows that network segment 192.168.5.0 is allowed.

```
!
ip access-list standard filter
permit 192.168.5.0 255.255.255.0
!
```

Note:

The IP access control list ends with an implicit deny rule.

Related command

deny

ip access-group

ip access-list

show ip access-list

50.2.5 show ip access-list

To display the content of the current IP access control list, run the following command:

show ip access-list[*access-list-name*]

Parameter

Parameter	Description
access-list-name	Name of the access control list, which is a string with up to 20 characters

Default

All standard/expanded IP access control lists will be displayed.

Command Mode

EXEC

Usage Description

The **show ip access-list** command enables you to specify an access control list.

Example

The following information is displayed after the **show ip access-list** command is run while an access control list is not specified:

```
Router# show ip access-list
ip access-list standard aaa
  permit 192.2.2.1
  permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
  permit tcp any any eq www
  permit ip any any
```

The following information is displayed after you run the **show ip access-list** command with an access control specified:

```
ip access-list extended bbb
permit tcp any any eq www
```

Chapter 51 IP ACL Application Commands

51.1 Configuration Commands for Applying IP ACL

The commands for applying the IP Access Control List (ACL) are shown below:

- ip access-group
- ipv6 access-group

51.1.1 ip access-group

To designate an access group, run the **ip access-group**. To cancel the designated access group, run **no ip access-group.**

To apply a created IP ACL on a port, run the following command:

[**no**] **ip access-group** *name* **[egress]**

To apply a created IP ACL globally, run the following command:

[**no**] **ip access-group** *name* **[egress | vlan {***word* **| add** *word* **| remove** *word***}]**

You can use this command to apply the established IP ACL to an interface or globally or cancel the applied IP ACL on an interface or globally.

Parameter

Parameter	Description
name	Stands for the name of IP ACL.
egress	Applies the ACL in an outbound direction.
Vlan	Applies the ACL in an inbound VLAN.
Word	Stands for the VLAN range table.
add	Adds a VLAN range table.
remove	Cancels a VLAN range table.

Command mode

Global or port configuration mode

Explanation

Most rules in the ACL take effect through hardware; those that hardware does not support give no errors but they have no actual effects; a few rules such as time-range take effect through software.

Note:

The IPv4 standard ACL supports the following rules:

any: means any source IP address.

source-addr source-mask: means matching up the source address.

reverse-mask *source-addr source-mask*: means to use the reverse source address for match-up.

The IPv4 extended ACL supports the following rules:

any: means any IP address.

ip-protocol: means the IP protocol ID.

ip-addr source-mask: means IP address match-up.

Interface *interface-id*: means layer-3 interface match-up.

eq/gt/lt/src-portrange: means TCP/UDP port ID match-up.

totallen: means the length match-up of IP packets.

established/tos/is-fragment/not-fragment/precedence/ttl/offset-not-zero/offset-zero/donotfragment-set/ donotfragment-notset/*icmp-type*: means field match-up, among which **ttl** must be set to **equal**.

Example

The following example shows how to apply the ACL filter at the ingress direction of interface g0/1.

Switch_config#inter g0/1

Switch_config_g0/1# ip access-group filter

51.1.2 ipv6 access-group

To designate an access group, run the **ipv6 access-group**. To cancel the designated access group, run **no ipv6 access-group.**

To apply a created IPv6 ACL on a port, run the following command:

[**no**] **ipv6 access-group** *name* **[egress]**

To apply a created IPv6 ACL globally, run the following command:

[**no**] **ipv6 access-group** *name* **[egress | vlan {***word* **| add** *word* **| remove** *word***}]**

You can use this command to apply the established IPv6 ACL to an interface or globally or cancel the applied IPv6 ACL on an interface or globally.

Parameter

Parameter	Description
name	Stands for the name of IPv6 ACL.
egress	Applies the IPv6 ACL in an outbound direction.
Vlan	Applies the IPv6 ACL in an inbound VLAN.
Word	Stands for the VLAN range table.
add	Adds the VLAN range table.
remove	Cancels the VLAN range table.

Command mode

Global configuration mode or port configuration mode

Explanation

Most rules in the ACL take effect through hardware; those that hardware does not support give no errors but they have no actual effects; a few rules such as time-range take effect through software.

Note:

The IPv6 ACL supports the following rules:

any: means any IPv6 address.

Ipv6-addr/ host *Ipv6-addr*： means IPv6 address match-up.

Ipv6-protocol: means the IPv6 protocol ID.

eq/gt/lt/src-portrange: means TCP/UDP port ID match-up.

dscp/flow-label: means field match-up.

Example

The following example shows how to apply the ACL filter at the ingress direction of interface g0/1.

```
Switch_config#inter g0/1
Switch_config_g0/1# ipv6 access-group filter
```

Chapter 52 RIP Configuration Commands

52.1 RIP Configuration Commands

RIP Configuration Commands Include:

- auto-summary
- default-information originate
- default-metric
- ip rip authentication
- ip rip message-digest-key
- ip rip passive
- ip rip password
- ip rip receive version
- ip rip send version
- ip rip split-horizon
- neighbor
- network
- offset
- router rip
- timers expire
- timers holddown
- timers update
- validate-update-source
- version
- distance
- filter
- maximum-count
- show ip rip

- show ip rip database
- show ip rip protocol
- debug ip rip database
- debug ip rip protocol

52.1.1 auto-summary

To activate the automatic summarization function, use the auto-summary command. To turn off this function, use the no form of this command.

auto-summary

no auto-summary

parameter

This command has no parameter or keywords.

default

Enabled by default

command mode

router configuration

instruction

Routing summarization reduces the amount of routing information in the routing tables and switching information. Routing Information Protocol(RIP) do not support subnet mask, therefore, if it is forwarded to subnets, routing possibly cause ambiguity. RIP Version 1 always uses routing summarizarion. If using RIP Version 2, you can turn off routing summarization by using the no auto-summary command. When routing summarization is off,. Subnets are advertised..

example

To specify RIP version on Serial 1/0 as RIP Version 2 and turn off routing summarization function

router rip

version 2

no auto-summary

related commands

version

52.1.2 default-information originate

To generate a default route, use the default-information originate command. To disable this function , use the no form of this command..

default-information originate

no default-information originate

parameter

none

default

disable this function by default

command mode

router configuration

instruction

After the default-information originate command is activated, the routing information(0.0.0.0/0) is accompanied when send routing updating.

example

When send routing updating information, the default routing(0.0.0.0/0) is accompanied.

router rip
version 2
network 172.68.16.0
default-information originate
ip route default f0/0

52.1.3 default-metric

To set default metric values for import routing, use the default-metric command. To return the default stata, use the no form of this command..

default-metric number

no default-metric

parameter

parameter	description
number	Default metric value. It has a value from 1 to 16.

default

Built-in, automatic metric translations, as appropriate for each routing protocol

command mode

router configuration

instruction

The default-metric command is used to set default routing metric used in importing routing of other routing protocols into Rip packets. When import routing of other protocols, use the specified default routing by default-metric if no specified routing metric.

example

The following example shows a routing switch in autonomous system 119 using both the RIP and the OSPF routing protocols. The example advertises OSPF-derived routes using the RIP protocol and assigns the OSPF-derived routes a RIP metric of 8.

```
router rip
default-metric 8
redistribute ospf 119
```

related commands

redistribute

default-information originate

52.1.4 ip rip authentication

To specify the type of authentication used in Routing Information Protocol (RIP) Version 2 packets, use the ip rip authentication mode command in interface configuration mode. To restore plain text authentication, use the no form of this command.

ip rip authentication {**simple** | **message-digest**}

no ip rip authentication

parameter

parameter	description
simple	Plain text authentication.
message-digest	Keyed Message Digest 5 (MD5) authentication.

default

disabled

command mode

interface configuration mode

instruction

RIP Version 1 does not support authentication.

example

The following example configures the interface to use MD5 authentication:

ip rip authentication message-digest

related commands

ip rip password

ip rip message-digest-key

52.1.5 ip rip message-digest-key

To activate Routing Information Protocol (RIP) Version 2 packets authentication and specify Message Digest 5 (MD5) authentication used on the interface, use the ip rip message-digest-key md5 command. To prevent the authentication, use the no form of this command

ip rip message-digest-key *key-id* **md5 password**

no ip rip message-digest-key [*key-id*]

parameter

parameter	description
key-id	A key identifier
password	The specified password

default

MD5 authentication is invalid.

command mode

interface configuration mode

instruction

No authentications are carried out on interface if no passwords are configured using the ip rip message-digest-key key-id md5 password command.

example

The following example configures interface to receive and send MD5 authentication packets that belong to password ‘mykey’:

ip rip message-digest-key 4 md5 mykey

related commands

ip rip authentication

52.1.6 ip rip passive

To cancel the routing switch to send routing updating on interface, use the ip rip passive command. To reactivate the routing updating, use the no form of this command.

ip rip passive

no ip rip passive

parameter

none

default

send routing updates on the interface

command mode

interface configuration mode

instruction

If you cancel routing updating on a certain interface, a specified subnetwork will keep on announcing to other interfaces, and the routing updating that from other routing switches can be continuedly accepted and dealt with on this interface.

example

The following example sends RIP packets updating to all interfaces that belong to the network 172.16.0.0 (except Ethernet interface 1/0):

interface ethernet 1/0
ip address 172.15.0.1 255.255.0.0
ip rip passive
router rip
network 172.16.0.0

related commands

none

52.1.7 ip rip password

To activate Routing Information Protocol (RIP) Version 2 packets authentication and specify the plain text authentication used on the interface, use the ip rip password command Use the no form of this command to prevent authentication.

ip rip password *password*

no ip rip password *password*

parameter

parameter	description
password	the specified password

default

no authenctication

command mode

interface configuration mode

instruction

No authentications are carried out on interface without using the ip rip password command to configure any password.

example

The following example configures interface to receive and send any plain text authentication packet that belong to password ‘mykey’

ip rip password mykey

related commands

ip rip authentication

52.1.8 ip rip receive version

To specify a Routing Information Protocol (RIP) version to receive on specified interface, use the ip rip receive version command in interface configuration mode. To follow the global version rules, use the no form of this command.

ip rip receive version [**1**] [**2**]

no ip rip receive version

parameter

parameter	description
1	(Optional) Accepts only RIP Version 1 packets on the interface.
2	(Optional) Accepts only RIP Version 2 packets on the interface.

default

Accepts RIP Version 1 and RIP Version 2 packets

command mode

interface configuration mode

instruction

Use this command to override the default behavior of RIP as specified by the version command. This command applies only to the interface being configured. You can configure the interface to receive both RIP versions.

example

The following example configures the interface to receive both RIP Version 1 and Version 2 packets:

ip rip receive version 1 2

The following example configures the interface to receive only RIP Version 1 packets:

ip rip receive version 1

related commands

ip rip send version

version

52.1.9 ip rip send version

To specify a Routing Information Protocol (RIP) version to send on specified interface, use the ip rip send version command in interface configuration mode. To follow the global version rules, use the no form of this command.

ip rip send version [**1** | **2** | **compatibility**]

no ip rip send version

parameter

parameter	description
1	(Optional) Sends only RIP Version 1 packets out the interface.
2	(Optional) Sends only RIP Version 2 packets out the interface.
compatibility	(Optional) Broadcasts only RIP Version 2 packets out the interface.

default

Sends only RIP Version 1 packets

command mode

interface configuration mode

instruction

Use this command to override the default behavior of RIP as specified by the version command. This command applies only to the interface being configured. the interface can be configured to receive both RIP Version 1 and Version 2 packets

example

The following example configures the interface to send only RIP Version 1 packets out the interface:

ip rip send version 1

The following example configures the interface to send only RIP Version 2 packets out the interface:

ip rip send version 2

related commands

ip rip receive version

version

52.1.10 ip rip split-horizon

To enable the split horizon mechanism, use the ip split-horizon command in interface configuration mode. To disable the split horizon mechanism, use the no form of this command.

ip rip split-horizon

no ip rip split-horizon

parameter

none

default

Default behavior varies with media type.

command mode

interface configuration mode

instruction

For all interfaces except those for which either Frame Relay or Switched Multimegabit Data Service (SMDS) encapsulation is enabled, the default condition for this command is ip split-horizon; in other words, the split horizon feature is active. If the interface configuration includes either the encapsulation frame-relay or encapsulation smds command, then the default is for split horizon to be disabled.

Note: For networks that include links over X.25 packet switched networks (PSNs), the neighbor routing switch configuration command can be used to defeat the split horizon feature. You can as an alternative explicitly specify the no ip split-horizon command in

your configuration. However, if you do so you must similarly disable split horizon for all routing switches in any relevant multicast groups on that network.

If split horizon has been disabled on an interface and you want to enable it, use the ip split-horizon command to restore the split horizon mechanism.

Note: In general, changing the state of the default for the ip split-horizon command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a PSN), you must disable split horizon for all routing switches and access servers in any relevant multicast groups on that network.

example

The following simple example disables split horizon on a serial link. The serial link is connected to an X.25 network.

```
interface serial 1/0
encapsulation x25
no ip rip split-horizon
```

related commands

neighbor

52.1.11 neighbor

To define a neighboring routing switch with which to exchange routing information, use the neighbor command in routing switch configuration mode. To remove an entry, use the no form of this command.

neighbor *ip-address*

no neighbor *ip-address*

parameter

parameter	description
ip-address	IP address of a peer routing switch with which routing information will be exchanged.

default

No neighboring routing switches are defined.

command mode

router configuration

instruction

This command permits the point-to-point (nonbroadcast) exchange of routing information in order to meet special requirements of the specified nonbroadcast network.

example

In the following example, the neighbor routing switch configuration command permits the sending of routing updating to specific neighbors.

router rip

neighbor 131.108.20.4

related commands

network

52.1.12 network

To specify a list of networks for the Routing Information Protocol (RIP) routing process, use the network command in routing switch configuration mode. To remove an entry, use the no form of this command.

network *network-numbe <network-mask>*

no network *network-number <network-mask>*

parameter

parameter	description
Network-number	IP address of the network of directly connected networks.
Network-mask	(optional) IP mask of the network of directly connected networks

default

No networks are specified.

command mode

router configuration

instruction

The network number specified must not contain any subnet information. There is no limit to the number of network commands you can use on the routing switch. RIP routing updates will be sent and received only through interfaces on this network.

RIP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP updates.

example

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 128.99.0.0 and 192.31.7.0:

router rip
network 128.99.0.0
network 192.31.7.0

related commands

router rip

52.1.13 offset

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the offset command in routing switch configuration mode. To remove an offset list, use the no form of this command.

offset {*type number* | ***}** {**in | out**} *access-list-name* **offset**

no offset {*type number* | ***}** {**in | out**}

parameter

parameter	description
In	Applies the access list to incoming metrics.
Out	Applies the access list to outgoing metrics.
access-list-name	Standard access list number to be applied. Access list number 0 indicates all access lists. If offset is 0, no action is taken.
offset	Positive offset to be applied to metrics for networks matching the access list.
type	Interface type to which the offset list is applied.
number	(Optional) Interface number to which the offset list is applied.

default

This command is disabled by default.

command mode

router configuration

instruction

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

example

In the following example, the routing switch applies an offset of 10 to routes learned from Ethernet interface 1/0:

offset ethernet 1/0 in 21 10

52.1.14 router rip

To configure the Routing Information Protocol (RIP) routing process, use the router rip command in global configuration mode. To turn off the RIP routing process, use the no form of this command.

router rip

no router rip

parameter

none

default

No RIP routing process is defined.

command mode

global configuration mode

instruction

User should first enable RIP to enter router configuration mode to configure all global parameters of RIP. However, it is regardless whether RIP is enabled if you configure parameters related to interface,

example

The following example shows how to begin the RIP routing process:

router rip

related commands

network (RIP)

52.1.15 timers expire

To adjust RIP network timers, use the timers expire router configuration command. To restore the default timers, use the no form of this command.

timers expire interval

no timers expire

parameter

parameter	description
expire	Interval of time in seconds after which a route is declared invalid; it should be at least three times the value of update. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.

default

180 seconds

command mode

router configuration

instruction

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note: The current and default timer values can be seen by the show ip rip command.

example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable.

router rip

timers expire 30

52.1.16 timers holddown

To adjust RIP network timers, use the timers holddown routing switch configuration command. To restore the default timers, use the no form of this command.

timers holddown second

no timers holddown

parameter

parameter	description
second	Interval in seconds during which routing information regarding better paths is suppressed. It should be at least three times the value of update. A route enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 120 seconds.

default

120 seconds

command mode

router configuration

instruction

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note:

The current and default timer values can be seen by the show ip rip command.

example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable.

router rip

timers holddown 30

52.1.17 timers update

To adjust RIP network timers, use the timers update routing switch configuration command. To restore the default timers, use the no form of this command.

timers update update

no timers update

parameter

parameter	description
update	Rate in seconds at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.

default

30 seconds

command mode

router configuration

instruction

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note:

The current and default timer values can be seen by the show ip rip command.

example

In the following example, updates are broadcast every 5 seconds.

router rip

timers update 5

Note that by setting a short update period, you run the risk of congesting slow-speed serial lines; however, this is not a big concern on faster-speed Ethernets and T1-rate serial lines. Also, if you have many routes in your updates, you can cause the routing switches to spend an excessive amount of time processing updates.

52.1.18 validate-update-source

To have the software validate the source IP address of incoming routing updates for RIP routing protocols, use the validate-update-source routing switch configuration command. To disable this function, use the no form of this command.

validate-update-source

no validate-update-source

parameter

This command has no parameters or keywords.

default

Enabled

command mode

router configuration

instruction

This command is only applicable to RIP and IGRP. The software ensures that the source IP address of incoming routing updates is on the same IP network as one of the addresses defined for the receiving interface.

Disabling split horizon on the incoming interface will also cause the system to perform this validation check.

For unnumbered IP interfaces (interfaces configured as ip unnumbered), no checking is performed.

example

In the following example, a routing switch is configured to not perform validation checks on the source IP address of incoming RIP updates:

```
router rip
 network 128.105.0.0
 no validate-update-source
```

52.1.19 version

To specify a RIP version used globally by the routing switch, use the version routing switch configuration command. Use the no form of this command to restore the default value.

version {1 | 2}

no version

parameter

parameter	description
1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

default

The software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets.

command mode

router configuration

instruction

To specify RIP versions used on an interface basis, use the ip rip receive version and ip rip send version commands; or it will send RIP packets in terms of the global configuration version.

example

The following example enables the software to send and receive RIP Version 2 packets:

version 2

related commands

ip rip receive version

ip rip send version

52.1.20 distance

To define an administrative distance for RIP routes, use the distance command in routing switch configuration mode.

Distance weight <address mask <access-list-name>>

parameter

parameter	description
weight	Administrative distance. An integer from 1 to 255. It is recommended to use 10 to 255. (The values 0 to 9 are reserved for internal use.) Routes with a distance value of 255 are not installed in the routing table.)
address	(Optional) Source IP address (in four-part, dotted decimal notation)
mask	(Optional) IP address mask (in four-part, dotted decimal notation) If a certain digit is 0, software will omit the corresponding value in the address.
access-list-name	(Optional) Named access list to be applied to incoming routing updates.

default

120

command mode

EXEC

instruction

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. When the optional access list name or number is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows filtering of networks according to the IP address of the routing switch that supplies the routing information.

example

The following example sets the administrative distance to 100 for the routing switch with the address 192.1.1.0/24.

```
router rip
distance 100 192.1.1.0 255.255.255.0
```

52.1.21 filter

To filter for RIP routes, use the filter command.

filter * in access-list {*access-list-name*}

filter * in gateway {*access-list-name*}

filter * in prefix { *prefix-list-name*}

filter type *number* **in access-list** {*access-list-name*}

filter type *number* **in gateway** {*access-list-name*}

filter type *number* **in prefix** {*prefix-list-name*}

no filter * in

no filter type *number* **in**

filter * out access-list {*access-list-name*}

filter * out gateway {*access-list-name*}

filter * out prefix { *prefix-list-name*}

filter type number out access-list {*access-list-name*}

filter type number out gateway {*access-list-name*}

filter type number out prefix {*prefix-list-name*}

no filter * out

no filter type *number* **out**

parameter

parameter	description
access-list-name	Standard IP access list name. This list defines networks of which are received or suppressed in routing update.
prefix-list-name	Standard IP prefix list name. This list defines networks of which are received or suppressed in routing update.
in/out	Applies access list for in/out routing update.
type	(Optional) Interface type
number	(Optional)Indicates number of interface on which applies the access list for in/out routing update. If no interface is defined, the access list is applicabale to all in/out routing update.

default

disabled

command mode

EXEC

instruction

Filter the route that are to be sent and received.If you use the access-list command to configure access list for dynamic routing protocol, you shoul use the standard access list.

example

The following example filter route 10.0.0.0/8 from interface s2/1:

router rip
filter s2/1 out access-list mylist
ip access-list standard mylist
deny 10.0.0.0 255.0.0.0

52.1.22 maximum-count

To configure the maximum route count in local RIP routing table, use the maximum-count command. Use the no form of this command to restore default setting.

maximum-count *number*

no maximum-count

parameter

parameter	description
number	The maximum route count to be confgirued, in the range from 512 to 4096.

default

1024

command mode

router configuration

instruction

Use this command to configure the maximum route count in local RIP routing table. When routes in local routing table exceed the maximum value, no routes will be added to routing table.

example

The following example configures 2000 as the maximum route count in the local RIP routing table:

router rip
maximum-count 2000

related commands

none

52.1.23 show ip rip

To display RIP main information, use the show ip rip command.

show ip rip

parameter

none

default

none

command mode

EXEC

instruction

User can see the current configuration status about RIP according to the output of this command.

example

The following example displays configuration parameter information about RIP:

router#show ip rip
RIP protocol: Enabled
Decided on the interface version control
AUTO-SUMMARY: Yes
Update: 30, Expire: 180, Holddown: 120
Distance: 120
default-metric: 1

The meaning of the above fields are as follows:

field	description
Enabled	Indicates current state of the active routing protocol process.
Distance	Indicates current administrative distance.

version	Indicates current version of the protocol.
AUTO-SUMMARY	Indicates whether to allow auto-summary or not.
Update	Interval of time at which updates are sent.
Holddown	Interval (in seconds) during which routing information regarding better paths is suppressed.
Expire	Interval of time after which a route is expired.
RIP default-metric	Default metric value during redistribute

52.1.24 show ip rip database

To display summary address entries in the Routing Information Protocol (RIP),use the show ip rip database command

show ip rip database

parameter

none

default

none

command mode

EXEC

instruction

Summary address entries will appear in the database from output of this command.

example

The following output shows a summary address entry:

router#show ip rip database
1.0.0.0/8 auto-summary
1.1.1.0/24 directly connected Loopback1
100.0.0.0/8 via 192.1.1.2 00:00:02
192.1.1.0/24 directly connected Serial2/1
192.1.1.0/24 auto-summary

The meanings of the following fields are as follows:

field	description

Network-number/network-mask	RIP routes
Summary/connected/via gateway	The corresponding RIP route types
interface	RIP directly connected and summary routes interface
time	refreshed time

52.1.25 show ip rip protocol

To display RIP protocol configuration information, use the show ip rip protocol command.

show ip rip protocol

parameter

none

default

none

command mode

EXEC

instruction

User can see the current RIP protocol configuration information from output of this command.

example

The following example displays RIP protocol configuration information:

```
router#show ip rip protocol
RIP is Active
  Sending updates every 30 seconds, next due in 30 seconds
  Invalid after 180 seconds, holddown 120
  update filter list for all interfaces is:
  update offset list for all interfaces is:
  Redistributing:
  redistribute connect
  Default version control: send version 1, receive version 1 2
    Interface          Send               Recv
    Async0/0             1                  1 2
```

```
  FastEthernet0/0       1                   1 2
  Serial1/0             1                   1 2
  Ethernet1/1           1                   1 2
  Serial2/0             1                   1 2
  Serial2/1             1                   1 2
  Loopback1             1                   1 2
 Automatic network summarization is in effect
 Routing for Networks:
  174.168.0.0/16
 Distance: 120 (default is 120)
```

52.1.26 debug ip rip database

To monitor RIP routed events, use the debug ip rip database command.

debug ip rip database

parameter

none

default

none

command mode

EXEC

instruction

User can see some events of the current RIP routes from output of this command.

example

Thd following example monitors some events of the RIP routes:

```
router# debug ip rip database
RIP-DB: Adding summary route 192.1.1.0/24 <metric 0> to RIP database
```

The meanings of the above fields are as follows:

field	description
summary	Indicates the route type that added to the routing table
192.1.1.0/24	Indicates the route that added to the routing table
<metric 0>	Route metric value

52.1.27 debug ip rip protocol

To monitor RIP packets, use the debug ip rip protocol command.

debug ip rip protocol

parameter

none

default

none

command mode

EXEC

instruction

User can see the current content of RIP packets from the output of this command.

example

The following example monitors RIP packets:

router# debug ip rip protocol
RIP: send to 255.255.255.255 via Loopback1
vers 1, CMD_RESPONSE, length 24
192.1.1.0/0 via 0.0.0.0 metric 1.

The following output will be displayed when ran on the version 2:

RIP: send to 255.255.255.255 via Loopback1
vers 2, CMD_RESPONSE, length 24
192.1.1.0/24 via 0.0.0.0 metric 1

The meaning of the above fields are as follows:

field	description
Send/Recv	Indicates packets that are sent or received packets
to 255.255.255.255	Iindicates the destination address of IP packets
via Loopback1	Indicatesthe interface on which RIP packets that are sent and received.
vers 2	Indicates version of RIP packets that are sent and received.
CMD_RESPONSE/ CMD_REQUEST	Indicates type of the packet
length 24	Indicates length of packet.

192.1.1.0/24	Indicates destination network in routing informaiohti
via 0.0.0.0	Indicates next hop address.
metric	Route metric value

Chapter 53 BEIGRP Configuration Commands

53.1 BEIGRP Configuration Commands

BEIGRP Configuration Commands Include:

- auto-summary
- clear ip beigrp neighbors
- debug ip beigrp
- debug ip beigrp fsm
- debug ip beigrp neighbours
- debug ip beigrp packet
- debug ip beigrp transmit
- default-metric
- distance
- filter
- beigrp log-neighbor-changes
- beigrp router-id
- ip beigrp bandwidth-percent
- ip beigrp hello-interval
- ip beigrp hold-time
- ip beigrp passive
- ip beigrp split-horizon
- ip beigrp summary-address
- metric weights
- network
- offset
- redistribute
- router beigrp

- show ip beigrp interface
- show ip beigrp neighbors
- show ip beigrp protocol
- show ip beigrp topology
- show ip beigrp traffic

53.1.1 auto-summary

To allow automatic summarization of BEIGRP routes, use the auto-summary command in routing switch configuration mode.The automatic summarization function is abled by default. To disable this function and send every specific routing information to its neighbours, use the no form of this command.

auto-summary

no auto-summary

parameter

none

default

Enabled

command mode

router configuration

instruction

In the current BEIGRP version, route summarization is closely related to network commands. It enforces the following summarization rules:

- When one BEIGRP process defines various networks, creat route summarization of defined network as long as BEIGRP Topology Table includes one subnet in the current network.
- The summary routes point to Null0 interface, which have the minimum distance of all the concrete routes that summary routes contain. The summary routes insert to the main IP routing table, and the administrative distance is 5(which cannot be configured)
- When send updates to neighbours of different main IP networks, cancel the subnets in automatic summarization of the first rule and the second rule, just send the summarization route.

- Summarize the subnets in networks that belong to BEIGRP process definition list.

related commands

ip beigrp summary-address

network

53.1.2 clear ip beigrp neighbors

To delete entries from the neighbor table, use the clear ip beigrp neighbors command in privileged EXEC mode.

clear ip beigrp [*as-number*] **neighbors** [*ip-address* | *interface*-type *interface-number*]

parameter

parameter	description
ip-address	(Optional) Address of BEIGRP's neighbor.
interface	(Optional) Interface name. After typing this parameter, all neighbors on this interface will perform adjacent reset.

default

none

command mode

EXEC

instruction

All BEIGRP's neighbors will be reset without specifying any parameter.

The use of this command will lead adjacent reset of one or several neighbors, and then triggers routing operation. In the case when many routes are influenced, it may cause route fluctuation, and it needs some time to convergence again. So we recommend not to use this command unless the system is in the network debugging stage.

Example

The following example removes all neighbors on ethernet1/1 and triggers recalculation of the related routes:

clear ip beigrp ethernet1/1

53.1.3 debug ip beigrp

To trace BEIGRP protocol information, you can press this command in the privileged EXEC mode.

debug ip beigrp

1. **no debug ip beigrp**

parameter

none

default

none

command mode

EXEC

instruction

It helps to find network malfunction using this command.

Example

The following example removes all neighbors on Ethernet 1/1 and triggers recalculation of the related routes:

clear ip beigrp ethernet1/1

53.1.4 debug ip beigrp fsm

To trace the change of state machine of BEIGRP DUAL algorithm, use the debug ip beigrp fsm command in EXEC command.

debug ip beigrp fsm [**detail**]

parameter

parameter	description
detail	(Optional) Displays detailed information.

default

none

command mode

EXEC

instruction

It helps to find network malfunction using this command

related commands

debug ip beigrp packet

53.1.5 debug ip beigrp neighbors

To display the establishment and deletion of BEIGRP neighbors, use the debug ip beigrp neighbors command in EXEC mode.

debug ip beigrp neighbors

parameter

none

default

none

command mode

EXEC

instruction

It helps to find network malfunction using this command.

example

```
TestC#debug ip beigrp neighbors
BEIGRP: Neighbor 192.168.20.141 went down on Ethernet1/1 for peer restarted.
BEIGRP: Neighbor(192.168.20.141) not yet found.
BEIGRP: Neighbor(192.168.20.141) not yet found.
BEIGRP: New neighbor 192.168.20.141
BEIGRP: Neighbor 202.117.80.143 went down on Ethernet2/1 for manually cleared.
BEIGRP: Neighbor 192.168.20.141 went down on Ethernet1/1 for manually cleared.
BEIGRP: New neighbor 192.168.20.204
BEIGRP: New neighbor 202.117.80.143
```

BEIGRP: New neighbor 192.168.20.141

related commands

debug ip beigrp fsm

53.1.6 debug ip beigrp packet

To display BEIGRP packets situations, use the debug ip beigrp packet command in EXEC mode.

debug ip beigrp packets [**ack | hello | query | reply | retry | terse | update**]

no debug ip beigrp packets [**ack | hello | query | reply | retry | terse | update**]

parameter

parameter	description
ack	(Optional) Traces ACK pacekts
hello	(Optional) Traces hello packets.
query	(Optional) Traces query packets.
reply	(Optional) Traces reply packets
retry	(Optional) Traces retry packets.
terse	(Optional) Traces all packets except hello packets.
update	(Optional) Traces update packets.

default

none

command mode

EXEC

instruction

It helps to find network malfunction using this command.

example

router#debug ip beigrp packet
BEIGRP: Send HELLO packet to 224.0.0.10 via Ethernet2/1 with Ack 0/0
BEIGRP: Receive ACK packet from 192.168.20.141 via Ethernet1/1 with Ack 0/54
BEIGRP: Receive HELLO packet from 202.117.80.143 via Ethernet2/1 with Ack 0/0
BEIGRP: Receive UPDATE packet from 192.168.20.204 via Ethernet1/1 with Ack 142/0

BEIGRP: Send HELLO packet to 192.168.20.204 via Ethernet1/1 with Ack 0/142
BEIGRP: Receive HELLO packet from 192.168.20.141 via Ethernet1/1 with Ack 0/0
BEIGRP: Receive HELLO packet from 192.168.20.204 via Ethernet1/1 with Ack 0/0
BEIGRP: Receive QUERY packet from 192.168.20.204 via Ethernet1/1 with Ack 143/0
BEIGRP: Send HELLO packet to 192.168.20.204 via Ethernet1/1 with Ack 0/143
BEIGRP: Send REPLY packet to 192.168.20.204 via Ethernet1/1 with Ack 55/143
BEIGRP: Send UPDATE packet to 224.0.0.10 via Ethernet2/1 with Ack 57/0
BEIGRP: Receive ACK packet from 192.168.20.204 via Ethernet1/1 with Ack 0/55
BEIGRP: resend UPDATE packet for neighbor 192.168.20.204 with retry num 1.
BEIGRP: Receive ACK packet from 202.117.80.143 via Ethernet2/1 with Ack 0/57
BEIGRP: Send UPDATE packet to 202.117.80.143 via Ethernet2/1 with Ack 57/77
BEIGRP: Send UPDATE packet to 224.0.0.10 via Ethernet1/1 with Ack 56/0
BEIGRP: Receive ACK packet from 192.168.20.204 via Ethernet1/1 with Ack 0/56
BEIGRP: Send UPDATE packet to 192.168.20.141 via Ethernet1/1 with Ack 56/88
BEIGRP: Send UPDATE packet to 192.168.20.204 via Ethernet1/1 with Ack 56/143
BEIGRP: Receive UPDATE packet from 202.117.80.143 via Ethernet2/1 with Ack 79/0
BEIGRP: Send HELLO packet to 202.117.80.143 via Ethernet2/1 with Ack 0/79
BEIGRP: Receive ACK packet from 192.168.20.204 via Ethernet1/1 with Ack 0/56
BEIGRP: Send QUERY packet to 224.0.0.10 via Ethernet1/1 with Ack 60/0
BEIGRP: Send UPDATE packet to 224.0.0.10 via Ethernet1/1 with Ack 61/0

FIeld	Description
Recv / Send / Enqueueing	Receives, sends or enqueueings packet to send -queue
HELLO / UPDATE / QUERY / ACK	Packet types that are received or sent.
192.1.1.1	Neighbor IP address to send packet
Serial1/2	In or out interface of packet
Ack 56/88	Acknowledgement number of packet/ sequence number of neighbor packet

related commands

debug ip beigrp fsm

To display transmit event of BEIGRP packet, use the debug ip beigrp transmit command in EXEC mode.

debug ip beigrp transmit [**ack | build | link | packetize | peerdown | startup**]

no debug ip beigrp transmit [**ack | build | link | packetize | peerdown | startup**]

parameter

parameter	description
ack	(Optional) Traces events
build	(Optional)Traces BUILD events.
link	(Optional)Traces LINK events
packetize	(Optional)Traces PACKETIZE events.
peerdown	(Optional)Traces PEERDOWN events
startup	(Optional)Traces STARTUP events.

default

none

command mode

EXEC

instruction

It helps to find network malfunction using this command.

related commands

debug ip beigrp fsm

53.1.8 default-metric

To reset the default vector metric for the Enhanced Interior Gateway Routing Protocol (BEIGRP), use the default-metric command in routing switch configuration mode. To restore the default state, use the no form of this command.

default-metric bandwidth delay reliability loading mtu

no default-metric

parameter

parameter	description
bandwidth	Default bandwidth
delay	Default interface delay.
reliability	Default interface reliability
loading	Default interface load

mtu	The default value for the maximum transmission unit (MTU),

default

bandwidth: 128kpbs

delay: 2000 (10ms)

reliability: 255 (255 indicates 100%)

loading: 255 (255 indicates 100%)

mtu: 1500

command mode

router configuration

instruction

it is generally used with redistribute command to specify default metrics of route of other routing protocols assigned into BEIGRP. This command will trigger the new algorithm of related route that are previously assigned into BEIGRP.

Forwarding static route, straight connected route and BEIGRP protocol route, you can not configure default-metric command, or you must configure this command

Example

The following example shows how the redistributed Routing Information Protocol (RIP) metrics are translated into EIGRP metrics with values as follows: bandwidth = 200, delay = 100, reliability = 100, loading = 200, and MTU = 1500:

default-metric 200 1000 100 200 1500

related commands

redistribute

53.1.9 distance

To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the distance beigrp command in routing switch configuration mode. To reset these values to their defaults, use the no form of this command.

distance beigrp internal-distance external-distance

no distance beigrp

distance weight *ip-address ip-address-mask* [*ip-access-list*]

no distance weight *ip-address ip-address-mask* [*ip-access-list*]

parameter

parameter	description
internal-distance	Administrative distance for Enhanced Internal Gateway Routing Protocol (BEIGRP) internal routes. The distance can be a value from 1 to 255.
external-distance	Administrative distance for EIGRP external routes. The distance can be a value from 1 to 255.
ip-address	BEIGRP neighbor IP address
ip-address-mask	BEIGRP neighbor IP address mask
ip-access-list	BEIGRP neighbor access list

default

internal-distance: 90

external-distance: 170

command mode

router configuration

instruction

An administrative distance is to compare the priority of routes of different protocols. Therefore, adjustment on the administrative distance value of BEIGRP will affect the choice of routing switch to meet different demands od users

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list.

Example

```
router beigrp 2
network 192.10.0.0 255.255.0.0
distance beigrp 100 200
distance 110 192.31.7.0 255.255.255.0
distance 220 128.88.1.0 255.255.255.0
```

In the above example, the routing switch beigrp global configuration command sets up BEIGRP internal administrative and external administrative to 100 and 200. The network routing switch configuration commands specify BEIGRP routing on networks 192.31.7.0/24 and 128.88.1.0/24 to 110 and 220.

related commands

show ip protocol

53.1.10 filter

To allows us to filter the routes that learned or sent on the specified interface, use the filter command. Use the no form of this command to disable filter.

filter {*interface*-type *interface*-number | *} {**in** | **out**} {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

no filter {*interface*-type *interface*-number | *} {**in** | **out**} {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

parameter

parameter	description
interface-type interface-number	Interface type and number
*	all intefaces
in	Applies access-list to the incoming routing update
out	Applies access-list to the ourcoming routing update
access-list	Applies standard access list to filter routes, to define which network is sent and which network is suppressed in routing update.
gateway	Filters gateway of route using standard access list.
access-list-name	Standard IP access list number or name
prefix-list	Filters route using the prefix-list
prefix-list-name:	Standard IP prefix- list-name. This list defines which networks are received and which are surpressed.

default

none

command mode

router configuration

instruction

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list.

example

The following example permits only one network at 131.108.0.0 to be declared by BEIGRP routing process:

```
access-list 1 permit 131.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router beigrp 64
network 131.108.0.0
filter * out 1
```

53.1.11 beigrp log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (BEIGRP) neighbor adjacencies, use the beigrp log-neighbor-changes command in router configuration mode. To disable the logging of changes in BEIGRP neighbor adjacencies, use the no form of this command.

beigrp log-neighbor-changes

no beigrp log-neighbor-changes

parameter

none0

default

disabled

command mode

router configuration

53.1.12 beigrp router-id

To set the routing switch ID used by Enhanced Interior Gateway Routing Protocol (BEIGRP), use the eigrp router-id command in router configuration mode. To remove the configured routing switch ID, use the no form of this command.

beigrp router-id *ip-address*

no beigrp router-id

parameter

parameter	description
ip-address	Router ID in dotted decimal notation.

default

EIGRP automatically selects an IP address to use as the routing switch ID. Set the largest loopback interface as the routing switch ID if there is a loopback interface or set the largest direct-connect interface address as the the routing switch ID.

command mode

router configuration

53.1.13 ip beigrp bandwidth-percent

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (BEIGRP) on an interface, use the ip bandwidth-percent eigrp command. To restore the default value, use the no form of this command.

ip beigrp bandwidth-percent *percent*

no ip beigrp bandwidth-percent *percent*

parameter

parameter	description
percent	Percent of bandwidth that EIGRP may use.

default

50％

command mode

interface configuration mode

instruction

For low speed lines, you can adjust the configuration of this command to restrict the enabled bandwidth for BEIGRP to avoid that BEIGRP affect the normal data transmission. .

Example

interface Ethernet1/1
ip beigrp bandwidth-percent 100

The above example allows BEIGRP to use all bandwidth of the interface

related commands

bandwidth

53.1.14 ip beigrp hello-interval

To configure the hello interval for an Enhanced Interior Gateway Routing Protocol (BEIGRP) process, use the ip hello-interval eigrp command in interface configuration mode. To restore the default value, use the no form of this command.

ip beigrp hello-interval *seconds*

no ip beigrp hello-interval *seconds*

parameter

parameter	description
second	Hello interval (in seconds).

default

5 seconds-

command mode

interface configuration mode

instruction

example

interface Ethernet1/1
ip beigrp hello-interval 20

The above example sets 20 seconds as the hello interval for ethernet1/1:

related commands

ip beigrp hold-time

53.1.15 ip beigrp hold-time

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (BEIGRP) process, use the ip hold-time eigrp command in interface configuration mode. To restore the default value, use the no form of this command.

ip beigrp hold-time *seconds*

no ip beigrp hold-time *seconds*

parameter

parameter	description
second	Hold time is in seconds if do not receive any BEIGRP

default

15 seconds

command mode

interface configuration mode

instruction

example

interface Ethernet1/1
ip beigrp hold-time 60

The above example sets 60 seconds the hold time for ethernet1/1:

related commands

ip beigrp hello-interval

53.1.16 ip beigrp passive

To enable interacting BEIGRP routing update on a certain interface, use the ip beigrp passive command. Use the no form of this command to restore the default value.

ip beigrp passive

no ip beigrp passive

parameter

none

default

the interface is not in passive mode

command mode

interface configuration mode

instruction

If the ip beigrp passive is configured on an interface, then no routing update is received on this interface, and also no neighborhood relation is established between this interface and any accessible neighbors. But a direct route genereate on this interface will be broadcast by other interface that runs the BEIGRP.

example

The following command set ethernet1/1 as the passive interface:

```
interface ethernet1/1
ip beigrp passive
```

53.1.17 ip beigrp split-horizon

To enable Enhanced Interior Gateway Routing Protocol (BEIGRP) split horizon, use the ip beigrp split-horizon command in interface configuration mode. To disable split horizon, use the no form of this command.

ip beigrp split-horizon

no ip beigrp split-horizon

parameter

none

default

The behavior of this command is enabled by default.

command mode

interface configuration mode

instruction

Using this command is to prevent route cycle, so you must confirm that it will not cause any bad effects before turn off the split horizon.

example

interface Ethernet1/1
no ip beigrp split-horizon

The above example disables split horizon on ethernet 1/1:

53.1.18 ip beigrp summary-address

To configure a summary aggregate address for a specified interface, use the ip beigrp summary-address command in interface configuration mode. To disable a configuration, use the no form of this command.

ip beigrp summary-address *as_number address mask*

no ip beigrp summary-address *as_number address mask*

parameter

parameter	description
as_number	Autonomous system number.
address	Summary IP address to apply to an interface.
mask	Subnet mask.

default

none

command mode

interface configuration mode

instruction

The following is default behavior if an incomplete configuration is entered:

When the ip beigrp summary-address command is configured on an interface, the summary routes of the defined network are generated as if there is a subnet in BEIGRP topology table.

The summary routes point to Null0 interface, which have the minimum distance of all the concrete routes that summary routes contain. The summary routes insert to the main IP routing table, and the administrative distance is 5(which cannot be configured).

Configuring the sending of routing updates on an interface in the rummary routes range cancels concrete routes that belong to the summary network. The update sent to the other interfaces is not affected.

example

an administrative distance of 95 on interface Ethernet 0/0 for the 192.168.0.0/16 summary address:

interface Ethernet1/1

ip beigrp summary-address 100 12.1.0.0 255.255.0.0

The above example configures all the concrete routes that belong to the network 12.1.0.0/16(which belong to router beigrp 100) not to be broadcast on ethernet1/1

related commands

auto-summary

53.1.19 metric weights

To tune Enhanced Interior Gateway Routing Protocol (BEIGRP) metric calculations, use the metric weights command in routing switch configuration mode. To reset the values to their defaults, use the no form of this command

metric weights k1 k2 k3 k4 k5

no metric weights

parameter

parameter	description
k1,k2,k3,k4,k4	Constants that convert an EIGRP metric vector into a scalar quantity.

default

k1: 1

k2: 0

k3: 1

k4: 0

k5: 0

command mode

router configuration

instruction

Use this command to alter the default behavior of EIGRP routing and metric computation and allow the tuning of the EIGRP metric calculation for a particular type of service (ToS).

The tuning of the EIGRP metric calculation for a composite metric adopts two steps:

If k5 equals 0, the composite EIGRP metric is computed according to the following formula:

metric = [k1 * bandwidth + (k2 * bandwidth)/(256 - load) + k3 * delay]

If k5 does not equal zero, an additional operation is performed:

Composite metric = Composite metric * [k5/(reliability + k4)]

K2, K4 and K5 are the left objects of IGRP, compatible with Eigrp protocol of Cisco. In general, Load and Reliability are not used in composite metric algorithm. Therefore, do not change the default value of K2, K4 and K5, unless you confirm that will not cause bad effect, to prevent unexpected result on route decision

example

```
router beigrp 2
network 131.108.0.0 255.255.0.0
metric weights 2 0 2 0 0
```

related commands

bandwidth

delay

53.1.20 network

To specify the network for an Enhanced Interior Gateway Routing Protocol (BEIGRP) routing process, use the network command in routing switch configuration mode. To remove an entry, use the no form of this command.

network *network-number* [*netmask*]

no network *network-number* [*netmask*]

parameter

parameter	description
network-number	Network address.
netmask	Network mask.

default

none

command mode

router configuration

instruction

Various network statements (network commands) can be configured on a routing switch, to enable BEIGRP dynamic routing protocol to run on many networks; use the default mask if there is no configured mask.

example

router beigrp 2
network 131.108.0.0 255.255.0.0
network 122.11.2.0

related commands

router beigrp

53.1.21 offset

To add an offset to incoming and outgoing metrics to routes learned via Enhanced Interior Gateway Routing Protocol (BEIGRP), use the offset command in router configuration mode. To remove an offset list, use the no form of this command.

offset {**type** *number* **| ***} {**in | out**} *access-list-name* **offset**

no offset {**type** *number* | *****} {**in | out**}

parameter

parameter	description
In	Applies the access list to incoming metrics.
Out	Applies the access list to outgoing metrics.
access-list-name	Standard access list name to be applied
Offset	Positive offset to be applied to metrics for networks matching the access list.
Type	(Optional) Interface type to which the offset list is applied.
Number	(Optional) Interface number to which the offset list is applied.

default

none

command mode

router configuration

instruction

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

BEIGRP is a vector metric, so the offset is added to delay

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list

example

In the following example, the router applies an offset of 10 to the delay component of the router only to access list 21:

offset * out 21 10

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0:

offset e0/0 in 21 10

related commands

ip access-list

53.1.22 redistribute

To redistribute routes from other routing protocols into the local BEIGRP routing process routing table, use the redistribute command.

redistribute protocol [**process**] **route-map** *name*

redistribute protocol [**process**]

parameter

parameter	description
protocol	Source protocol from which routes are being redistributed. It must be one of following keywords: bgp, ospf, static , connected, and rip.
process	(Optional) For bgp or bigp, this parameter indicates the 16-digit autonomous number. For OSPF, this parameter indicates the relevant OSPF process ID of the routes need to be redistributed. This marks the rouing process. It is a non-zero decimal number. For rip, there is no need to mark the process.
route-map	(Optional) Identifier of a configured route map. The route map should be examined to filter the importation of routes from this source routing protocol to IS-IS. If not specified, all routes are redistributed. If the keyword is specified, but no route map tags are listed, no routes will be imported.
name	Name character string of route-map

default

none

command mode

BEIGRProuter configuration

instruction

To redistribute direct routes, static routes and routes from other BEIGRP process, the default-metric command is not necessarily to be configured;otherwise, the default-metric must be configueid.

example

default-metric 64 250 255 255 1500
redistribute ospf 1

53.1.23 router beigrp

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the router beigrp command in global configuration mode. To delete the BEIGRP routing process, use the no form of this command.

router beigrp *autonomous-system-number*

no router beigrp *autonomous-system-number*

parameter

parameter	description
autonomous-system-number	Autonomous system number that identifies the routes to the other BEIGRP routers.

default

none

command mode

global configuration mode

instruction

This command can be used to operate multiple BEIGRP processes.

example

The following example configures EIGRP process 30:

router beigrp 30

related commands

network

53.1.24 show ip beigrp interface

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the show ip beigrp interfaces command in privileged EXEC mode.

show ip beigrp interfaces [**interface-type** *interface-number*] [*as-number*]

parameter

parameter	description
as-number	Autonomous system number. If the parameter is specified, it will display only the neighbour of BEIGRP process
interface	Interface name. If the parameter is specified, it will display only the neighbour on this BEIGRP interface

default

none

command mode

EXEC or global configuration mode

instruction

Use the show ip eigrp interfaces command to learn information about BEIGRP dynamic routing relating to those interfaces.

related commands

show ip beigrp topology

53.1.25 show ip beigrp neighbors

To display neighbors discovered by Enhanced Interior Gateway Routing Protocol (BEIGRP), use the show ip eigrp neighbors command in EXEC mode.

show ip beigrp neighbors [*interface-type interface-number*] [*as-number*] [*detail*]

parameter

parameter	description
as-number	Autonomous system number. If the parameter is specified, it will display only the neighbour of BEIGRP process
interface	Interface name. If the parameter is specified, it will display only the neighbour on this BEIGRP interface
detail	Displays detailed neighbor information.

default

none

command mode

EXEC or global configuration mode

instruction

Use the show ip beigrp neighbors command to determine what neighbours they are and when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

example

```
Router# show ip beigrp neighbors
Information of BEIGRP neighbors with AS 1024
Address         interface     hold   uptime    Q_cnt   Seq
192.168.20.204  Ethernet1/1   15   00:08:06    0     159
202.117.80.143  Ethernet2/1   10   00:08:05    0     100
192.168.20.141  Ethernet1/1   12   00:07:38    0     254
```

field	explanation
AS 64	Autonomous system number
Address	IP address of the BEIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Hold	Length of time that the software will wait to hear from the peer before declaring it down.
Uptime	Elapsed time since the local router first heard from this neighbor.
Q Count	Number of EIGRP packets that the software is waiting to send.
Seq	Sequence number of the last update that was received from this neighbor.

related commands

show ip beigrp topology

53.1.26 show ip beigrp protocol

To display the Enhanced Interior Gateway Routing Protocol (BEIGRP) routing protocol process parameter and statistics, use the show ip beigrp protocols command.

show ip beigrp protocols [*as-number*]

parameter

parameter	description
as-number	(Optional) Autonomous system number. If the parameter is specified, it will display only the parameters and statistics of this BEIGRP process

command mode

EXEC or global configuration mode

instruction

This command can be used to check BEIGRP topology table at any time.

example

```
R142#show ip bei pro
Protocol Information of BEIGRP with AS 1024:
  Metric Weight: K1=1, K2=0, K3=1, K4=0, K5=0.
  Filter * in access-list in12
  Filter * out access-list ou12
  Offset * in in23 12
  Offset * out ou23 12
  Redistributing: connect, ospf 1, ospf 2
  Automatic network summarization is enable.
  Active-time: 3(minutes)
  Routing for Networks:
192.168.20.0/24
    10.0.0.0/8
    167.20.0.0/16
    202.117.80.0/24
  Distance: internal 90, external 170
  Active Route:
```

related commands

show ip beigrp topology

53.1.27 show ip beigrp topology

To display entries in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the show ip beigrp topology command in privileged EXEC mode.

show ip beigrp topology [*as-number*] [*network-number subnet-mask* |*active* | *all-links* | *pending* | *summary* | *zero-successors*]

parameter

parameter	description
as-number	(Optional) Autonomous system number. If the parameter is specified, it will display only the topology table of BEIGRP process
network-number	Displays detailed information about the specified network.
subnet-mask	(Optional) Subnet mask.
active	(Optional) Displays only active entries in the BEIGRP topology table.
all-link	(Optional) Displays all entries in the BEIGRP topology table.
pending	(Optional) Displays all entries in the BEIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays a summary of the BEIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table.

default

none

command mode

EXEC or global configuration mode

instruction

This command can be used to check BEIGRP topology table at any time.

example

```
Router# show ip beigrp topology
P 10.10.10.0/24 successors: 1 FD: 13056
        via connect(Loopback1) Metric: 13056/0
P 167.20.0.0/16 successors: 1 FD: 261132
        via 202.117.80.143(Ethernet2/1) Metric: 261132/258560
P 192.166.100.0/24 successors: 1 FD: 281856
        via redistribute Metric: 281856/0
P 192.168.20.0/24 successors: 1 FD: 258560
```

via connect(Ethernet1/1) Metric: 258560/0
P 202.1.1.0/24 successors: 1 FD: 297246988
via 192.168.20.204(Ethernet1/1) Metric: 297246988/297244416
P 202.117.80.0/24 successors: 1 FD: 258560
via connect(Ethernet2/1) Metric: 258560/0
A 202.117.93.0/24 successors: 1 FD: unaccessible, R serno: 32
via 192.168.20.141(Ethernet1/1) Metric: 271372/13056
SIA-Info: (active: 00:02:20 query-origin: Local origin)
Unreplied Neighbors:
via 202.117.80.143, Ethernet2/1
P 202.192.168.0/24 successors: 1 FD: 284172
via 192.168.20.204(Ethernet1/1) Metric: 284172/281600

field	description
160.89.90.0 and so on	Destination network number
255.255.255.0	Destination network mask
successors	Number of successors.
FD	Feasible distance.
Via	Gateway address
Ethernet1/1	Interface from which this information was learned.
SIA-Info	active routing information
active	Lasting time when entering Active status.
query-origin	Origin of entering query state
Unreplied Neighbors	Neighbor lists that are not received reply.

related commands

show ip beigrp neighbor

53.1.28 show ip beigrp traffic

To display the flow information of Enhanced Interior Gateway Routing Protocol (BEIGRP) packets sent and received, use the show ip beigrp traffic command in EXEC mode.

show ip beigrp traffic [*as-number*]

parameter

parameter	description
as-number	(Optional) Autonomous system number. If the parameter is specified ,then display the flow statistics information

default

none

command mode

EXEC or global configuration mode

instruction

Use this command to check the flow statistics information of BEIGRP packets sent and received at any time.

example

```
R142#show ip bei tra
Traffic Statistics of BEIGRP 1024
Packet Type      Hello     Update    Query     Reply     ACK
Send/Receive     770/1021  133/44    29/7      7/9       60/147
```

related commands

show ip beigrp topology

Chapter 54 OSPF Configuration Commands

54.1 OSPF Configuration Commands

OSPF Configuration Commands Include:

- area authenticaion
- area default-cost
- area range
- area stub
- area virtual-link
- debug ip ospf adj
- debug ip ospf events
- debug ip ospf flood
- debug ip ospf lsa-generation
- debug ip ospf packet
- debug ip ospf retransmission
- debug ip ospf spf
- debug ip ospf tree
- default-information originate
- default-metric
- distance ospf
- filter
- ip ospf cost
- ip ospf dead-interval
- ip ospf hello-interval
- ip ospf message-digest-key
- ip ospf network
- ip ospf passive

- ip ospf password
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- neighbor
- network area
- redistribute
- router ospf
- show ip ospf
- show ip ospf border-routers
- show ip ospf database
- show ip ospf interface
- show ip ospf neighbor
- show ip ospf virtual-link
- summary-address
- timers delay
- timers hold

54.1.1 area authentication

To enable authentication for an Open Shortest Path First (OSPF) area, use the area authentication command in routing switch configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the no form of this command.

area *area-id* **authentication** [**simple | message-digest**]

no area *area-id* **authentication**

no area *area-id*

parameter

parameter	description
area-id	Identifier of the area for which authentication is to be enabled.

simple	(Optional)authentication information, Plain text authentication
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the area-id argument.

default

no authentication of interface receiving OSPF packet by default

command mode

router configuration

instruction

The authentication value will be added into OSPF packet.The authentication type of all routing swithces in the same area must be the same.The authentication password for all OSPF routing switches on a network must be the same if they are to communicate with each other via OSPF..

example

The following example mandates authentication simple for areas 0 and 36.0.0.0.

```
interface ethernet 1/0
ip address 131.119.251.201 255.255.255.0
ip ospf password adcdefgh
!
interface ethernet 1/0
ip address 36.56.0.201 255.255.0.0
ip ospf password ijklmnop
!
router ospf 1
network 36.0.0.0 255.0.0.0 area 36.0.0.0
network 131.119.0.0 255.255.0.0 area 0
area 36.0.0.0 authentication simple
area 0 authentication simple
```

related commands

ip ospf password

ip ospf message-digest-key

54.1.2 area default-cost

To specify a cost for the default summary route that is sent into a stub area or not-so-stubby area (NSSA), use the area default-cost command in router address

family topology or routing switch configuration mode. To remove the assigned default route cost, use the no form of this command.

area *area-id* **default-cost cost**

no area *area-id* **default-cost**

no area *area-id*

parameter

parameter	description
area-id	Identifier for the stub area.
cost	Cost for the default summary route used for a stub

default

cost.1

command mode

router configuration

instruction

This command is used only on an routing switch attached to a stub area or NSSA.

After configured the area stub default-information-originate command, the routing switch will send LSA(SUM-NER-LSA) including default router information to correspondent field, the cost configured I this command is the correspondent cost used in LSA.

Note:

To remove the specified area from the software configuration, use the no area area-id command (without other keywords). That is, the no area area-id command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
interface ethernet 1/0
ip address 36.56.0.201 255.255.0.0
!
```

router ospf 201
network 36.0.0.0 255.0.0.0 area 36.0.0.0
area 36.0.0.0 stub
area 36.0.0.0 default-cost 20

related commands

area nssa

area stub

54.1.3 area range

To consolidate and summarize routes at an area boundary, use the area range command. To disable this function, use the no form of this command.

area *area-id* **range** *address mask*[**not-advertise**]

no area *area-id* **range** *address mask* **not-advertise**

no area *area-id* **range** *address mask*

no area *area-id*

parameter

parameter	description
area-id	Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IPv6 prefix.
address	IP address
mask	IP address mask
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

default

This command is disabled by default.

command mode

router configuration

instruction

The area range command is used only with Area Border Routing switches. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization.

Multiple area range routing switch configuration commands can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Note: To remove the specified area from the software configuration, use the no area area-id command (with no other keywords). That is, the no area area-id command removes all area options, such as area default-cost, area nssa, area range, area stub, and area virtual-link.

example

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 36.0.0.0 and for all hosts on network 192.42.110.0:

```
interface ethernet 0
ip address 192.42.110.201 255.255.255.0
!
interface ethernet 1
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
network 36.0.0.0 255.0.0.0 area 36.0.0.0
network 192.42.110.0 255.0.0.0 area 0
area 36.0.0.0 range 36.0.0.0 255.0.0.0
area 0 range 192.42.110.0 255.255.255.0
```

54.1.4 area stub

To define an area as a stub area, use the area stub command. To disable this function, use the no form of this command.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub**

no area *area-id*

parameter

parameter	description
area-id	Identifier for the stub area; either a decimal value or an IP address.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

default

No stub area is defined.

command mode

router configuration

instruction

You must configure the area stub command on all routers and access servers in the stub area. Use the area router configuration command with the default-cost keyword to specify the cost of a default internal route sent into a stub area by an ABR switch.

There are two stub area router configuration commands: the stub and default-cost options of the area routing switch configuration command. In all routing switches attached to the stub area, the area should be configured as a stub area using the stub keyword of the area command. Use the default-cost keyword only on an ABR attached to the stub area. The default-cost keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the no-summary keyword on the ABR switch to prevent it from sending summary LSAs (LSA type 3) into the stub area.

Note: To remove the specified area from the software configuration, use the no area area-id command (with no other keywords). That is, the no area area-id command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
interface ethernet 0
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
```

network 36.0.0.0 255.0.0.0 area 36.0.0.0
area 36.0.0.0 stub
area 36.0.0.0 default-cost 20

related commands

area authentication

area default-cost

54.1.5 area virtual-link

To define a virtual link, use the area virtual-link command

area *area-id* **virtual-link** *neighbor-ID* [**authentication** simple | message-digest] [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transdly** *dly-value*][**password** *pass-string*] [message-digest-key key-id MD5 md5-string]

no area *area-id* **virtual-link** *neighbor-ID*

parameter

parameter	description
area-id	Area ID assigned to the transit area for the virtual link.
neighbor-id	Router ID associated with the virtual link neighbor.
simple	Plain text authentication. The value must be the same for all routing switches and access servers attached to a common network.
message-digest	Enables Message Digest 5 (MD5) on virtual-link. The value must be the same for all routing switches and access servers attached to a common network.
dead-value	Time (in seconds) that hello packets are not seen before a neighbor declares the router down. The value must be the same for all routing switches and access servers attached to a common network.
hello-value	Time (in seconds) between the hello packets that the software sends on an interface. The value must be the same for all routing switches and access servers attached to a common network.
retrans-value	Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The value must be the same for all routing switches and access servers attached to a common network.
dly-value	Delay value in seconds to inform LSA on virtual-link for a routing switch. The configured value on both sides of the virtual-link should be the same.
pass-string	If virtual-link uses plain text authentication, the the maximum character of the configured password should be 8. The configuied value on both sides of the virtual-link should be the same.

key-id	If virtual-link uses MD5 authentication, the valid range of the used MD5 key should from 1 to 255. The configured value on both sides of the virtual-link should be the same.
MD5-String	Configures MD5 password, which is 16-character at most. The configured value on both sides of the virtual-link should be the same.

default

No virtual-link is configured.

Default value of other parameters are as follows:

Hello-value: 10s, Dead-value : 40s, Retrans-value : 5s, dly-value : 1s, no authentication

command mode

OSPFrouter configuration

instruction

To establish a virtual link, user should configure both sides of the virtual link. The virtual link will fail if this command is only configured on one side.

The parameter-id must be a non-zero character, for the virtual link and the transit areda must be a non-backbone area. The configured area-id of the virtual link must be the same.

The neighbor-ID must be the same as the ospf router-id on the remote side during configuration, or the virtual link will not be established. Even if the configured neighbor-ID is another IP address of the other side.

You must make sure that all parameters on both sides must be the same.

The authentication parameters that configured on virtual-link become effective only when configured authentication types of virtual-link or configured the relevant authentication methods in backbone are (via the command area authentication)Only one kind of authentication parameter can be configured on virtual-link, that is, the MD5 and the plain text authenticationm are mutually exclusive.

Use the command no area area-id veitual-link neighbor-ID to cancel the formerly-configured virtual link.

Use the command show ip ospf virtual-link to check state of the virtual link.

example

The following example configured a virtual link between router A and router B:

The configuration on router A (router-id: 200.200.200.1)

!

router ospf 100
network 192.168.20.0 255.255.255.0 area 1
area 1 virtual-link 200.200.200.2
!

The configuration on router B :

!
router ospf 100
network 192.168.30.0 255.255.255.0 area 1
area 1 virtual-link 200.200.200.1
!

related commands

show ip ospf virtual-link

54.1.6 debug ip ospf adj

To monitor Open Shortest Path First (OSPF)-related estabilishment process , use the debug ospf adj command

debug ip ospf adj

parameter

none

default

none

command mode

EXEC

instruction

User can check the process of OSPF-related estabilishment process from the output of this command.

example

Router# debug ip ospf adj
OSPF: Interface 192.168.40.0 on Serial1/0 going down
OSPF NBR: 192.168.40.2 address 192.168.40.2 on Serial1/0 is dead, state DOWN
OSPF NBR: 192.168.40.3 address 192.168.40.3 on Serial1/0 is dead, state DOWN
Line on Interface Serial1/0, changed state to up

Line protocol on Interface Serial1/0 changed state to up
OSPF: Interface 192.168.40.0 on Serial1/0 going Up
OSPF: 2 Way Communication to 192.168.40.2 on Serial1/0, state 2WAY
OSPF: NBR 192.168.40.2 on Serial1/0 Adjacency OK, state NEXSTART.
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: NBR 192.168.40.2 on Serial1/0 Negotiation Done. We area the SLAVE
OSPF: Exchange Done with 192.168.40.2 on Serial1/0
OSPF: Loading Done with 192.168.40.2 on Serial1/0, database Synchronized (FULL)
OSPF: 2 Way Communication to 192.168.40.3 on Serial1/0, state 2WAY
OSPF: NBR 192.168.40.3 on Serial1/0 Adjacency OK, state NEXSTART.
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: NBR 192.168.40.3 on Serial1/0 Negotiation Done. We area the SLAVE
OSPF: Bad Sequence with 192.168.40.3 on Serial1/0, state NEXSTART
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: NBR 192.168.40.3 on Serial1/0 Negotiation Done. We area the SLAVE
OSPF: Exchange Done with 192.168.40.3 on Serial1/0
OSPF: Loading Done with 192.168.40.3 on Serial1/0, database Synchronized (FULL)
……

54.1.7 debug ip ospf events

To monitor OSPF interface and OSPF-related events, , use the debug ip ospf events command.

debug ip ospf events

parameter

none

default

none

command mode

EXEC

instruction

To display OSPF interface and OSPF-related adjacency events from the ouput of this command.

example

Router# debug ip ospf events
OSPF: Interface Serial1/0 going Up

OSPF: INTF(192.168.40.0) event INTF_UP
OSPF: NBR(192.168.40.2) event HELLO_RX
OSPF: NBR(192.168.40.2) event TWOWAY
OSPF: NBR(192.168.40.2) event ADJ_OK
OSPF: NBR(192.168.40.2) event NEGO_DONE
OSPF: NBR(192.168.40.2) event EXCH_DONE
OSPF: NBR(192.168.40.2) event LOAD_DONE
OSPF: NBR(192.168.40.3) event HELLO_RX
OSPF: NBR(192.168.40.3) event TWOWAY
OSPF: NBR(192.168.40.3) event ADJ_OK
OSPF: NBR(192.168.40.3) event NEGO_DONE
OSPF: NBR(192.168.40.3) event SEQ_MISMATCH
OSPF: NBR(192.168.40.3) event NEGO_DONE
OSPF: NBR(192.168.40.3) event EXCH_DONE
OSPF: NBR(192.168.40.3) event LOAD_DONE
……

54.1.8 debug ip ospf flood

To display OSPF-related database pervasion process, use the debug ip ospf flood command.

debug ip ospf flood

parameter

none

default

none

command mode

EXEC

instruction

To display OSPF-related database pervasion process from the output of this command.

example

Router# debug ip ospf flood
OSPF: recv UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 2 SEQ 0x8000022B

OSPF: Send UPDATE, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000234

OSPF: Send ACK, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 2 SEQ 0x8000022B

OSPF: recv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000234

OSPF: recv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 18 SEQ 0x80000233

OSPF: Send UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 10 SEQ 0x8000022B

OSPF: recv UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 5 SEQ 0x8000021C

OSPF: Send UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 6 SEQ 0x8000021C

OSPF: Send UPDATE, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000235

OSPF: recv ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 4 SEQ 0x8000021C

……

54.1.9 debug ip ospf lsa-generation

To display OSPF-related LSA generation process, use the debug ip ospf lsa generation command.

debug ip ospf lsa-generation

parameter

none

default

none

command mode

EXEC

instruction

To display OSPF interface and adjacency events from the output of this command.

example

router# debug ip ospf lsa-generation

……

OSPF: Send UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 10 SEQ 0x8000022D

OSPF: recv UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 5 SEQ 0x8000021E

OSPF: Send UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 6 SEQ 0x8000021E

OSPF: Send UPDATE, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000239

OSPF: recv ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 4 SEQ 0x8000021E

OSPF: Send ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 5 SEQ 0x8000021E

OSPF: recv UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 1 SEQ 0x8000022E

OSPF: Send UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 2 SEQ 0x8000022E

OSPF: recv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000239

OSPF: recv ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 6 SEQ 0x8000021E

OSPF: recv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000239

……

54.1.10 debug ip ospf packet

To display OSPF packets, use the debug ip ospf packet command.

debug ip ospf packet

parameter

none

default

none

command mode

EXEC

instruction

To display OSPF interface and adjacency events from the output of this command.

example

router# debug ip ospf packet

OSPF: Recv HELLO packet from 192.168.40.3 (addr: 192.168.40.3) area 0 from Serial1/0

OSPF: End of hello processing

OSPF: Send HELLO to 224.0.0.5 on Loopback0

HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44

OSPF: Send HELLO to 224.0.0.5 on Loopback0
HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44
OSPF: Send HELLO to 224.0.0.5 on Loopback0
HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44
OSPF: Recv HELLO packet from 192.168.40.2 (addr: 192.168.40.2) area 0 from Serial1/0
OSPF: End of hello processing
OSPF: Send HELLO to 224.0.0.5 on Serial1/0
HelloInt 30 Dead 120 Opt 0x2 Pri 1 len 52
OSPF: Recv HELLO packet from 192.168.40.3 (addr: 192.168.40.3) area 0 from Serial1/0
OSPF: End of hello processing
OSPF: Send HELLO to 224.0.0.5 on Loopback0
HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44
……

54.1.11 debug ip ospf retransmission

To display retransmission of OSPF paceket, uset the debug ip ospf retransmission command;

debug ip ospf retransmission

parameter

none

default

none

command mode

EXEC

instruction

To display transmission processo OSPF packets.

example

router# debug ip ospf retransmission
OSPF: retransmit UPDATE to 192.168.40.3 (RID 192.168.40.3), state FULL
……

54.1.12 debug ip ospf spf

To display information of SPF algorithm, use the debug ip ospf spf statistic command

debug ip ospf spf statistic

debug ip ospf spf

debug ip ospf spf intra

debug ip ospf spf inter

debug ip ospf spf external

parameter

none

default

none

command mode

EXEC

instruction

The debug ip ospf spf statistic command displays the OSPF routes calculation process.

example

router# debug ip ospf spf
OSPF: run ospf_spf_run
OSPF: start doing SPF for AREA 0.0.0.0
OSPF: RTAB_REV(ospf) 1390.
OSPF : Initializing to do SPF
OSPF: addroute LSID 192.168.20.240
OSPF: ospf_nh_find: 192.168.40.2
……
OSPF: addroute LSID 192.168.40.3
OSPF: build a OSPF_ROUTE, dest: 192.168.40.3
OSPF: addroute LSID 192.168.40.2
……
OSPF: SPF Area A running Network Summary
OSPF: Processing LS_SUM_NET 192.168.40.24, mask 255.255.255.248, adv 192.168.40.3, age 599
OSPF: addroute LSID 192.168.40.24
OSPF: ospf_build_route RT 192.168.40.24

OSPF: build route 192.168.40.24(255.255.255.248).
……
OSPF: Processing LS_SUM_NET 1.1.1.1, mask 255.255.255.255, adv 192.168.20.240, age 228
OSPF: addroute LSID 192.168.20.236
OSPF: build a OSPF_ROUTE, dest: 192.168.20.236
OSPF: start Building AS External Routes
OSPF: processing LS_ASE 192.168.42.0, mask 255.255.255.248, adv 192.168.20.236, age 258
OSPF: addroute LSID 192.168.42.0
OSPF: ospf_build_route RT 192.168.42.0
OSPF: build route 192.168.42.0(255.255.255.248).
OSPF: processing LS_ASE 192.168.43.0, mask 255.255.255.0, adv 192.168.20.236, age 258
OSPF: addroute LSID 192.168.43.0
OSPF: ospf_build_route RT 192.168.43.0
OSPF: build route 192.168.43.0(255.255.255.0).
OSPF: processing LS_ASE 192.168.44.0, mask 255.255.255.0, adv 192.168.20.236, age 258
OSPF: addroute LSID 192.168.44.0
OSPF: ospf_build_route RT 192.168.44.0
OSPF: build route 192.168.44.0(255.255.255.0).
……
OSPF: end doing SPF for AREA 0.0.0.0

2. Description of the displaying fields:

Field	Description
LSA(192.168.20.236, LS_SUM_ASB)	ID and type of LSA

54.1.13 debug ip ospf tree

To display establishment of SPF tree of OSPF, use the debug ip ospf tree.

debug ip ospf tree

parameter

none

default

none

command mode

EXEC

instruction

To display establishment of SPF tree of OSPF from the output of this command.

example

```
router# debug ip ospf tree
B3710_221#
OSPF: add LSA(192.168.40.0, LS_STUB) 1600 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.2, LS_RTR) 1600 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.3, LS_RTR) 1600 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.1, LS_STUB) 0 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.3, LS_STUB) 1600 under LSA(192.168.40.3, LS_RTR)
OSPF: add LSA(192.169.1.5, LS_RTR) 3200 under LSA(192.168.40.2, LS_RTR)
OSPF: add LSA(192.168.40.18, LS_STUB) 1600 under LSA(192.168.40.2, LS_RTR)
OSPF: add LSA(192.168.40.2, LS_STUB) 1600 under LSA(192.168.40.2, LS_RTR)
OSPF: add LSA(192.168.40.17, LS_STUB) 3200 under LSA(192.169.1.5, LS_RTR)
OSPF: add LSA(192.168.40.24, LS_SUM_NET) 1601 under LSA(192.168.40.3, LS_RTR)
OSPF: add LSA(192.168.40.32, LS_SUM_NET) 3200 under LSA(192.168.40.2, LS_RTR)
OSPF: add LSA(192.168.40.40, LS_SUM_NET) 14577 under LSA(192.169.1.5, LS_RTR)
OSPF: add LSA(192.168.20.236, LS_SUM_ASB) 3200 under LSA(192.168.40.2, LS_RTR)
```

Description of the displaying fields:

Field	Description
LSA(192.168.20.236, LS_SUM_ASB)	ID and type of LSA
add	Sub-LSA
under	parent LSA

54.1.14 default-information originate (OSPF)

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the default-information originate command

default-information originate [**always**] [**route-map** *map-name*]

no default-information originate [**always**] [**route-map** *map-name*]

parameter

parameter	description
originate	Generate a default external route into an Open Shortest Path First (OSPF) routing domain
Always	(Optional) Always advertises the default route regardless of whether the

	software has a default route.
route-map map-name	(Optional) Routing process will generate the default route if the route map is satisfied.

default

This command is disabled by default. No default external route is generated into the OSPF routing domain.

command mode

router configuration

instruction

Whenever you use the redistribute or the default-information router configuration command to redistribute routes into an OSPF routing domain, the software automatically becomes an Autonomous System Boundary Router Switch. However, an ASBR Switch does not, by default, generate a default route into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the always keyword.

When you use this command for the OSPF process, you must satisfy the route-map argument. Use the default-information originate always route-map command when you do not want the dependency on the default network in the routing table.

example

The following example specifies a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

router ospf 109

redistribute rip

default-information originate

related commands

Redistribute

54.1.15 default-metric

To set default metric values for the Open Shortest Path First (OSPF) routing protocol, use the default-metric command. To return to the default state, use the no form of this command.

default-metric *value*

no default-metric

parameter

parameter	description
value	Default metric value appropriate for the specified routing protocol, in the range 1~4294967295.

default

Default metric value is 10.

command mode

router configuration

instruction

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

example

The example assigns 10 as the default metric routes.

router_config_ospf_100#default-metric 3

related commands

redistribute

54.1.16 distance ospf

To define Open Shortest Path First (OSPF) route administrative distances based on route type, use the distance ospf command To restore the default value, use the no form of this command.

distance ospf {[**intra-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]}

no distance ospf [**intra-area**] [**inter-area**] [**external**]

parameter

parameter	description

intra-area dist1	(Optional) Sets the distance for routes in an area, learned by redistribution. The default value is 110.
inter-area dist2	(Optional) Sets the distance for all routes from one area to another area. The default value is 110.
external dist3	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. The default value is 110.

default

intra-area: 110

inter-area: 110

external: 150

command mode

router configuration

instruction

This command performs the same function as the distance command used with an access list. However, the distance ospf command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

example

The following example changes the external distance to 200:

Router A
router ospf 1
redistribute ospf 2
distance ospf external 200
!
router ospf 2
redistribute ospf 1
distance ospf external 200
Router B
router ospf 1
redistribute ospf 2
distance ospf external 200
!
router ospf 2
redistribute ospf 1
distance ospf external 200

related commands

distance

54.1.17 filter

To configure routing fliter list, use the filter command. Use the no filter command to restore the default.

filter {**interface-type** *interface*-number | *****} {**in | out** } {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

no filter {**interface-type** *interface*-number | *****} {**in** | out} {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

parameter

parameter	description
***interface*-type**	Interface type
interface-number	Interface number
*****	All interfaces
In	Filters incoming ospf routes
out	Filters outgong routes
access-list-name	Name of access list
access-list-name	Name of access list
prefix-list-name	Name of prefix list

default

none

command mode

router configuration

instruction

none

example

filter * in access-list mylist

54.1.18 ip ospf cost

To specify the cost of OSPF protocol on an interface, use the ip ospf cost command in interface configuration mode. To restore to the default value, use the no form of this command.

ip ospf cost cost

no ip ospf cost

parameter

parameter	description
cost	the cost of OSPF protocol. It can be a value in the range from 1 to 65535.

default

Default value of the OSPF protocol cost depends on rate of the interface.

command mode

interface configuration mode

example

The following example sets the interface cost value to 2:

ip ospf cost 2

specify the the interface cost of OSPF protocol, to restore the default value,use the no ip ospf command

54.1.19 ip ospf dead-interval

To set the dead-interval of specified routing switch in neighbourhood, use the ip ospf dead-interval command in interface configuration mode. To restore the default value, use the no form of this command.

ip ospf dead-interval *seconds*

ip ospf dead-interval

parameter

parameter	description
Seconds	Interval (in seconds) of specified routing switch in neighbourhood. The

	range is 1 to 65535.

default

40 seconds

command mode

interface configuration

instruction

The dead interval is advertised in OSPF hello packets and sent with OSPF hello packets. This value must be the same for all networking devices on a specific network and four times the interval set by the ip ospf hello-interval command.

example

The following example sets the OSPF dead interval to 60 seconds:

router_config_S1/0#ip ospf dead-interval 60

related commands

ip ospf hello-interval

54.1.20 ip ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the ip ospf hello-interval command. To return to the default value, use the no form of this command.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

parameter

parameter	description
Seconds	Specifies the interval (in seconds)of sending hello packets. The range is from 1 to 255.

default

10 seconds

command mode

interface configuration mode

instruction

This value is advertised in the hello packets and sent with the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

example

The following example sets the interval between hello packets to 20 seconds:

router_config_S1/0#ip ospf hello-interval 20

related commands

ip ospf dead-interval

54.1.21 ip ospf message-digest-key

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the ip ospf message-digest-key md5 command. To remove an old MD5 key, use the no form of this command.

ip ospf message-digest-key *keyid* **md5 key**

no ip ospf message-digest-key *keyid*

parameter

parameter	description
keyid	An identifier in the range from 1 to 255.
key	Alphanumeric password of up to 16 bytes.

default

OSPF MD5 authentication is disabled.

command mode

interface configuration mode

instruction

Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value.

The process of changing keys is as follows. Suppose the current configuration is as follows:

```
interface ethernet 1
ip ospf message-digest-key 100 md5 OLD
```

You change the configuration to the following:

```
interface ethernet 1
ip ospf message-digest-key 101 md5 NEW
```

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet—the first one authenticated by key 100 and the second one authenticated by key 101.

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

```
interface ethernet 1
no ip ospf message-digest-key 100
```

Then, only key 101 is used for authentication on Ethernet interface 1.

We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

example

The following example sets a new key 19 with the password 8ry4222:

```
interface ethernet 1
ip ospf message-digest-key 10 md5 xvv560qle
ip ospf message-digest-key 19 md5 8ry4222
```

related commands

area authentication

54.1.22 ip ospf network

To configure the Open Shortest Path First (OSPF) network type, use the ip ospf network command. To return to the default value, use the no form of this command.

ip ospf network { **broadcast | nonbroadcast | point_to_multipoint** | **point-to-point**}

no ip ospf network { **broadcast | nonbroadcast | point_to_multipoint | point-to-point**}

parameter

parameter	description
broadcast	Sets the network type to broadcast.
nonbroadcast	Sets the network type to nonbroadcast multiaccess
point-to-point	Sets the network type to point-to-point.
point-to-multipoint	Sets the network type to point-to-multipoint.

command mode

interface configuration mode

instruction

Using this feature, you can configure broadcast networks as NBMA networks. Configuring NBMA networks as point-to-multipoint network if there is no assurance to direct connection between any two routing switches..

example

The following example sets serial1/0 as a nonbroadcast network type:

router_config_S1/0#ip ospf network nonbroadcast

54.1.23 ip ospf passive

To cancel sending a HELLO packets on an interface, use the ip ospf passive command. Use the no form of this command to reactivate the sending of HELLO packet.

ip ospf passive

no ip ospf passive

parameter

This command has no keywords or parameters.

default

disabled

command mode

all configruration mode

instruction

If you cancel sending a HELLO packet on an interface, a specified subnetwork wll keep on declaring to other interfaces, and the routing update from other routing switch to this interface can still be received and dealt with. This is usually applicable to the STUB network, for in this kind of network there is usually no other OSPF routing switches.

example

The following example sends a HELLO packet to all interfaces(except for Ethernet 1/0) overridden by network 172.16.0.0:

interface ethernet 1/0
ip address 172.16.0.1 255.255.0.0
ip ospf passive
router ospf 110
network 172.16.0.0 255.255.0.0 area 1

related commands

none

54.1.24 ip ospf password

To configure password for a neighbor route, use the ip ospf password command. Use the no form of this command to cancel the configuration.

ip ospf password *password*

no ip ospf password

parameter

parameter	description
password	Any consecutive 8-digit character string

default

No password is predefined by default.

command mode

Interface configuration mode

instruction

The password generated by this command directly inserts OSPF information packet. This command can configure one password for each network of each interface. All neighbor routers must have the same password to exchange OSPD routing information.

Note: This command is only valid when configured with the area authentication command.

example

ip ospf password yourpass

related commands

area authentication

54.1.28 ip ospf priority

To set the router priority, use the ip ospf priority command. To return to the default value, use the no form of this command.

ip ospf priority *priority*

no ip ospf priority

parameter

parameter	description
priority	specifies the priority. The range is from 0 to 255.

default

Priority of 1

command mode

interface configuration mode

instruction

When two routing switches attached to a network both attempt to become the designated routing switch, the one with the higher routing switch priority takes precedence. If there is a tie, the routing switch with the higher routing switch ID takes precedence. A routing switch with a routing switch priority set to zero is ineligible to become the designated routing switch or backup designated routing switch. routing switch priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

This priority value is used when you configure Open Shortest Path First (OSPF) for nonbroadcast networks using the neighbor routing switch configuration command for OSPF.

example

The following example sets the routing switch priority value to 8:

router_config_S1/0#ip ospf priority 8

related commands

neighbor

54.1.29 ip ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the ip ospf retransmit-interval command. To return to the default value, use the no form of this command.

ip ospf retransmit *seconds*

no ip ospf retransmit

parameter

parameter	description
seconds	Time (in seconds) between retransmissions. The range is from 1 to 65535 seconds.

default

The default is 5 seconds.

command mode

interface configuration mode

instruction

When a routing switch sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the routing switch receives no acknowledgment, it will resend the LSA. The setting of the seconds argument should be greater than the expected round-trip delay between any two routing switches on the attached network..

example

The following example sets the retransmit interval value to 8 seconds:
router_config_S1/0#ip ospf retransmit 8

54.1.30 neighbor

To configure Open Shortest Path First (OSPF) routing switch interconnecting to nonbroadcast networks, use the neighbor command. To remove a configuration, use the no form of this command.

neighbor *ip-address* [*priority number*] [**poll-interval** *seconds*] [**cost** *number*]

no neighbor *ip-address* [*priority number*] [**poll-interval** *seconds*] [*cost number*]

parameter

parameter	description
ip-address	Interface IP address of the neighbor.
priority number	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces.

poll-interval seconds	(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.
cost number	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ip ospf cost command. For point-to-multipoint interfaces, the cost keyword and the number argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks.

default

no default value

command mode

router configuration

instruction

In X.25 and Frame Relay networks you can configure OSPF to run as a broadcast network. Detailed information is as follow:

In X.25 and frame relay map

One nonbroadcast network neighbor must be configured in the routing switch. The neighbor address must be on the primary address of the interface.

If a neighboring router has become inactive, it may still be necessary to send hello packets to the dead neighbor. These hello packets will be sent at a reduced rate called Poll Interval.

When the routing switch first starts up, it sends only hello packets to those routing switches with nonzero priority, that is, routing switches that are eligible to become designated routeing switch (DRs) and backup designated routing switches (BDRs). After the DRs and BDRsare selected, DRs and BDRs will then start sending hello packets to all neighbors in order to form adjacencies.

example

The following example declares a routing switch at address 131.108.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
router ospf
neighbor 131.108.3.4 priority 1 poll-interval 180
```

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
interface Serial0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
no keepalive
frame-relay local-dlci 200
frame-relay map ip 10.0.1.3 202
frame-relay map ip 10.0.1.4 203
frame-relay map ip 10.0.1.5 204
no shut
!
router ospf 1
network 10.0.1.0 255.255.255.0 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
```

related commands

ip ospf priority

54.1.31 network area

To define the interfaces on which Open Shortest Path First (OSPF) runs and to define the area ID for those interfaces, use the network area command. To disable the feature, use the no form of this command.

network *network mask* **area** *area_id* [**advertise** | **not-advertise**]

[**no**] **network** *network mask* **area** *area_id* [**advertise** | **not-advertise**]

parameter

parameter	description
network	Network Ip address, in dotted decimal format.
mask	Mask, in dotted decimal format.
area_id	Id of area.
Advertise notadvertise	Specifies whether to advertise the abstract information or not

default

This command is disabled by default. command mode

router configuration

instruction

Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the network command list and ignore the subsequent overlapping portions. Importing network range and specifying the range can reduce the switch state of routing information among areas

Example

The following example defines network range 10.0.0.0 255.0.0.0 and adds to area 2:

router_config_ospf_10#network 10.0.0.0 255.0.0.0 area 2

54.1.32 redistribute

To configure OSPF to redistribute routes of other routing protocols, use the redistribute command. Use the no form of this command to restore the default.

redistribute protocol [*as-number*] [**route-map map-tag**]

no redistribute protocol [*as-number*] [**route-map map-tag**]

parameter

parameter	Description
protocol	Redistributes former protocols that learned, it should be one of the following: beigrp、bgp、connect、ospf、rip、static
as_number	(Optional) Autonomous system number. There is no parameter for connect, rip and static.
map-tag	(Optional) Name of the route map

default

disabled

command mode

router configuration

instruction

none

example

The following example redistributes OSPF protocol from the autonomous system 0:

Redistribute ospf 0

54.1.33 router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the router ospf command. To terminate an OSPF routing process, use the no form of this command.

router ospf *process-id*

no router ospf *process-id*

parameter

parameter	description
process-id	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.

default

No OSPF routing process is defined.

command mode

global configuration mode

instruction

You can specify multiple OSPF routing processes in each router.

example

The following example configures an OSPF routing process and assign a process number of 109:

router ospf 109

related commands

network area

54.1.34 show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the show ip ospf command.

show ip ospf [*process-id*]

parameter

parameter	description
process-id	(Optional) Process ID. If

default

none

command mode

EXEC

instruction

Troubleshoot OSPF problems according to the output of this command. To display only the global configuration information of the corresponding OSPF process if configured with the process-id parameter.

example

The following display the configuration information of OSPF process :

router#show ip ospf
OSPF process: 1, Router ID is 192.168.99.81
Distance: intra-area 110 inter-area 130 external 150
Source Distance Access-list
240.240.1.1/24 1 what
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Number of areas is 3
AREA: 1
Number of interface in this area is 1(UP: 1)
Area authentication type: None
AREA: 36.0.0.1
This is a stub area.
Number of interface in this area is 0(UP: 0)
Area authentication type: None
AREA: 192.168.20.0
Number of interface in this area is 0(UP: 0)

Area authentication type: None
Net Range list:
10.0.0.0/255.0.0.0 Not-Advertise
140.140.0.0/255.255.0.0 Advertise
filter list on receiving UPDATE is Gateway: weewe
filter list on sending UPDATE is Prefix: trtwd
Summary-address list:
150.150.0.0/16 advertise
router#

description of the displaying fields

field	description
OSPF process: 1	OSPF process ID
Router ID is 192.168.99.81	Routing switch ID
Distance: intra-area 110 inter-area 130 external 150	The default administrative distance that the current routing switch adopts
Source Distance Access-list	Administrative distance based on concrete routing configuration
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs	Value of two timer related to OSPF
Number of areas is 3	The number of the field that currently configured and the parameter configured in each field
filter list on receiving	The configured filter list on receiving routes
filter list on sending	The configured filter list on sending routes
Summary-address list	The configured routing summary address

54.1.35 show ip ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the show ip ospf border-routers command.

show ip ospf border-routers

parameter

none

default

none

command mode

EXEC

example

router#
router#sh ip os bor
OSPF process: 1
Codes: i - Intra-area route, I - Inter-area route
Destination Adv-Rtr Cost Type Area
i 192.168.20.77 192.168.20.77 11 ABR 0
router#

field description:

field	description
Destination	Routing switch ID of the destination.
Adv-Rtr	Next hop toward the destination.
Cost	Cost of using this route.
Type	The routing switch type of the destination; it is either an ABR or ASBR or both.
Area	The area ID of the area from which this route is learned.

54.1.36 show ip ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database, use the show ip ospf database command.

show ip ospf database

parameter

none

default

none

command mode

EXEC

instruction

Display lists of information related to the Open Shortest Path First (OSPF) database in accordance with debugging information of the command, and it is helpful for users in troubleshooting

example

router#
router#show ip ospf database
OSPF process: 1
(Router ID 192.168.99.81)
AREA: 0
Router Link States
Link ID ADV Router Age Seq # Checksum Link count
192.168.20.77 192.168.20.77 77 0x8000008a 0x90ed 1
192.168.99.81 192.168.99.81 66 0x80000003 0xd978 1
Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.20.77 192.168.20.77 80 0x80000001 0x9625
Summary Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.99.0 192.168.99.81 87 0x80000003 0xd78c
AREA: 1
Router Link States
Link ID ADV Router Age Seq # Checksum Link count
192.168.99.81 192.168.99.81 70 0x80000002 0x0817 1
Summary Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.20.0 192.168.99.81 66 0x80000006 0xd1c1
router#

field description:

field	Description
AREA: 1	OSPF area.
Router Link States/Net Link States/Summary Net Link States	LSA type
Link ID	LSA ID.
ADV Router	Advertising routing switch's ID.

Age	Link state age.
Seq #	Link state sequence number
Checksum	Fletcher checksum of the complete contents of the link state advertisement.

54.1.37 show ip ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the show ip ospf interface command.

show ip ospf interface

parameter

none

default

none

command mode

EXEC

instruction

To display configuration and operation situation of OSPF on an interface according to the debugging information of this command. Users can confirm whether the configuration is right or not and it is helpful in troubeshooting

example

router#sh ip os int
Ethernet 1/0 is up, line protocol is up
Internet Address: 192.168.20.81/24, Nettype: BROADCAST
OSPF process is 1, AREA 0, Router ID 202.96.135.201
Cost 10, Transmit Delay is 1 sec, Priority 1
Hello interval 10, Dead timer 40, Retransmit 5
OSPF INTF State is DrOther
Designated Router id 131.119.254.10, Interface address 131.119.254.10
Backup Designated router id 131.119.254.28, Interface addr 131.119.254.28
Neighbor Count is 8, Adjacent neighbor count is 2
Adjacent with neighbor 131.119.254.28 (Backup Designated Router)
Adjacent with neighbor 131.119.254.10 (Designated Router)
router#

displaying field description:

field	description
Internet Address:	Interface IP address
Nettype	Net type of OSPF interface
OSPF process is	OSPF process number
AREA	OSPF area.
Router ID	Routing switch ID
Cost	Cost of routing switch OSPF interface
Transmit Delay is	Transmit delay
Priority	Priority of routing switch interface
Hello interval	Number of seconds until next hello packet is sent out this interface.
Dead timer	Dead timer
Retransmit	Retransmit interval
OSPF INTF State is	OSPF nterface state
Designated Router id	Designated router id and interface ip address
Backup Designated router id	Backup Designated routing switch id and interface ip address
Neighbor Count is	Number of the neighbor routing switch
Adjacent neighbor count is	Number of the adjacent neighbor that has established
Adjacent with neighbor	List of the adjacent neighbor

54.1.38 show ip ospf neighbor

To display Open Shortest Path First (OSPF)-neighbor information, use the show ip ospf neighbor command.

show ip ospf neighbor

parameter

none

default

none

command mode

EXEC

instruction

To display neighbor situation of OSPF from the output of this command to help user troubleshoot OSPF.

example

router#show ip ospf neighbor
OSPF process: 1
AREA 1
Neighbor Pri State DeadTime Address Interface
21.0.0.32 1 FULL /DR 31 192.168.99.32 Ethernet1/0
AREA 36.0.0.1
Neighbor Pri State DeadTime Address Interface
199.199.199.137 1 EXSTART/DR 31 202.19.19.137 Ethernet2/1
AREA 192.168.20.0
Neighbor Pri State DeadTime Address Interface
140.140.0.46 1 FULL /DR 108 140.140.0.46 Serial 1/0
133.133.2.11 1 FULL /DR 110 133.133.2.11 Serial1/0
192.31.48.200 1 FULL / DROTHER 31 192.31.48.200 Ethernet1/0

Displaying field description:

field	description
OSPF process	OSPF process number
AREA	OSPF area
Neighbor	Neighbor routing switch ID.
Pri	Routing switch priority of the neighbor, neighbor state.
State	OSPF state.
DeadTime	Expected time before software will declare the neighbor dead.
Address	Neighbor ip address
Interface	Interface to which connects the neighbor

54.1.39 show ip ospf virtual-link

To display information of Open Shortest Path First (OSPF) virtual links, use the show ip ospf virtual-links command.

show ip ospf virtual-link

parameter

none

default

none

command mode

EXEC

instruction

The information displayed by the show ip ospf virtual-links command is useful in debugging OSPF routing operations. To display the detailed information of adjacency relation of the OSPF neighbour, use the show show ip ospf neighbour command

example

router#show ip ospf vir
Virtual Link Neighbor ID 200.200.200.2 (UP)
Run as Demand-Circuit
TransArea: 1, Cost is 185
Hello interval is 10, Dead timer is 40 Retransmit is 5
INTF Adjacency state is IPOINT_TO_POINT

Description of the displaying fields:

field	description
neibhbor ID	The configured neighbor ID of the remote side
neighbour state	Adjacency relation of the OSPF neighbor
Demand-Circuit	Indicates working under DC mode
TransArea	The transit area through which the virtual link is formed.
cost	The cost of reaching the OSPF neighbor through the virtual link.
Hello Interval	The current Hello interval
DeadTime	Expected time before software will declare the neighbor dead.
Retrans	Retransmit interval
INTF Adjacency State	The state of virtual link.

related commands

area vritual-link

show ip ospf neighbor

54.1.40 summary-address

To create aggregate addresses for Open Shortest Path First (OSPF), use the summary-address command. To restore the default, use the no form of this command.

summary-address *address mask* [**not-advertise**]

no summary-address *address mask*

parameter

parameter	description
address	Summary address designated for a range of addresses.
Mask	IP subnet mask used for the summary route.
not-advertise	(Optional) Suppress match routes that creat LSA

default

none

command mode

router configuration

instruction

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Routing switch (ASBRs) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the area range command for route summarization.

example

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

```
summary-address 10.1.0.0 255.255.0.0
```

related commands

area range

ip ospf password

ip ospf message-digest-key

54.1.41 timers delay

To specify the delay interval between OSPF receiving a topology structure variety and initializing a minimum route priority computation, use the timer delay command. Use the no form of this command to resotre default value.

timers delay *spf-delay*

no timers delay

parameter

parameter	description
spf-delay	Delay between topology variety and computation commencement in seconds, from 0 to 65535. Default value is 5 seconds. If the value is o, that indicates there is no delay, namely, once there is a variety, the commencement of computation immediately starts.

default

spf-delay: 5 seconds

command mode

router configuration

instruction

The less the configured time is, the quicker the response to network variety. But this will take up more processing time.

example

timers spf 10

54.1.42 timers hold

To configure the interval between two continuous SPF computation, use the timers hold command. Use the no form of this command to restore the default value.

timers hold *spf-holdtime*

no timers hold

parameter

parameter	description
spf-holdtime	The minimum value between two continuous computation, in the range from 0 to 65535.

default

spf-holdtime: 10 seconds

command mode

router configuration

instruction

The less the configured time is, the quicker the response to network variety. But this will take up more processing time.

example

3. timers spf 20

Chapter 55 BGP Configuration Commands

BGP Configuration Commands include:

- aggregate-address
- bgp always-compare-med
- bgp bestpath med
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation identifier
- bgp confederation peers
- bgp dampening
- bgp default
- bgp deterministic-med
- bgp redistribute-internal
- clear ip bgp
- debug chat
- debug dialer
- debug ip bgp
- distance
- filter
- neighbor default-originate
- neighbor description
- neighbor distribute-list
- neighbor ebgp-multihop
- neighbor filter-list
- neighbor maximum-prefix
- neighbor next-hop-self
- neighbor password

- neighbor prefix-list
- neighbor remote-as
- neighbor route-map
- neighbor route-reflector-client
- neighbor route-refresh
- neighbor send-community
- neighbor shutdown
- neighbor soft-reconfiguration
- neighbor timers
- neighbor update-source
- neighbor weight
- network (BGP)
- redistribute(BGP)
- router bgp
- show ip bgp
- show ip bgp community
- show ip bgp neighbors
- show ip bgp paths
- show ip bgp prefix-list
- show ip bgp regexp
- show ip bgp summary
- synchronization
- table-map
- timers

55.1.43 aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the aggregate-address command in address family or routing switch configuration mode. To disable this function, use the no form of this command.

aggregate-address A.B.C.D/n [**summary-only**] [**route-map** *map-name*]

no aggregate-address A.B.C.D/n [**summary-only**] [**route-map** *map-name*]

parameter

parameter	description
A.B.C.D/n	Aggregate network
summary-only	Filters all more-specific routes from updates.
route-map	Name of the route map used to set the attribute of the aggregate route.
map-name	Name of the route map

default

none

command mode

BGP configuration mode

instruction

You can implement aggregate routing in BGP in three methods:first,dynamic implement routing by forwarding redistribute; second, static implement routing by network command; third, static implement routing by aggregate. The routing created in this way are local routing, which can be announced to other equivalent, but not implement local IP address table.

Using the aggregate-address command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix which matches the aggregate must exist in the RIB.) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the as-set keyword.)

Using the as-set keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the aggregate-address command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the summary-only keyword not only creates the aggregate route (for example, 19.*.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the neighbor distribute-list command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the suppress-map keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the match clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the advertise-map keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the aggregate-address command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists match clauses are supported.

Using the attribute-map keyword allows attributes of the aggregate route to be changed. This form of the aggregate-address command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

example

In the following example, an aggregate BGP address is created :

```
router bgp 5
aggregate-address 193.0.0.0/8
```

related commands

route-map

55.1.44 bgp always-compare-med

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the bgp always-compare-med command. To disallow the comparison, use the no form of this command.

bgp always-compare-med

no bgp always-compare-med

parameter

none

default

Default does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the no form of this command is entered..

command mode

BGP configuration mode

instruction

Default does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the no form of this command is entered. The MED is compared only if the autonomous system path for the compared routes is identical.

example

The following example enables the function

router bgp 5

bgp always-compare-med

related commands

bgp bestpath med

bgp deterministic-med

55.1.45 bgp bestpath med

To modify the process way of Border Gateway Protocol (BGP) on Multi Exit Discriminator (MED) attribute, use the bgp bestpath med command. To disable the feature, use the no form of this command.

parameter

parameter	description
confed	Autonous system confederation MED comparison attrubute
missing-as-worst	(Optional) Assigns the value of infinity to received routes that do not carry the MED attribute, making these routes the least desirable.

default

none

command mode

BGP configuration mode

instruction

If the MED attribute of BGP route is not configured, the value of MED is always considered to be 0, that is the least value, which has the most priority. When configured with the missing-as-worst option, if the MED attribute of BGP route is not configured, the value of MED is always considered to be the most maximum value, which has the least priority.

example

By default, the MED comparison between(100)and (200) doesn't occur for they are not the routes from the same sub-autonomous system. But the MED comparison occurs when configured with the bgp bestpath med confed command, for they come from the sub-autonomous system 100 and 200 respecitively in the autonomous system alliance.

related commands

bgp always-compare-med

bgp deterministic-med

55.1.46 bgp client-to-client reflection

To enable or restore route reflection from a BGP route reflector to clients, use the bgp client-to-client reflection command. To disable client-to-client route reflection, use the no form of this command.

bgp client-to-client reflection

no bgp client-to-client reflection

parameter

none

default

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients.

command mode

BGP configuration mode

instruction

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the no bgp client-to-client reflection command to disable client-to-client reflection.

example

In the following example, the local routing switch is a route reflector, and the three neighbors are fully meshed, turn off client-to-client reflection

```
router bgp 5
neighbor 192..168.20.190 router-reflector-client
neighbor 192..168.20.191 router-reflector-client
neighbor 192..168.20.192 router-reflector-client
no bgp client-to-client reflection
```

related commands

neighbor route-reflector-client

bgp cluster-id

55.1.47 bgp cluster-id

To set the cluster ID on a route reflector in a route reflector cluster, use the bgp cluster-id command in router configuration mode. To remove the cluster ID, use the no form of this command.

bgp cluster-id *cluster-id*

no bgp cluster-id *cluster-id*

parameter

parameter	description
cluster-id	Cluster ID of this router acting as a route reflector; maximum of 4 bytes.

default

The local routing switch ID of the route reflector is used as the cluster ID when no ID is specified or when the no form of this command is entered.

command mode

BGP configuration mode

instruction

Together, a route reflector and its clients form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the routing switch ID of the route reflector. The bgp cluster-id command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.

example

In the following example, the local routing switch is one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster.

```
router bgp 5
neighbor 198.92.70.24 route-reflector-client
bgp cluster-id 50000
```

related commands

neighbor route-reflector-client

show ip bgp summary

55.1.48 bgp confederation identifier

To specify a BGP confederation identifier, use the bgp confederation identifier command. To remove the confederation identifier, use the no form of this command.

bgp confederation identifier autonomous-system

no bgp confederation identifier autonomous-system

parameter

parameter	description
autonomous-system	Autonomous system number to be configured to internally include multiple autonomous systems.

default

none

command mode

BGP configuration mode

instruction

The bgp confederation identifier command is used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation.

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. The subautonomous systems within the confederation exchange routing information like iBGP peers. External peers interact with the confederation as if it is a single autonomous system.

Each subautonomous system is fully meshed within itself and has a few connections to other autonomous systems within the confederation. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you enables to you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems.

example

In the following example, the routing domain is divided into autonomous systems AS4001, 4002, 4003, 4004, 4005, 4006 and 4007 and identified by the confederation identifier 50000. Neighbor 1.2.3.4 is a peer inside of the routing domain confederation. Neighbor 3.4.5.6 is a peer outside of the routing domain confederation.

```
router bgp 4001
bgp confederation identifier 5
bgp confederation peers 4002 4003 4004 4005 4006 4007
neighbor 1.2.3.4 remote-as 4002
neighbor 3.4.5.6 remote-as 510
```

related commands

bgp confederation peers

show ip bgp summary **30**

55.1.49 bgp confederation peers

To configure subautonomous systems to belong to a single confederation, use the bgp confederation peers command in router configuration mode. To remove an autonomous system from the confederation, use the no form of this command.

bgp confederation peers autonomous-system [**autonomous-system**]

no bgp confederation peers autonomous-system [**autonomous-system**]

parameter

parameter	description
autonomous-system	Autonomous system numbers for BGP peers that will belong to the confederation.

default

none

command mode

BGP configuration mode

instruction

The bgp confederation peers command is used to configure multiple autonomous systems as a single confederation. The ellipsis (...) in the command syntax indicates that your command input can include multiple values for the as-number argument.

The autonomous systems specified in this command are visible internally to the confederation. Each autonomous system is fully meshed within itself. The bgp confederation identifier command specifies the confederation to which the autonomous systems belong.

example

In the following example, autonomous systems 1091, 1092 and 1093 are configured to belong to a single confederation under the identifier 1090:

router bgp 1090

bgp confederation identifier 23

bgp confederation peers 1091 1092 1093

related commands

bgp confederation identifier

show ip bgp summary

55.1.50 bgp dampening

To enable BGP route dampening or change BGP route dampening parameters, use the bgp dampening command in address family or router configuration mode. To disable BGP dampening, use the no form of this command.

bgp dampening [**route-map** *name*] | [*half-time resuse-value suppress-value hold-time*]

no bgp dampening [**route-map** *name*] | [*half-time resuse-value suppress-value hold-time*]

parameter

parameter	description
route-map	Name of route map that controls where BGP route dampening is enabled.
name	Name of route map that controls parameters
half-time	Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period
reuse-value	Reuse values based on accumulated penalties.
suppress-value	A route is suppressed when its penalty exceeds this limit.
hold-time	Maximum time (in minutes) a route can be suppressed.

default

half-time: 15 minutes

reuse-value: 750

suppress-value: 2000

hold-time: 60 minutes

command mode

BGP configuration mode

instruction

The bgp dampening command is used to enable BGP route dampening. This command can be entered without any arguments or keywords. The half-life, reuse, suppress, and hold-time arguments are position-dependent; meaning that if any of these arguments are entered, then all optional arguments must be entered.

When BGP dampening is configured and a prefix is withdrawn, BGP considers the withdrawn prefix as a flap and increases the penalty by a 1000. If BGP receives an attribute change, BGP increases the penalty by 500. If then the prefix has been withdrawn, BGP keeps the prefix in the BGP table as a history entry. If the prefix has not been withdrawn by the neighbor and BGP is not using this prefix, the prefix is marked as dampened. Dampened prefixes are not used in the BGP decision process and not installed to the routing table.

example

In the following example, the bgp dampening command can be used to enable BGP route dampening function and use default parameter configuration. Use the following commands to configure different dampening parameters for different rouing configurations:

```
Router bgp 100
bgp dampening route-map DMAP
!
route-map DMAP 10 permit
match as-path ASLIST-1
set dampening 15 750 2000 60
!
route-map DMAP 20 permit
  match as-path ASLIST-2
  set dampening 2 750 2000 8
!
ip as-path access-list ASLIST-1 permit ^3_
ip as-path access-list ASLIST-2 permit ^5_
```

related commands

set dampening

55.1.51 bgp default

To configure default parameter of BGP process, use the bgp default command. Use the no form of this command to restore the default value.

bgp default local-preference *<0-4294967295>*

no bgp default local-preference *<0-4294967295>*

parameter

parameter	description
local-preference	Configures default parameter of the local preference.
<0-4294967295>	Default value of the local preference

default

100

command mode

BGP configuration mode

instruction

The route received from IBGP will be set as the local preference by BGP. The default value is 100, which can be modified via this command.

example

The following example configures 200 as the local preference for the route from IBGP neighbor:

router bgp 100

bgp default local-preference 200

related commands

none

55.1.52 bgp deterministic-med

To enforce the deterministic comparison of the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system, use the bgp deterministic-med command in router configuration mode. To disable the required MED comparison, use the no form of this command.

bgp deterministic-med

no bgp deterministic-med

parameter

none

default

none

command mode

BGP configuration mode

instruction

The bgp always-compare-med command is used to enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. After the bgp always-compare-med command is configured, all paths for the same prefix that are received from different neighbors, which are in the same autonomous system, will be grouped together and sorted by the ascending MED value (received-only paths are ignored and not grouped or sorted). The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a per neighbor autonomous system basis and then global basis. The grouping and sorting of paths occurs immediately after this command is entered. For correct results, all routers in the local autonomous system must have this command enabled (or disabled).

example

none

related commands

bgp bestpath med

bgp always-compare-med

55.1.53 bgp redistribute-internal

To configure IBGP redistribution into an interior gateway protocol (IGP), such as RIP or OSPF, use the bgp redistribute-internal command in address family or router configuration mode. To return the router to default behavior and stop iBGP redistribution into IGPs, use the no form of this command.

bgp redistribute-internal

no bgp redistribute-internal

parameter

none

default

IBGP routes are not redistributed into IGP.

command mode

BGP configuration mode

instruction

The bgp redistribute-internal command is used to configure iBGP redistribution into an IGP. The clear ip bgp command must be entered to reset BGP connections after this command is configured. When redistributing BGP into any IGP, be sure to use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed.

example

In the following example, BGP to OSPF3 route redistribution is enabled:

```
router ospf 3
 redistribute bgp 2
!
router bgp 2
 bgp redistribute-internal
!
```

related commands

none

55.1.54 clear ip bgp

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the clear ip bgp command in privileged EXEC mode.

clear ip bgp {***** | *ip-address* | *as-number* | **peer-group** *name* | **aggregates** | **networks** | **redistribute}** [**soft** [**in** | **out]**]

parameter

parameter	description

*	Specifies that all current BGP sessions will be reset.
ip-address	Specifies that only the identified BGP neighbor will be reset.
AS	Specifies that sessions with BGP peers in the specified autonomous system will be reset.
peer-group-name	Specifies that the identified BGP peer group will be reset.
aggregates	Specifies that all aggregate routes will be reset
networks	Specifies that all static network routes will be reset
redistribute	Specifies that all redistributed routes will be reset
soft	Initiates a soft reset
in | out	Initiates inbound or outbound reconfiguration.

command mode

EXEC

instruction

The clear ip bgp command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the neighbor soft-reconfiguration inbound command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

If all BGP routers support the route refresh capability, use the clear ip bgp command with the in keyword. You need not use the soft keyword, because soft reset is automatically assumed when the route refresh capability is supported.

example

The following example clear all the current BGP sessions:

```
clear ip bgp *
```

related commands

neighbor soft-reconfiguration

show ip bgp

55.1.55 debug chat

To display script events, like to startup a script, to stop a script, to display the enforcement process of a script, use the debug chat command. Use the no form of this command to stop displaying information.

debug chat

no debug chat

parameter

This command has no parameters or keywords.

command mode

EXEC

example

```
Router#debug chat
Router#SCRIPT: start script default_dialer_script...
SCRIPT:Sending string: ATZ
SCRIPT:Expecting string: OK
SCRIPT: Receive string:
41 54 0D 0D 0A 4F 4B 0D 0A AT...OK..
SCRIPT:Completed match for expect:OK
SCRIPT:Sending string: ATDT 2
SCRIPT:Expecting string: CONNECT
SCRIPT: Receive string:
43 4F 4E 4E 45 43 54 CONNECT
SCRIPT: Completed match for expect:CONNECT
SCRIPT:Chat script finished
```

The first message indicates the script named default_dialer_script is started up.

The second message indicates the ATZ character string is sent.

The third message indicates the character string OK is expected to be received.

The fourth message indiates the character string OK s received.

The fifth message indicates ATDT 2 character string is send, that is asking for modem dial-up.

The sixth message indicates the character string CONNECT is expected to be received.

The seventh message indicates the expected character string CONNECT is received.

The eighth message indicates the success of script enforcement.

related commands

chat-script

55.1.56 debug dialer

To display debugging information about the packets received on a dialer interface, use the debug dialer events command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug dialer

no debug dialer

parameter

This command has no parameters or keywords.

command mode

EXEC

example

```
Router#debug dialer
DIALER Serial 1/0: Dialing cause ip(PERMIT).
DIALER Serial 1/0: Dialing using Modem script: default_dialer_script    & System script: none
DIALER Serial 1/0: Attempting to dial 2
DIALER Serial 1/0: process started
DIALER Serial 1/0: Chat script default_dialer_script (dialer) started.....
DIALER Serial 1/0: Connection established
DIALER Serial 1/0: Modem script finished successfully
```

The first message indicates that dialer checks whether the packet is permitted to cause dialing, and the result is the ip packet allows cause dialing.

The second message indicates that dialing uses default dialer script as the modem script rather than the system script.

The third message indicates that the dialer number is 2.

The fourth message indicates that the dialer process is started.

The fifth message indicates thath the dialer script is started.

The sixth and seventh message indicate that the connection is established successfully.

55.1.57 debug ip bgp

To display information related to processing of the Border Gateway Protocol (BGP), use the debug ip bgp command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug ip bgp {**all | fsm | keepalive | open | update**}

no debug ip bgp {**all | fsm | keepalive | open | update**}

parameter

parameter	description
all	Displays all BGP debugging functions.
dampening	Displays BGP dampening.
event	Displays BGP events.
fsm	Displays BGP fsms
keepalive	Displays BGP keepalives.
notify	Displays BGP notifies
open	Displays BGP opens
update	Displays BGP updates.

default

No default behavior or values

command mode

EXEC

instruction

It is valid globally when configured with the debug ip bgp command to display debugging information and other VTY. If configured with the terminal monitor command, the debugging information will also be displayed. Use the no terminal monitor to close this function to disable displaying any debugging information on the VTY.

The command debug ip bgp all can enable all BGP debugging function, including dampening, fsm,keepalives,open and update. Use the no debug ip bgp all command to disable all BGP debugging functions.

example

The following example is the process to establish a BGP. The debugging information shows that a router establishes a connection with BGP neighbor 10.1.1.3.

BGP: 10.1.1.3 start connecting to peer
BGP: 10.1.1.3 went from Idle to Connect
BGP: 10.1.1.3 went from Connect to OpenSent
BGP: 10.1.1.3 send OPEN, length 41
BGP: 10.1.1.3 recv OPEN, length 41
BGP: 10.1.1.3 went from OpenSent to OpenConfirm
BGP: 10.1.1.3 send KEEPALIVE, length 19
BGP: 10.1.1.3 recv KEEPALIVE, length 19
BGP: 10.1.1.3 went from OpenConfirm to Established
BGP: 10.1.1.3 send KEEPALIVE, length 19
BGP: 10.1.1.3 send UPDATE, length 43
BGP: 10.1.1.3 send UPDATE, length 43
BGP: 10.1.1.3 recv KEEPALIVE, length 19
BGP: 10.1.1.3 recv KEEPALIVE, length 19

55.1.58 distance

To configure the administrative distance for BGP routes, use the distance command in router configuration mode. To return to the administrative distance to the default value, use the no form of this command.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

parameter

parameter	description
external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The default value is 20.
internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The default value is 200.
local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The default value is 200.

default

external-distance: 20

internal-distance: 200

local-distance: 200

command mode

BGP configuration

instruction

The distance bgp command is used to configure a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.

example

In the following example, the administrative distance for BGP routes is set:

router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
distance 20 20 200

related commands

set metric

set tag

55.1.59 filter

To filter routes based on an interface in order to realize the administrative strategy. Use the no form of this command to delete the configuration.

filter interface <**in | out**> **access-list** *access-list-name* **gateway** *access-list-name* **prefix-list** *prefix-list-name*

no filter interface <**in | out**> **access-list** *access-list-name* **gateway** *access-list-name* **prefix-list** *prefix-list-name*

parameter

parameter	description

interface	Interface name. Asterisk signifies all interfaces.
in | out	Filter the incoming of outgoing routes
access-list	Specifies the access-list to filter routes
access-list-name	Name of the access list
gateway	Specifies the access list to filter gateway
access-list-name	Name of the access list
prefix-list	Specifies the prefix list to filter routes
prefix-list-name	Name of the prefix list

default

none

command mode

BGP configuration mode

instruction

The access-list option specifies the access list to filter network prefix of routes; the gateway option specifies the access list to filter nexthop attribute of routes; the prefix list option specifies the prefix list filter network prefix of routes.

The access list and the prefix list options are mutually exclusive simultaneously. But then can be used with the gateway option together.

The asterisk signifies all interfaces.

If a none-existant prefix list or access list is configured on an interface, then all routes will pass.

example

The following example configures prefix and gateway to filter routes received on all interface:

```
router bgp 109
filter * in prefix-list prefix-guize gateway gateway-guize
```

related commands

neighbor distribute-list

neighbor filter-list

neighbor route-map

55.1.60 neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the neighbor default-originate command in address family or router configuration mode. To send no route as a default, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **default-originate**

no neighbor {*ip-address* | *peer-group-name*} **default-originate**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.

default

No default route is sent to the neighbor.

command mode

BGP configuration mode

instruction

This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a match ip address clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also. You can use standard or extended access lists with the neighbor default-originate command.

example

In the following example, the local router injects route 0.0.0.0 to the neighbor 160.89.2.3 rather than to 160.89.2.1:

```
router bgp 109
network 160.89.0.0
neighbor 160.89.2.1 remote-as 100
neighbor 160.89.2.3 remote-as 200
neighbor 160.89.2.3 default-originate
```

related commands

neighbor ebgp-multihop

55.1.61 neighbor description

To associate a description with a neighbor, use the neighbor description command in router configuration mode. To remove the description, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **description LINE**

no neighbor {*ip-address* | *peer-group-name*} **description LINE**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
line	Text that describes the neighbor.

default

There is no description of the neighbor.

command mode

BGP configuration mode

instruction

It is easier for user to understand the configuration to associate a description with a neighbor.

example

In the following example, the description of the neighbor is "peer with abc.com":

```
router bgp 109
network 160.89.0.0
neighbor 160.89.2.3 description peer with abc.com
```

55.1.62 neighbor distribute-list

To distribute BGP neighbor information as specified in an access list, use the neighbor distribute-list command in address family or router configuration mode. To remove an entry, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list name* } {**in | out**}

no neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list name* } {**in | out**}

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
access-list name	Name of a standard or extended access list.
In	Access list is applied to incoming advertisements to that neighbor.
Out	Access list is applied to outgoing advertisements to that neighbor.

default

none

command mode

BGP configuration mode

instruction

Use access-list filters network prefix of BGP routes; use aspath-list filters AS_PATH attribute of BGP routes; use prefix list to filter network prefix of BGP routes.

The access-list option specifies the access list to filter network prefix of routes; the gateway option specifies the access list to filter nexthop attribute of routes; the prefix list option specifies the prefix list filter network prefix of routes.

If you specify a non-existant access list, all routes will be allowed to pass as a result.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

example

The following router configuration mode example applies list beijing to incoming advertisements from neighbor120.23.4.1.

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 distribute-list beijing in
```

related commands

ip aspath-list

neighbor filter-list

ip prefix-list 1

neighbor prefix-list

55.1.63 neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in router configuration mode. To return to the default, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*ip-address* | *peer-group-name*} **ebgp-multihop**

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
ttl	Time-to-live in the range from 1 to 255 hops.

default

For EBGP-speaking neighbor, only directly connected neighbors are allowed, ttl default value is 1; for IBGP-speaking neighbor, ttl default is 255.

command mode

BGP configuration mode

instruction

Under default, BGP connection can not be established unless EBGP neighbors are directly connected ones. The allowable maximum number of hops for EBGP neighbors can be set with the neighbor ebgp-multihop command. Ttl is configured to 255 if not specified. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example allows connections to neighbor 131.108.1.1, which resides on a network that is not directly connected:

router bgp 109:

neighbor 131.108.1.1 ebgp-multihop

related commands

neighbor default-originate

55.1.64 neighbor filter-list

To set up a BGP filter, use the neighbor filter-list command in address family or router configuration mode. To disable this function, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **filter-list** *as-path-list name* {**in | out** }

no neighbor {*ip-address* | *peer-group-name*} **filter-list** *as-path-list name* {**in | out** }

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
as-path-list name	AS-PATH list name. The ip as-path-list command can be used to define this list.
In	Access list applied to incoming routes.
Out	Access list applied to outgoing routes.

default

none

command mode

BGP configuration mode

instruction

Use access-list filters network prefix of BGP routes; use aspath-list filters AS_PATH attribute of BGP routes; use prefix list to filter network prefix of BGP routes.

If you specify a non-existant access list, all routes will be allowed to pass as a result.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

example

In the following router configuration mode example, the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent autonomous system AS123:

```
ip as-path-list shanghai deny _123_
ip as-path-list shanghai deny ^123$

router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
neighbor 128.125.1.1 filter-list shanghai out
```

related commands

ip aspath-list

neighbor distribute-list

ip prefix-list 1

neighbor prefix-list

55.1.65 neighbor maximum-prefix

To control how many prefixes can be received from a neighbor, use the neighbor maximum-prefix command in router configuration mode. To disable this function, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum*

no neighbor {*ip-address* | *peer-group-name*} **maximum-prefix**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
Maximum	Maximum number of prefixes allowed from this neighbor.

default

This command is disabled by default. There is no limit on the number of prefixes.

command mode

BGP configuration mode

instruction

This command allows you to configure a maximum number of prefixes that a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer. When the number of received prefixes exceeds the maximum number configured, the router terminates the peering (by default). However, if the warning-only keyword is configured, the router instead only sends a log message, but continues peering with the sender. If the peer is terminated, the peer stays down until the clear ip bgp command is issued.

example

The following example sets the maximum number of prefixes allowed from the neighbor at 129.140.6.6 to 1000:

router bgp 109

network 131.108.0.0

neighbor 129.140.6.6 maximum-prefix 1000

related commands

clear ip bgp

55.1.66 neighbor next-hop-self

To configure the router as the next hop for a BGP-speaking neighbor or peer group, use the neighbor next-hop-self command in router configuration mode. To disable this feature, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **next-hop-self**

no neighbor {*ip-address* | *peer-group-name*} **next-hop-self**

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.

default

This command is disabled by default.

command mode

BGP configuration mode

instruction

The disposal of nexthop attribute in BGP is more complicated than IGP . It usually follows three rules:

4. For EBGP session, configure the local ip address of BGP connection as the nexthop attribute when sending routes;

5. For IBGP session, configure the local ip address of BGP connection as the nexthop attribute if the routes are locally generated; if the routes are learned from EBGP, the nexthop attribute is to be filled in intactly the packet when sending routes;

6. If the nexthop parameter of the ip address of the routes belong to the network of BGP session, then the nexthop attribute always adopts the former nexthop;

This command is useful in unmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP subnet. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

example

The following example forces all updates destined for 131.108.1.1 to advertise this router as the next hop:

router bgp 109

neighbor 131.108.1.1 next-hop-self

related commands

set ip next-hop 18

55.1.67 neighbor password

To enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers, use the neighbor password command in router configuration mode. To disable this function, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **password** *LINE*

no neighbor {*ip-address* | *peer-group-name*} **password**

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
password	Enables MD5 authentication
LINE	Plainr text password

default

none

command mode

BGP configuration mode

instruction

Use the neighbor remote-as command to specify the neighbor before using this command.

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The length of password should between 1 and 20 characters.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example configures ‘abcd’ as the authentication password of neighbor 120.23.4.1:

router bgp 109
neighbor 120.23.4.1 remote-as 108
neighbor 120.23.4.1 password abcd

related commands

neighbor remote-as

55.1.68 neighbor prefix-list

To prevent distribution of Border Gateway Protocol (BGP) neighbor information as specified in a prefix list, a Connectionless Network Service (CLNS) filter expression, or a CLNS filter set, use the neighbor prefix-list command in address family or router configuration mode. To remove a filter list, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **prefix-list** *prefix-listname* {**in | out**}

no neighbor {*ip-address* | *peer-group-name*} **prefix-list** *prefix-listname* {**in | out**}

parameter

parameter	description
ip-address	IP address of neighbor.
peer-group-name	Name of a BGP peer group.
prefix-list	Prefix list is applied to advertisements of that neighbor
prefix-listname	Prefix list名Name of a prefix list.
In	Filter list is applied to incoming advertisements from that neighbor.
Out	Filter list is applied to outgoing advertisements to that neighbor.

default

none

command mode

BGP configuration mode

instruction

Using prefix lists is one of three ways to filter BGP advertisements. You can also use AS-path filters, defined with the ip as-path access-list global configuration command

and used in the neighbor filter-list command to filter BGP advertisements. The third way to filter BGP advertisements uses access or prefix lists with the neighbor distribute-list command. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group. Use the neighbor prefix-list command in address family configuration mode to filter NSAP BGP advertisements.

example

The following router configuration mode example applies the prefix list named abc to incoming advertisements from neighbor 120.23.4.1:

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 prefix-list abc in
```

The following router configuration mode example applies the prefix list named CustomerA to incoming advertisements from neighbor 120.23.4.1:

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 prefix-list CustomerA in
```

related commands

ip prefix-list

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

neighbor filter-list

55.1.69 neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the neighbor remote-as command in router configuration mode. To remove an entry from the table, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **remote-as** *number*

no neighbor {*ip-address* | *peer-group-name*} **remote-as** *number*

parameter

parameter	description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
Number	Nmuber of autonomous system to which the neighbor belongs.

default

none

command mode

BGP configuration mode

instruction

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the router bgp global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example assigns a BGP router to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 131.108.0.0 and 192.31.7.0 with the neighbor routers.

```
router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1   remote-as 167
neighbor 131.108.234.2   remote-as 109
neighbor 150.136.64.19   remote-as   99
```

related commands

neighbor peer-group (creating)

55.1.70 neighbor route-map

To apply a route map to incoming or outgoing routes, use the neighbor route-map command in address family or router configuration mode. To remove a route map, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **route-map** *map-name* {*in* | *out*}

no neighbor {*ip-address* | *peer-group-name*} **route-map** *map-name* {*in* | *out*}

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP or multiprotocol BGP peer group.
map-name	Name of a route map.
in	Applies route map to incoming routes.
Out	Applies route map to outgoing routes.

default

none

command mode

BGP configuration mode

instruction

It is only based on neighbor to filter routes using distribute-list, prefix-list and as-path-list, while it is not only based on neighbor to filter routes but also based on neighbor to modify the attribute of routes to realize a more flexible routing strategy.

Different routes have different attributes. The route-map can modify attributes of different kinds of routes. If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map. The rules which is valid to BGP route are as follows: match aspath-list、match community-list、match ip address、match ip nexthop、match ip prefix-list、match metric、match tag、set aggregator、set as-path、set atomic-aggregate、set community、set community-additive、set ip nexthop、set local-preference、set metric、set origin、set tag、set weight.

If configured with a non-existent route-map, then all routes is allowed to receive as a result without any modification.

If you specify a BGP or multiprotocol BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

example

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 198.92.70.24:

```
router bgp 5
neighbor 198.92.70.24 route-map internal-map in
route-map internal-map
match as-path abc
set local-preference 100
```

related commands

neighbor peer-group (creating)

route-map 1

55.1.71 neighbor route-reflector-client

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the neighbor route-reflector-client command in address family or router configuration mode. To indicate that the neighbor is not a client, use the no form of this command.

neighbor *ip-address* **route-reflector-client**

no neighbor *ip-address* **route-reflector-client**

parameter

parameter	description
ip-address	IP address of the BGP neighbor being identified as a client.

default

There is no route reflector in the autonomous system.

command mode

BGP configuration mode

instruction

By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a route reflector responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the neighbor route-reflector-client command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

The bgp client-to-client reflection command controls client-to-client reflection.

example

In the following router configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 198.92.70.24.

```
router bgp 5
neighbor 198.92.70.24 route-reflector-client
```

related commands

bgp cluster-id

show ip bgp

55.1.72 neighbor route-refresh

To allow neighbor to use route refresh function, use the neighbor route-refresh command. Use the no form of this command to disable route refresh function.

neighbor *ip-address* **route-refresh**

no neighbor *ip-address* **route-refresh**

parameter

parameter	description
ip-address	BGP neighbor and ip address

default

disabled

command mode

BGP configuration mode

instruction

By default, BGP route exchange for only once when the connection is established, then only exchanging changed routes afterwards. If the routing strategy configuration is modified, it will not become effective immediately. Generally, there are two methods:

- Reset BGP connection
- Use soft-reconfiguration function

The first method is relatively slow, and the routes vary greatly. The second method needs too much storage space and occupies more CPU time. These two methods are not good method, and therefore a new method arises, that is, the route refresh.

The route refresh is a negotiation option based on BGP connection, aiming to send the route refresh request packet to ask neighbor to re-send all update packets to oneself, which do not need to reset BGP connection and also do not need to store a great amount of routes. This a a more ideal solution at the moment.

example

The following example allows neighbor at address 198.92.70.24 to use route refresh function:

router bgp 5

neighbor 198.92.70.24 route-refresh

related commands

show ip bgp neighbors

55.1.73 neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the neighbor send-community command in address family or router configuration mode. To remove the entry, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **send-community**

no neighbor {*ip-address* | *peer-group-name*} **send-community**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.

default

The communities attribute can be sent to the neighbor.

command mode

BGP configuration mode

instruction

The route's group attribute of routes can be configured via the set community command of route-map or via neighbor's routing inform.

Use the show ip bgp neighbors command to see whether allows to send group attribute to neigh or not.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

In the following router configuration mode example, the router belongs to autonomous system 109 and is not permitted to send the communities attribute to its neighbor at IP address 198.92.70.23:

```
router bgp 109
no neighbor 198.92.70.23 send-community
```

related commands

match community-list 4

neighbor peer-group (creating)

set community 15

set community-additive 17

55.1.74 neighbor shutdown

To disable a neighbor or peer group, use the neighbor shutdown command in router configuration mode. To reenable the neighbor or peer group, use the no form of this command.

neighbor {*ip-address* | *peer-group-name}* **shutdown**

no neighbor {*ip-address* | *peer-group-name}* **shutdown**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.

default

none

command mode

BGP configuration mode

instruction

The neighbor shutdown command terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly. To display a summary of BGP neighbors and peer group connections, use the show ip bgp summary command. Those neighbors with an Idle status and the Admin entry have been disabled by the neighbor shutdown command.

related commands

show ip bgp summary

show ip bgp neighbors

55.1.75 neighbor soft-reconfiguration

To configure the software to start storing updates, use the neighbor soft-reconfiguration command in router configuration mode. To not store received updates, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]

no neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
inbound	Indicates that the update to be stored is an incoming update.

default

The incoming update is not stored and the outgoing update is stored.

command mode

BGP configuration mode

instruction

Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration. Outbound BGP soft reconfiguration does not require inbound soft reconfiguration to be enabled.

To use soft reconfiguration, or soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the open message sent when the peers establish a TCP session. Clearing the BGP session using the neighbor soft-reconfiguration command has a negative effect on network operations and should only be used as a last resort. Routers can use the clear ip bgp {* | address | peer-group name} in command to clear the BGP session.

To determine whether a BGP router supports this capability, use the show ip bgp neighbors command. If a router supports the route refresh capability, the following message is displayed:

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example enables inbound soft reconfiguration for the neighbor 131.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy.

```
router bgp 100
neighbor 131.108.1.1 remote-as 200
neighbor 131.108.1.1 soft-reconfiguration inbound
```

related commands

clear ip bgp

neighbor peer-group (creating)

55.1.76 neighbor timers

To set the timers for a specific BGP peer or peer group, use the neighbor timers command in router configuration mode. To clear the timers for a specific BGP peer or peer group, use the no form of this command.

neighbor {*ip-address* | *peer-group-name}* **timers keepalive** *holdtime*

no neighbor {*ip-address* | *peer-group-name*} **timers keepalive** *holdtime*

parameter

parameter	description
ip-address	A BGP peer or peer group IP address.
peer-group-name	Name of the BGP peer group.
Keepalive	Frequency (in seconds) with which the software sends keepalive messages to its peer.
Holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead.

default

keepalive: 60 s

holdtime: 180 s

command mode

BGP configuration mode

instruction

Generally, the value of holdtime is three times larger than keepalive. If you configure 0 as the value of keealive and holdtime, then the sending of keepalive packets is disabled, which needs tcp connection manager to inform BGP module for state change.

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the timers bgp command.

example

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.98.47.10:

router bgp 109

neighbor 192.98.47.10 timers 70 210

55.1.77 neighbor update-source

To have the software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the neighbor update-source command

in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **update-source interface**

no neighbor {*ip-address* | *peer-group-name*} **update-source interface**

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
Interface	Interface name

default

Best local address

command mode

BGP configuration mode

instruction

By default, the ip module decides the local ip address of TCP connection when BGP establishes the connection. IP module decides interface depending on routes, and then binds the main ip address of this interface as the local address of TCP. Use the update-source command can bind the main ip address of the local specified interface during the establishment of TCP connection.

It is generally specified to use loopback interface, for the loopback interface ‘s protocol state is always up. And so this keeps the stability of BGP session and avoids route fluctuation.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface:

router bgp 110

network 160.89.0.0

neighbor 160.89.2.3 remote-as 110

neighbor 160.89.2.3 update-source Loopback0

related commands

neighbor peer-group (creating)

55.1.78 neighbor weight

To assign a weight to a neighbor connection, use the neighbor weight command in address family or router configuration mode. To remove a weight assignment, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **weight** *weight*

no neighbor {*ip-address* | *peer-group-name*} **weight** *weight*

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
Weight	Weight to assign. Acceptable values are from 0 to 65535.

default

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

command mode

BGP configuration mode

instruction

BGP routing metric is the important standard to choose routes. The default metric of all routes that learned from neighbors is 0. Use this command to set metric for routes that learned from neighbor.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following router configuration mode example sets the weight of all routes learned via 151.23.12.1 to 50:

router bgp 109 neighbor 151.23.12.1 weight 50

related commands

neighbor peer-group (creating)

set weight 23

55.1.79 network (BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP), use the network command. To remove an entry from the routing table, use the no form of this command.

network A.B.C.D/n route-map *map-name* **backdoor**

no network A.B.C.D/n route-map *map-name* **backdoor**

parameter

parameter	description
A.B.C.D/n	Network prefix that BGP will advertise
route-map	The specified route map
map-name	Name of the route map
backdoor	Backdoor network

default

No networks are specified.

command mode

BGP configuration mode

instruction

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other peers but not to be included by local IP routing table.

A totally same route in the main routing table of IP is the basis for the network configured with the network command to become effective.

A more precise or totally same route in the local BTP routing table is the basis for the network to become effective that configured with the aggretgate-address command.

The length of mask code is generated in term of standard network type if not specified

Use the route-map to configure route's attribute.

The backdoor network is used to modify route distance rather than to generate routes. It changes route's default distance that learned from the neighbor to the local route's distance. The default value is 200.

The maximum number of network commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

example

The following example sets up network 131.108.0.0/8 to be included in the BGP updates:

```
router bgp 120
network 131.108.0.0/8
```

related commands

redistribute (BGP)

aggregate-address

55.1.80 redistribute(BGP)

To redistribute a route process to Border Gateway Protocol (BGP), use the redistribute command. To remove the redistribute command from the configuration file, use the no form of this command.

redistribute protocol [*process-id*] [route-map *map-name*]

no redistribute protocol [*process-id*] [route-map *map-name*]

parameter

parameter	description
protocol	Type of routing protocol
process-id	Process id of routing protocol, such as process if of ospf

route-map	Applies route map to configure route attribute
map-name	Name of route map

default

disabled

command mode

BGP configuration mode

instruction

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other peers but not to be included by local IP routing table.

Use redistribute command to include routes dynamically to BGP. The change of route source will be reflected to BGP automatically. The automatically-included routes will be informed to other neighbors. The configuration of the redistribute command will re-check the specified type of routes in the routing table. The outer routes in OSPF will not be included to BGP.

Use the route-map to configure route's attribute.

example

The following example configures routes from OSPF process 23 to be redistributed into BGP:

```
router bgp 109
redistribute ospf 23
```

related commands

route-map 1

55.1.81 router bgp

To configure the BGP routing process, use the router bgp command in global configuration mode. To remove a routing process, use the no form of this command.

router bgp *as-number*

no router bgp *as-number*

parameter

parameter	description
as-number	Number of autonomous system

default

No BGP routing process is enabled by default.

command mode

global configuration mode

instruction

The system allows to configure one BGP process at most. The BGP task is established in the process of system initialization, and it is activated when the BGP process is started up. The BGP task only receives information from command module without configuring the BGP process. It is not related to routing module or any other module and will not response other information. The related show and clear command are all invalid.

Use no router bgp command to delete BGP process, and at the same time other configuration related to BGP will also be deleted, such as neighbors and so on. The BGP route in routing table is also be deleted.

To configure BGP process using the show running and show ip bgp summary command to check.

example

The following example configures a BGP process for autonomous system 200:

router bgp 200

related commands

neighbor remote-as

55.1.82 show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the show ip bgp command in user EXEC or privileged EXEC mode.

show ip bgp [**network**]

parameter

parameter	description
network	Displays the specified routing information

command mode

EXEC

instruction

The show ip bgp command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

example

The following is a group of BGP displaying information. The former two lines display some marked information.

Status code indicates the status of the table entry. The status is displayed at the beginning of each line in the table. S indicates the table entry is suppressed, which is the invalid route and will not be chosen. D indicates the table entry is dampened, which is the invalid route. H indicates the table entry history, which is not a ture route and is the invalid route. “* “indicates the table entry is valid, which can be chosen as the best route.” > “indiates the table entry is the best entry to use for that network. “I” indicates the table entry was learned via an internal BGP (iBGP) session.

Origin codes indicates the origin of the entry. I is the entry originated from an Interior Gateway Protocol (IGP). E is the entry originated from an Exterior Gateway Protocol (EGP). ? is the origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.

IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network. Local preference value as set with the set local-preference route-map configuration command. The default value is 100. Weight of the route as set via autonomous system filters. Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The last line displays number of routes, including all valid and invalid routes.

```
B3710_118#show ip bgp
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  192.168.10.0/24  192.168.69.5                         0 10 400 i
```

```
*>i192.168.10.0/24      192.168.69.14                100        0 (65030) 400 i
*>i192.168.11.0/24      192.168.69.14                100        0 (65030) 400 i
*   192.168.65.0/30     192.168.69.1                 100        0 (65020) 10 ?
*> 192.168.65.0/30      192.168.69.5                            0 10 ?
*   192.168.65.4/30     192.168.69.1                 100        0 (65020) 10 ?
*> 192.168.65.4/30      192.168.69.5                            0 10 ?
*   192.168.65.8/30     192.168.69.1                 100        0 (65020) 10 ?
*> 192.168.65.8/30      192.168.69.5                            0 10 ?
*   192.168.66.0/30     192.168.66.2                 100        0 (65020) ?
*> 192.168.66.0/30      0.0.0.0                                 32768 ?
* i192.168.66.4/30      192.168.66.6                 100        0 ?
*> 192.168.66.4/30      0.0.0.0                                 32768 ?
*>i192.168.66.8/30      192.168.66.6                 100        0 ?
*>i192.168.67.0/30      192.168.69.18          200   100        0 500 ?
```

Number of displayed routes: 15

related commands

show ip bgp community

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

55.1.83 show ip bgp community

To display routes that belong to specified BGP communities, use the show ip bgp community command in EXEC mode.

show ip bgp community

parameter

none

command mode

exec

instruction

This command is used to display statistics information of BGP communities attribute structure in the system.

related commands

show ip bgp

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

55.1.84 show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the show ip bgp neighbors command.

show ip bgp neighbors [*ip-address*] [**received-routes | routes** | **advertised-routes**]

parameter

parameter	description
ip-ddress	IP address of a neighbor. If this parameter is omitted, information about all neighbors is displayed.
received-routes	Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the received-routes keyword.
advertised-routes	Displays all routes that have been advertised to neighbors.

command mode

EXEC

instruction

Use the show ip bgp neighbors command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

related commands

show ip bgp

show ip bgp community

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

55.1.85 show ip bgp paths

To display all the BGP paths in the database, use the show ip bgp paths command in EXEC mode.

show ip bgp paths

parameter

none

command mode

EXEC

instruction

This command is used to display statistics information of BGP paths structure.

related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

55.1.86 show ip bgp prefix-list

To display information about a prefix list or prefix list entries, use the show ip prefix-list command.

show ip bgp prefix-list {*prefix-list name*}

parameter

parameter	description
prefix-list name	Name of prefix-list

command mode

EXEC

instruction

This command specifies prefix-list to filter display of the show ip bgp command. Only the routes matching the prefix-list will be displayed.

related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

ip prefix-list

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

55.1.87 show ip bgp regexp

To display routes matching the autonomous system path regular expression, use the show ip bgp regexp command in EXEC mode.

show ip bgp regexp regular-expression

parameter

parameter	description
regular-expression	Regular expression to match the BGP autonomous system paths.

command mode

EXEC

instruction

This command specifies the regular expression to filter the display of the show ip bgp command. Only the routes matching the regular expression will be displayed.

related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

55.1.88 show ip bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the show ip bgp summary command.

show ip bgp summary

parameter

This command has no parameters or keywords.

command mode

EXEC

instruction

The show ip bgp summary command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route. A path is a route to a given destination. By default, BGP will install only a single path for each destination. If multipath routes are configured, BGP will install a path entry for each multipath route, and only one multipath route will be marked as the bestpath.

BGP attribute and cache entries are displayed individually and in combinations that affect the bestpath selection process. The fields for this output are displayed when the related BGP feature is configured or attribute is received. Memory usage is displayed in bytes.

example

The following is sample output from the show ip bgp summary command:

router bgp 4
BGP local AS is 4
Router ID is 192.168.20.72
IGP synchronization is enabled
Distance: external 20 internal 200

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/Pref
192.168.20.12	4	5	0	0	0	0	0	never	Connect

related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

55.1.89 synchronization

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the synchronization command in address family or router configuration mode. Use the no form of this command to disable this function.

synchronization

no synchronization

parameter

none

default

enabled

command mode

BGP configuration mode

instruction

Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. By default, synchronization between BGP and the IGP is turned off to allow the software to advertise a network route without waiting for route validation from the IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

IGP function is enabled by default.

To enable to advertise a network route without waiting for the IGP, use the no form of this command.

example

The following example enables router to advertise the route without waiting for IGP synchronization.

```
router bgp 120
no synchronization
```

related commands

router bgp

55.1.90 table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the table-map command in address family or router configuration mode. To disable this function, use the no form of the command.

table-map <*name*>

no table-map <*name*>

parameter

parameter	description
name	Route map name from the route-map command.

default

none

command mode

BGP configuration mode

instruction

This command adds the route map name defined by the route-map command to the IP routing table. This command is used to set the tag name and the route metric to implement redistribution.

example

none

related commands

none

55.1.91 timers

To adjust BGP network timers, use the timers bgp command. To reset the BGP timing defaults, use the no form of this command.

timers bgp <*keepalive*> <*holdtime*>

no timers bgp <*keepalive*> <*holdtime*>

parameter

parameter	description
keepalive	Frequency (in seconds) with which the software sends keepalive messages to its peer.
holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead.

default

Keepalive: 60 seconds

Holdtime: 180 seconds

command mode

BGP configuration mode

instruction

Configure BGP neighbor clock in global configuration mode to modify default clock configuration. The configuration towards neighbor is prior to global configuration.

example

The following example changes the keepalive timer to 10 seconds and the hold-time timer to 40 seconds:

router bgp 100

timers bgp 10 40

related commands

neighbor timers

Chapter 56 IP Hardware Subnet Routing Configuration Commands

56.1 ip exf

Syntax

[no] ip exf

Parameter

N/A

Default value

Enabled

Command mode

Global configuration mode

Remarks

The IP hardware subnet routing function can be enabled through this command. If this function is not enabled, the hardware forwarding items can still be configured but they invalidates.

Example

The following example shows how to enable the IP hardware subnet route.

```
Switch_config#ip exf
```

56.2 ip exf down-up-threshold

Syntax

ip exf down-up-threshold *rate*

no ip exf down-up-threshold

Parameter

Name	Remarks
down-up-threshold *rate*	Stands for the trigger value (percent) of hardware subnet routing switch.

Default value

90

Command mode

Global configuration mode

Remarks

When the number of software routes exceeds the trigger value of hardware subnet routing, the hardware subnet routing will be shut down; when the number of software routes lowers to be less than the trigger value, the hardware subnet routing will be opened again.

Example

The following example shows how to enable the hardware subnet routing on a L3 switch and set the trigger value to 80%.

ip exf down-up-threshold 80

56.3 debug ip exf

Syntax

[no] debug ip exf

Parameter

N/A

Default value

N/A

Command mode

EXEC

Remarks

It is used to enable or disable the debugging switch of IP EXF.

Example

The following are common examples of debugging information output.

2004-7-30 15:50:40 [EXF]: EXF entry(destination 2.10.0.0/16) delete from hardware table, EXF disabled
It means that user enters the **no ip exf** command and all **exf** items invalidate.

2004-7-30 15:50:44 [EXF]: EXF entry(destination 2.10.0.0/16) add to hardware, NAT enabled, nexthop CPU
It means that the NAT function is enabled at the port where the next hop of the configured **exf** item belongs. In this case, the packet of the **exf** item is transmitted to CPU for processing.

2004-7-30 15:52:03 [EXF]: EXF entry(destination 2.9.0.0/16) add to hardware, no ARP, nexthop CPU
It means that the ARP of the IP address of the next hop of the configured **exf** item is not learned. In this case, the packet of the **exf** item is transmitted to CPU for processing.

2004-7-30 15:50:44 [EXF]: EXF entry(destination 2.3.0.0/16) add to hardware sucessfully
It means that the EXF entry is configured successfully.

2004-7-30 15:56:00 [EXF]: EXF entry(destination 2.2.0.0/16) delete from hardware table by command
It means that the EXF entry is deleted through the corresponding command.

2004-7-30 15:56:59 [EXF]: EXF entry(destination 2.3.0.0/16) delete from hardware table, delete by interface
It means that the interface for the next hop of the configured EXF entry is down or the EXF entry becomes invalid because of NAT settings.

Chapter 57 IP-PBR Configuration Commands

IP-PBR configuration commands include:

- ip pbr
- show ip pbr
- show ip pbr policy
- show ip pbr exf
- debug ip pbr

57.1.1 ip pbr

Description

ip pbr
no ip pbr

Parameter

None

Default value

The IP-PBR function is disabled by default.

Description

It is used to enable or disable the IP-PBR function. The **no ip pbr** command is used to resume the default value.

Example

```
switch(config)# ip pbr
switch(config)#
```

57.1.2 show ip pbr

Description

show ip pbr

Parameter

None

Default value

None

Description

It is used to display the information about RIP configuration.

Example

The following example shows how to display the information about IP-PBR running.

```
switch(config)# show ip pbr
  IP policy based route state: enabled


  No equiv exf apply item


  VLAN3 use route-map ddd, and has 1 entry active.
  ------------------
  Entry sequence 10, permit
    Match ip access-list:
      ac1
    Set Outgoing nexthop
      90.0.0.3
switch(config)#
```

57.1.3 show ip pbr policy

Description

show ip pbr policy

Parameter

None

Default value

None

Description

It is used to display the information about RIP configuration.

Example

The following example shows how to display the information about IP-PBR policy routing configuration.

```
IP policy based route state: enabled


VLAN3 use route-map ddd, and has 1 entry active.
------------------
Entry sequence 10, permit
  Match ip access-list:
    ac1
  Set Outgoing nexthop
 90.0.0.3
switch(config)#
```

57.1.4 show ip pbr exf

Description

show ip pbr exf

Parameter

None

Default value

None

Description

It is used to display the information about IP-PBR equivalent routing.

Example

The following example shows how to display the information about IP-PBR equivalent routing.

```
switch(config)# show ip pbr exf
```

IP policy based route state: enabled

Equiv EXF has 1 entry active.

Entry sequence 1, handle c1f95b0

Dest ip: 1.1.0.0/16

90.0.0.3

192.168.213.161

switch(config)#

57.1.5 debug ip pbr

Description

debug ip pbr
no debug ip pbr

Parameter

None

Default value

None

Description

It is used to enable or disable the debugging switch of IP-PBR.

Example

The following example shows how to enable the debugging switch of IP-PBR.

switch(config)# debug ip pbr

switch(config)#

Chapter 58 VRRP Configuration Commands

58.1 VRRP Configuration Commands

The VRRP protocol (RFC2338) is supported, and the extended track and preempt delay functions are added.

58.1.1 vrrp associate

To configure basic IP and secondary IP of the VRRP group, and activate VRRP, run **vrrp associate**. To cancel the configured IP and stop VRRP group, run **no vrrp associate**.

[**no**] **vrrp associate** *group-number ip-address netmask* [**secondary**]

no vrrp associate

Parameter

Parameter	Description
group-number	Added VRRP group numberIts default value is 0.
ip-address	Added IP address
netmask	Network address mask
secondary	Means that the currently-configured IP is a secondary IP.

Default

There is no default value.

Command mode

Interface configuration mode

Explanation

The added virtual IP address of VRRP can be the basic IP address of VRRP or the VRRP secondary IP address. This IP address (basic IP or secondary IP) cannot belong to the network segment where any other interface's IP lies, or cannot belong to the network segment where any interface module’s IP or global application module’s IP lies. Except that basic VRRP IP can be same to the basic IP of the interface where basic vrrp IP lies, the configured VRRP IP cannot be same to the IP of any current interface. However, the IP of the current interface and the configured VRRP IP can be in the same network segment.

You can run **no vrrp [group-number] associate** to cancel all VRRP IP addresses of the current interface group.

When an IP address of a VRRP group is same to the basic IP address of the current interface, VRRP enters the owner state, which is a special master state. The owner state has the following attributes: the precedence of the group is automatically changed to 255; this group must be in master state; the configured track gets ineffective in this case.

Example

The following example shows how to configure basic IP address and secondary IP address on interface ethernet1/0:

interface ethernet1/0

vrrp 3 associate 100.1.1.1

vrrp 3 associate 100.1.1.2 secondary

58.1.2 vrrp description

To configure the description of the interface, run **vrrp *group-number* description WORD**. To cancel the description of the interface, run no **no vrrp description WORD**.

vrrp *group-number* **description WORD**

no vrrp description WORD

Parameter

Parameter	Description
group-number	Group number, whose default value is 0
WORD	Configures the description character string of the group.

Default

There is no default value.

Command mode

Interface configuration mode

Explanation

This command is just to configure a description for an interface and has no effect on other functions of the interface.

Example

vrrp 3 description Shanghai_dial

58.1.3 vrrp priority

To configure the priority of a group, run **vrrp [*group-number*] priority *<1-254>***. To cancel the configured priority of the group and resume its default value, run **no vrrp [*group-number*] priority**.

vrrp [*group-number***] priority** *<1-254>*

no vrrp [*group-number***] priority**

Parameter

Parameter	Description
group-number	Group number, whose default value is 0
<1-254>	A value between 1 and 254

Default

The default value is 100.

Command mode

Interface configuration mode

Explanation

When the priority of a group is configured in the owner state, the priority can be configured but cannot be used currently for the current priority is 255. When the group is in owner state, its priority automatically changes to 255.

Example

vrrp 3 priority 180

58.1.4 vrrp preempt

To configure the preemption mode of a group, run **vrrp *group-number* preempt**. The preemption delay can also be configured.

[**no**] **vrrp** *group-number* **preempt**

[**no**] **vrrp** *group-number* **preempt delay** *<1-255>*

Parameter

Parameter	Description
group-number	Group number, whose default value is 0

<1-255>	Configured preemption delay, whose unit is second

Default

It is the preemption mode by default.

Command mode

Interface configuration mode

Explanation

When this group receives an advertise packet with a lower priority in preemption mode, this group would not update the master down timer and the preemption will occur later. If the preemption mode is not configured, the master down timer will carry on update even if this group's priority is higher than the packet's.

The preemption delay means the minimum time which has to wait before the preemption. When a packet with comparatively lower priority is received by this group, the master down timer will be updated as the delay value if the master down timer is shorter than the configured preempt delay.

The preemption is canceled and the preemption delay is set to 0.

Example

vrrp 3 preempt
vrrp 3 preempt delay 10

58.1.5 vrrp track

To track an interface, run **vrrp *group-number* track interface *interface-number* *<1-255>***.
When the tracked interface changes, you can justify its priority.

[**no**] **vrrp** *group-number* **track interface** *interface-number* *<1-255>*

Parameter

Parameter	Description
group-number	Group number, whose default value is 0
Interface-number	Interface number, such as f0/0
<1-255>	Configured preemption delay, whose unit is second

Default

There is no default value.

Command mode

Interface configuration mode

Explanation

When a group is configured with a track function and the protocol of the tracked interface changes to **down**, the priority of the group decreases to the configured value; if the protocol of the tracked interface changes to **up**, the priority of the group increases to the configured value.

Currently only the state of the link protocol of the interface can be tracked. The following actions will lead the change of the protocol state: the cut-off of the network cable that the interface connects, interface's shutdown and link protocol's disconnection.

When the group is in owner state, the configured track function will automatically get ineffective.

Example

vrrp 3 track interface ethernet2/1 20

no vrrp 3 track interface ethernet2/1

58.1.6 vrrp authentication

To configure the authentication character string of the VRRP group, run **vrrp *group-number* authentication WORD**.

[**no**] **vrrp** *group-number* **authentication WORD**

Parameter

Parameter	Description
group-number	Group number, whose default value is 0
WORD	An eight-byte authentication string

Default

The authentication string is null by default and the authentication is not performed.

Command mode

Interface configuration mode

Explanation

The packet received by a VRRP group is effective only when its authentication string is same to the configured authentication string. Pay attention that multiple masters will exist concurrently if different authentication strings appear in the same group during configuration.

Example

vrrp 3 authentication
no vrrp 3 authentication

58.1.7 vrrp timers

To configure the value of advertisement timer of the VRRP group, run **vrrp timers**.

[**no**] **vrrp** *group-number* **timers advertise** *<1-255>*

[**no**] **vrrp** *group-number* **timers advertise dsec** *<5-360>*

[**no**] **vrrp** *group-number* **timers learn**

Parameter

Parameter	Description
group-number	Group number, whose default value is 0
<1-255>	Configured time of advertise, whose unit is second
<5-360>	Configured time of advertise, whose unit is 0.1 second
learn	Configures the learning mode of advertise.

Default

The default value of the timer is 1 second.

The learning does not perform by default.

Command mode

Interface configuration mode

Explanation

This command is used to configure the value of the advertise timer in second. The value of master down timer is calculated through the advertise timer, and the value is [3*advertise, 3*advertise+256/(256-priority)].

Only when a group has no configured timer value and the learning ability has been set can the group learn the advertise timer value from the master-transmitted packets.

When using this command, you are recommended to use the same value.

Example

vrrp 3 timers advertise 3
vrrp 3 timers advertise dsec 15
no vrrp 3 timers advertise
vrrp 3 timers learn

58.1.8 show vrrp

To display the current running state of VRRP, run the following command:

show vrrp interface interface-numer [detail]

show vrrp brief

show vrrp detial

Parameter

detail：Displays the details about the running state.

Default

There is no default value.

Command mode

Interface command mode/configuration mode/privileged mode

Explanation

This command is used to display the running state of the currently-configured VRRP.

The **brief** mode is to display only the simple state, and the group in init state will not be displayed.

However, the **detail** mode can display more information about the configured group.

Example

show vrrp interface e2/1 detail

show vrrp brief

58.1.9 debug vrrp

To debug VRRP, run the following commands:

debug vrrp interface interface-number group-number all | packets | errors | events

debug vrrp all | packets | errors | events

no debug vrrp

Parameter

Parameter	Description
interface-number	Interface number
group-number	Number of the group

Default

There is no default value.

Command mode

Privileged mode

Explanation

This command can be used to export the debugging information about the error, packet and event of VRRP. The **all** parameter means that all three events will be exported.

Example

debug vrrp interface e2/1 3 all

no debug all

Chapter 59 Basic Multicast Commands

59.1 Basic Multicast Commands

59.1.1 debug ip mpacket

If you want to track the process for the multicast packet, you can use this command "**debug ip mpacket**", and use the"**no**" forma of the command to close debug information.

debug ip mpacket *access-list group-address* **detail**

no debug ip mpacket

Parameter

Parameter	Description
access-list	Range for tracked multicast packets
group-address	The tracked multicast packet group address
detail	Details for multicast packet processing

Default

Close debug information output

Command mode

Supervisor mode

Explanation

You can use this command to track the main process for igmp-host end protocol.

Example

The following example shows some situations for multicast packet processing.

You have received the (100.168.20.151,224.1.1.1) packet on e0/1 port, and the packet length is 112 bytes.

You have sent the (192.168.20.99,224.0.0.5) packet on e0/1 port, and the packet length is 64 bytes.

router#debug ip mpacket

MINPUT : IP Ethernet0/1 (100.168.20.151,224.1.1.1) , len=112

MOUTPUT : IP Ethernet0/1 (192.168.20.99,224.0.0.5) , len=64

59.1.2 debug ip mrouting

Use this command “debug ip mrouting” to enable “mrouting” tracking function, then you can see the change from the multicast transfer list. In addition, use the”**no**” forma of the command to close debug information.

Syntas

debug ip mrouting

no debug ip mrouting

Parameter

None

default

Close all tracking functions.

Command mode

Supervisor mode

Explanation

You can use this command to see the change from the multicast transfer list, such as (S, G)/(*,G) adding/deleting and downstream interface adding/deleting.

Example

The following example shows you some changes from the multicast transfer list. First the (192.168.20.110, 239.0.0.100) item is created, and then Loopback0 is added for downstream interface. Finally, the item is deleted due to timeout.

router#debug ip mrouting

MBR: create (192.168.20.110, 239.0.0.100)

MBR: w/ oif Loopback0

MBR: delete (192.168.20.110, 239.0.0.100)

Relevant command

ip multicast-routing

59.1.3 debug ip mroute-cache

Use this command “debug ip mrouting” to enable “mroute-cache” tracking function, then you can see the change from the multicast routing cache. In addition, you can use the “no”format of the command to close the tracking.

Syntas

debug ip mroute-cache *group-address*

no debug ip mroute-cache

Parameter

Parameter	Description
group-address	The tracked multicast routing cache group address

Default

Close all tracking functions.

Command mode

Supervisor mode

Explanation

You can use this command to see the change of the adding/deleting of multicast routing cache.

Example

The following example shows you some changes on the multicast routing cache, and the creating and timeout of (192.168.20.97,230.0.0.1) cache.

router#debug ip mroute-cache
MRC: create (192.168.20.97,230.0.0.1) mroute-cache
MRC: expired (192.168.20.97,230.0.0.1) mroute-cache

59.1.4 debug ip multicast

You can use this command “**debug ip multicast**” to enable multicast event tracking function, and then see the interaction between the multicast protocol and mrouting. you can use the “**no**”format of the command to close the function.

Syntas

debug ip multicast [**alert** | **border-router**]

no debug ip multicast [**alert** | **border-router**]

Parameter

Parameter	Description
alert	Track the alert interaction among multicast routing components
border-router	Track related events of multicast border router MBR

default

Close all tracking functions.

Command mode

Supervisor mode

Explanation

Defining some standard events between multicast routing protocol and mrouting indicates “alert”, for example: creation alert/deletion alert which related (S,G). You can use “debug ip multicast alert” to see these alerts.

’s multicast routing protocol supports MBR, and each multicast routing protocol is a “component”. You can use “debug ip multicast border-router” to see the component’s running information.

Example

In the following example, the alert router is turned on for output:

router#debug ip multicast alert
MBR: [(S, G) deletion alert], originated by OLNK, sent to all components
MBR: [(S, G) creation alert], originated by NONE, sent to all components
MBR: src = 192.168.20.110, grp = 239.0.0.100
MBR: sent to owner OLNK first
MBR: [(S, G) join alert], originated by NONE, sent to OLNK
MBR: src = 192.168.20.110, grp = 239.0.0.100
MBR: [(S, G) firstuse alert], originated by NONE, sent to OLNK
MBR: src = 192.168.20.110, grp = 239.0.0.100
MBR: [(S, G) deletion alert], originated by OLNK, sent to all components
MBR: src = 192.168.20.110, grp = 239.0.0.100

59.1.5 ip mroute

Use the command “ip mroute” to configure the static multicast routing, and use “no ip mroute” to delete the configured static multicast routing.

Syntas

ip mroute *source-address mask* [*rpf-address type-number* [**distance**]]

no ip mroute *source-address mask* [*rpf-address type-number* [**distance**]]

Parameter

Parameter	Description
source-address	Multicast source IP address
mask	Multicast source IP address mask
rpf-address	RPF address of Static multicast routing
type-number	RPF interface of Static multicast routing
distance	Optional management distance

Default

The default management distance is 0.

Command mode

global configuration mode

Explanation

This command allows you to manually configure the location information for the multicast source. It is used when the multicast and unicast topologies are not identical.

Example

The following example will configure a static multicast routing through the specified interface:

router_config#ip mroute 100.1.1.0 255.255.255.0 192.1.1.1 f0/0

Relevant command

show ip mroute static

59.1.6 ip mroute-cache

Use this command “ip mroute-cache” to configure a multicast routing cache on the port, and “no ip mroute-cache” to disable the multicast routing cache.

Syntas

ip mroute-cache

no ip mroute-cache

Parameter

None

Default

The default is to use the multicast routing cache on the port.

Command mode

interface configuration mode

Explanation

Use the command when a port uses the multicast routing cache to receive/send the packet, ip will search the cache when a multicast packet is received. If there is no routing information in the cache, the port will ask for multicast routing module.

Example

The following example will enable multicast routing cache on interface e1/0.

router_config_e1/0#ip mroute-cache

Relevant command

show ip mroute-cache

59.1.7 ip multicast-routing

Use this command “ip multicast-routing” to enable IP multicast packet transferring function, and “no ip multicast-routing” to disable the function.

Syntas

ip multicast-routing

no ip multicast-routing

Parameter

none

Default

The default is not to transfer multicast packets.

Command mode

global configuration mode

Explanation

If you disable this function, the router will no longer transfer multicast packets, meanwhile, the multicast routing list and the multicast cache will be empty.

Example

The following example will configure the router to transfer multicast packets:

router_config#ip multicast-routing

Relevant command

show ip mroute mfc

59.1.8 ip multicast route-limit

Use this command “ip multicast route-limit” to configure the maximum number of multicast routing item, and “no ip multicast route-limit” to un-limit the number.

Syntas

ip multicast route-limit *size*

no ip multicast route-limit *size*

Parameter

Parameter	Description
size	Maximum number of multicast routing item

Default

The default multicast routing item number is unlimited.

Command mode

global configuration mode

explanation

If you have configured this function, the multicast routing item number will be limited.

example

The following example will configure the maximum number of multicast routing list to 2000:

router_config#ip multicast route-limit 2000

Relevant command

show ip mroute mfc

59.1.9 ip multicast boundary

Use this command "**ip multicast boundary**" to manage the range for the port allowed processing multicast packets; it is valid for input/output packets on the port. use "**no ip multicast boundary**" to cancel this command.

Syntas

ip multicast boundary *access-list*

no ip multicast boundary

Parameter

Parameter	Description
access-list	the access-list name used to specify the range for processing multicast

	packets.

Default

Process all multicast packets.

Command mode

interface configuration mode

Explanation

If the function is configured, the range for the port allowed processing multicast packets will be limited.

Example

The following example will configure the range for the port e1/0 allowed processing multicast packets to the range limited by the access-list testacl:

router_config_e1/0#ip multicast boundary testacl

59.1.10 ip multicast helper-map

Use this command “ip multicast helper-map” to configure the connection of two broadcast networks with the multicast routing on the multicast network, and “**no ip multicast helper-map**” to cancel this command.

ip multicast boundary helper-map {*group-address*|**broadcast**} {*broadcast-address* |*multicast-address* } *access-list*

no ip multicast boundary helper-map {*group-address*|**broadcast**} {*broadcast-address* | *multicast-address* } *access-list*

Parameter

Parameter	Description
group-address	The multicast packet group address which needed to be converted to the broadcast packet. it is used with the broadcast-address keyword.
broadcast	It can convert the broadcast packet to the multicast packet. it is used with the multicast-address keyword.
broadcast-address	The target address of broadcast packet which is sent after converting. it is used with the group-address keyword.
multicast-address	The target address of multicast packet which is sent after converting. It is used with the broadcast keyword.
access-list	IP extended access-list name. You can use it to specify the port number for packet converting.

Default

Not perform the conversion between any multicast packets and broadcast packets.

Command mode

interface configuration mode

Explanation

If two broadcast networks are connected with a multicast network, you can convert the broadcast flow to multicast flow on the first hop router connected with the source broadcast network, and then convert the multicast flow to broadcast flow on the last hop router connected with the target broadcast network. Thus, you can utilize the multicast network's multicast characteristic between the two broadcast networks which are required to be connected with each other. Furthermore, it can prevent the packets between two broadcast networks from being sent repeatedly, and utilize the "quick forward" characteristic on the multicast network.

Before using "ip multicast helper-map", you should have configured this command "ip directed-broadcast" on the port.

Example

Configuration on the router is as follow:

if you configure command"ip directed-broadcast" on port e0 of the first hop router, it will be allowed to process the link broadcast packets.

If you have configured "ip multicast helper-map broadcast 230.0.0.1 testacl1", you can convert the udp broadcast packet, whose port number is 4000("ip forward-protocol" command specified) and the source address is 192.168.20.97/24 (testacl1 specified) ,to multicast packet whose target address is 230.0.0.1 ("ip multicast helper-map" command specified).

if you configure command"ip directed-broadcast" on port e1 of the last hop router, it will be allowed to process the link broadcast packets.

If you have configured "ip multicast helper-map broadcast 230.0.0.1 172.10.255.255 testacl2", you can convert the multicast packet, whose port number is 4000("ip forward-protocol" command specified), the source address is 192.168.20.97/24 (testacl2 specified) and target address is 230.0.0.1 ,to broadcast packet whose target address is 170.10.255.255 ("ip multicast helper-map" command specified).

On the first hop router which is connected with the source broadcast network:

```
interface ethernet 0
ip directed-broadcast
ip multicast helper-map broadcast 230.0.0.1 testacl
ip pim dense-mode
!
ip access-list extended testacl    permit udp 192.168.20.97 255.255.255.0 any
```

ip forward-protocol udp 4000

On the last hop router which is connected with the target broadcast network:

interface ethernet 1
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim dense-mode
!
ip access-list extended testacl2 permit udp 192.168.20.97 255.255.255.0 any
ip forward-protocol udp 4000

Relevant command

ip forward-protocol

ip directed-broadcast

59.1.11 ip multicast rate-limit

Use this command "**ip multicast rate-limit**" to limit the multicast packet flow receiving and sending in the range of a source/group on the port, and "**no ip multicast rate-limit**" to cancel this flow limitation.

Syntas

ip multicast rate-limit {**in** | **out**} [**group-list** *access-list*] [**source-list** *access-list*] kbps

no ip multicast rate-limit {**in** | **out**} [**group-list** *access-list*] [**source-list** *access-list*]

Parameter

Parameter	Description
in	Limit the input packet flow on the port.
out	Limit the output packet flow on the port.
group-list *access-list*	(optional) Limit the multicast packet flow for the group address in access-list.
source-list *access-list*	(optional) Limit the multicast packet flow for the source address in access-list.
kbps	(optional) Allowed maximum flow. If its value is 0, no packet will be allowed to pass.

Default

No limitation to the flow.

Command mode

interface configuration mode

Explanation

The packet flow in specified range has exceeded the limit at last second. You have to discard the packet, or the packet will be forwarded.

Example

The maximum output packet flow rate on port s0 (192.168.20.97 , 230.0.0.1) is limited to 64kbps.

interface serial 0

ip multicast rate-limit out group-list gacl source-list sacl 64

ip access-list standard sacl

permit 192.168.20.97 255.255.255.255

ip access-list standard gacl

permit 230.0.0.1 255.255.255.255

59.1.12 ip multicast ttl-threshold

Use this command “ip multicast ttl-threshold” to configure the maximum threshold value of multicast packet ttl on the port, and “no ip multicast ttl-threshold” to restore default.

Syntas

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold

Parameter

Parameter	Description
ttl-value	The multicast packet ttl threshold value on the port.

Default

The default ttl threshold value on the port is 1.

Command mode

interface configuration mode

Explanation

The ttl value of receiving/sending packet should be largerer than the specified threshold value on the port, you can use this command to configure a router to border router.

Example

The ttl threshold value configured on port s0 is 200, it means only the multicast packet with ttl value more than 200 is allowed to be received/sent on the port.

interface serial 0

ip multicast ttl-threshold 200

59.1.13 show ip mflow

You can use this command “show ip mflow” to display global flow information processed by system and multicast flow information processed on the port.

Syntas

show ip mflow [*group-address*|*source-address*]**interface**

Parameter

Parameter	Description
group-address	The displayed multicast flow information group address.
source-address	The displayed multicast flow information source address.
interface	The displayed port multicast flow information.

Default

none

Command mode

Supervisor mode

Explanation

Display the processed packet number from the multicast flow, wrong incoming interface packet number, and current flow value.

Example

The following example will display global multicast flow information:

router#show ip mflow
IP Multicast Flow
(100.168.20.151,224.1.1.1)
total process : 0 wrong_if_count : 0 curr-flux : 0.00
(192.167.20.131,239.1.1.1)
total process : 0 wrong_if_count : 0 curr-flux : 0.00

The following example will display port multicast flow information:

router#show ip mflow **interface** e0/1

IP Multicast Flow
(192.168.20.97,230.0.0.1)
total recv : 21180 total send : 0 curr-in-flux : 0.00 curr-out-flux : 0.00
(100.168.20.151,224.1.1.1)
total recv : 16822400 total send : 0 curr-in-flux : 0.00 curr-out-flux : 0.00
(192.168.20.97,232.0.0.1)
total recv : 240 total send : 0 curr-in-flux : 0.00 curr-out-flux : 0.00
(192.167.20.131,239.1.1.1)
total recv : 103264 total send : 0 curr-in-flux : 0.90 curr-out-flux : 0.00

59.1.14 show ip mroute-cache

use this command “show ip mroute-cache” to display the information on the multicast routing cache.

Syntas

show ip mroute-cache [*group-address*]

Parameter

Parameter	Description
group-address	The displayed multicast routing cache group address

Default

none

Command mode

Supervisor mode

Explanation

MRC (Multicast Route Cache) is a global multicast routing cache, and every MRC item contains the (S, G)/ (*, G) information, upstream/downstream interface information received from the multicast routing.

Example

The following example will display multicast routing list information:

```
router#show ip mroute-cache
IP Multicast Route Cache
(192.168.20.97, 230.0.0.1)|(192.168.20.97,230.0.0.1)
  Incoming interface: Ethernet0/2, Last used : 00:00:34
  Outgoing interface list:
    Loopback0
(192.168.20.97, 230.0.0.2)|(192.168.20.97,230.0.0.2)
  Incoming interface: Ethernet0/2, Last used : 00:00:12
  Outgoing interface list:
    Loopback1
```

59.1.15 show ip mroute mfc

You can use this command “show ip mroute mfc” to display the multicast forwarding list information, and then activate the multicast function.

Syntas

show ip mroute mfc

Parameter

none

Default

none

Command mode

Supervisor mode

Explanation

MFC (Multicast Forwarding Cache) is a global multicast forwarding list, and the multicast packet is forwarded by it. Every MFC item has (S, G)/ (*, G) information and upstream/downstream interface information.

Example

The following example will display multicast routing list information:

```
router#show ip mroute mfc
```

IP Multicast Forwarding Cache
(192.168.20.110/32, 239.0.0.100/32)
Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by OLNK
Outgoing interface list:
Loopback0, owned by OLNK
(192.168.20.110/32, 239.0.0.101/32)
Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by OLNK
Outgoing interface list:
Loopback0, owned by OLNK
(192.168.20.138/32, 239.1.1.1/32)
Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by OLNK
Outgoing interface list:
Loopback0, owned by OLNK

Relevant command

show ip mroute olnk

show ip mroute static

Chapter 60 IGMP Configuration Commands

60.1 IGMP Configuration Commands

60.1.1 clear ip igmp group

If you want to clear the multicast group member information saved in multicast router that supports IGMP, you can use the command "**clear ip igmp group**".

Syntas

clear ip igmp group *type-number group-address*

Parameter

Parameter	Description
type-number	port type and port number.
group-address	Multicast group's group address to clear information.

Default

None

Command mode

Supervisor mode

Explanation

Using this command, you can clear the multicast group member information saved in router when the saved multicast group information has a problem.

Example

The following example shows you how to clear the information of multicast group 233.33.1.1 on e1/0 port.

clear ip igmp group e1/0 233.33.1.1

Relevant command

None

60.1.2 debug ip igmp

If you want to track the process for igmp-router end protocol, you can use this command “**debug ip igmp**”, and use the”**no**” forma of the command to close debug information.

Syntas

debug ip igmp

no debug ip igmp

Parameter

None

Default

Close debug information output

Command mode

Supervisor mode

Explanation

You can use this command to track the main process for igmp-router end protocol to find the reason for protocol processing failure.

Example

igmp-router function module’s debug information usually use the natural language to make description. Due to its simplicity, we will not list all of the debug information.

60.1.3 debug ip igmp-host

If you want to track the process for igmp-host end protocol, you can use this command “**debug ip igmph**”, and use the”**no**” forma of the command to close debug information.

Syntas

debug ip igmph *group-address*

no debug ip igmph

Parameter

None

Default

Close debug information output

Command mode

Supervisor mode

Explanation

You can use this command to track the main process for igmp-host end protocol to find the reason for protocol processing failure.

Example

Igmp-host function module's debug information usually use the natural language to make description. Due to its simplicity, we will not list all of the debug information.

60.1.4 ip igmp helper-address

If you want a port to transit IGMP packet, you can use this command to configure the port. One port can configure the command only once time, so the next configured command will overwrite the original command.

Syntas

ip igmp helper-address *destination-address*

no ip igmp helper-address *destination-address*

Parameter

Parameter	Description
destination-address	The destination address of transitting IGMP packet。

Default

The port will not transit IGMP packet

Command mode

interface configuration mode

Explanation

Use this command “ip igmp helper-address” to transit all received igmp packets.

Example

ip igmp helper-address 192.168.20.10

60.1.5 ip igmp join-group

If you want to add a multicast group on the port, you can use this command to perform it.

Syntas

ip igmp join-group *group-address* [{**include**|**exclude**} *source-address*]

no ip igmp join-group *group-address* [{include|exclude} *source-address*]

Parameter

Parameter	Description
group-address	The multicast group required to be added to the port
include	The mode of SSM needed to add a multicast group is “include”.
exclude	The mode of SSM needed to add a multicast group is “exclude”.
source-address	Source filter address whose port is added to multicast group.

Default

No multicast group will be added to the port.

Command mode

interface configuration mode

Explanation

Use this command “ip igmp join-group” to dynamically add a multicast group to the port.

Example

ip igmp join-group 230.0.0.1

ip igmp join-group 230.0.0.1 exclude 192.168.20.10

60.1.6 ip igmp immediate-leave group-list

If you want the router port running IGMP version 2 to run the multicast group function “Exit Now”, you can use this command “**ip igmp immediate-leave group-list**” to perform configuring. In addition, you can use the “**no**”format of the command to forbid the IGMP host to “exit now”.

Syntas

ip igmp immediate-leave *group-list* *list-name*

no ip igmp immediate-leave *group-list*

Parameter

Parameter	Description
list-name	Pre-configured ip standard access-list name

Default

The IGMP host is not allowed to run “Exit Now” function.

Command mode

global configuration mode/interface configuration mode

Explanation

This command is available only for the port of running IGMP version 2.it can be used when the network connecting with the port has only one IGMP host. Through configuring this command, the host can immediately exit from a multicast group without the process for packet exchanging and delaying from the router. Besides, you can configure this command in “global configuration mode” and “interface configuration mode”, but this command configured in “global configuration mode” will be prior to the command configured in “interface configuration mode”. If you have configured the command in “global configuration mode”, the next command configured in “interface configuration mode “will be ignored. On the other hand, the command configured in “global configurationmode” will overwrite the original command configured in “interface configurationmode”.

Example

Prefer to “Configure multicast routing”.

Relevant command

ip access-list

60.1.7 ip igmp last-member-query-interval

To change the query interval of last group member l on the current port, use this command “**ip igmp last-member-query-interval”**. You can use the “**no**” format of the command to restore default settings.

Syntas

ip igmp last-member-query-interval *time*

no ip igmp last-member-query-interval

Parameter

Parameter	Description
time	The value of last member query interval configured on the port. Its unit is millisecond.

Default

The default of the last group member query interval on the port is 1000ms.

Command mode

interface configuration mode

Explanation

You can use this command “ip igmp last-member-query-interval” to modify the last group member query interval on the port.

Example

The following example will modify the last member query interval on the port to 2 seconds.

interface ethernet 0/0

ip igmp last-member-query-interval 2000

60.1.8 ip igmp querier-timeout

you can use this command “**ip igmp querier-timeout**”to modify other routers for IGMP querier timeout,.use the “**no**” f ormat of this command to restore default.

Syntas

ip igmp querier-timeout *time*

no ip igmp querier-timeout

Parameter

Parameter	Description
time	other querier timeout. Its unit is second.

Default

125 seconds

Command mode

interface configuration mode

Explanation

You can use this command “ip igmp querier-timeout” to modify other routers for querier timeout. This command is available only for the port which running IGMP version 2.

Example

The following example shows that the querier-timeout specified on interface Ethernet 0/0 is 100 seconds.

```
interface ethernet 0/0
ip igmp querier-timeout 100
```

60.1.9 ip igmp query-interval

To set the interval for IGMP General Query packet sending on the port, you can use this command “**ip igmp query-interval**”. Use the “**no**”format of this command to restore default.

Syntas

ip igmp query-interval *time*

no ip igmp query-interval

Parameter

Parameter	Description
time	Interval of sending general query packet. Its unit is second.

Default

60 seconds

Command mode

interface configuration mode

Explanation

you can use this command “**ip igmp query-interval**”to set the interval for IGMP General Query packet sending on the port,

Example

The following example shows that the interval of sending general query packet on Ethernet 0/0 port is specified to 50 seconds.

```
interface ethernet 0/0
ip igmp query-interval 50
```

60.1.10 ip igmp query-max-response-time

To specify the maximum interval for IGMP host to respond General Query packet, you can use this command “**ip igmp query-max-resposne-time**”. Use the “**no**”format of this command to restore default.

Syntas

ip igmp query-max-response-time *time*

no ip igmp query-max-response-time

Parameter

Parameter	Description
time	Value of the maximum response time configured on the port.

Default

10 seconds

Command mode

interface configuration mode

Explanation

you can use this command "**ip igmp query-max-resposne-time**"to specify the maximum interval for IGMP host to respond General Query packet. This command is available only for the port which running IGMP version 2 and 3.

Example

The following example will set the IGMP maximum response time on Ethernet 0/0 port as 15 seconds.

interface ethernet 0/0

ip igmp query-max-response-time 15

60.1.11 ip igmp static-group

If you want to configure a static multicast group on the port, you can use this command "**ip igmp static-group**" to perform it. Use the "**no**"format of this command to restore default.

Syntas

ip igmp static-group { ***** | ***group-address*** } {**include** *source-address* }

no ip igmp static-group { * | *group-address* } {**include** *source-address*}

Parameter

Parameter	Description
*	All multicast groups.
group-address	specified multicast group address.
source-address	specified host source address.

Default

In default, no multicast group is static configured on the port.

Command mode

interface configuration mode

Explanation

Configure the static IGMP multicast group information on the current port.

Notes:

For the same group-address, you can configure several “include source-address” commands for the corresponding static multicast group to have several source-addresses existing. However, for the same group-address, you can’t configure both commands with/without “include source-address”.

Example

Refer to “Configure multicast routing”

60.1.12 ip igmp version

To set the IGMP version number running on the port, you can use this command “**ip igmp version**”. use the “**no**”format of the command to restore default.

Syntas

ip igmp version *version-number*

no ip igmp version

Parameter

Parameter	Description
version-number	The value 1.2 or 3 indicates separately the IGMP version number 1,2 or3.

Default

If you don’t configure this command, the default version number for IGMP-Router end protocol running on the port is 3.

Command mode

interface configuration mode

Explanation

Use this command “**ip igmp version**”can set the IGMP version number running on the port,

Example

The following example will specify the IGMP version number running on Ethernet 0/0 port as 2.

```
interface ethernet 0/0
ip igmp version 2
```

60.1.13 show ip igmp groups

You can use the following command to see the multicast group member information that is saved on the current router.

Syntas

show ip igmp groups {***interface*** | ***group-address*** | ***detail***}

Parameter

Parameter	Description
interface	The port where you want to see the multicast group information. If you don't add this parameter, all multicast groups information on the port will be displayed.
group-address	The multicast group address to see. If you don't add this parameter, all multicast groups information on the router will be displayed.
detail	T he router whether you want to see the multicast group information.

Default

None

Command mode

Supervisor mode/global configuration mode/interface configuration mode.

Explanation

You can use this command to see the multicast group member information that is saved on the router.

Example

show ip igmp groups e0/0 detail

Running this command will display the following message:

……

Interface: Ethernet0/0

Group address: 233.33.1.3

Uptime: 00:03:46

Group status: Static

Group filter mode: INCLUDE

Last reporter: 0.0.0.0

Group source-list: (Flags: S-Static, R-Remote)

Source address:	Uptime	Timer	Fwd	Flags
192.168.20.5	00:03:46	stopped	Yes	S

Interface: Ethernet0/0
Group address: 233.33.1.1
Uptime: 00:03:46
Group status: Static
Group filter mode: INCLUDE
Last reporter: 0.0.0.0
Group source-list: (Flags: S-Static, R-Remote)

Source address:	Uptime	Timer	Fwd	Flags
192.168.20.5	00:03:46	stopped	Yes	S
192.168.20.3	00:03:46	stopped	Yes	S
192.168.20.1	00:03:46	stopped	Yes	S

……

show ip igmp groups 233.33.1.1 detail
Running this command will display the following message:
Interface: Ethernet0/0
Group address: 233.33.1.1
Uptime: 00:02:42
Group status: Static
Group filter mode: INCLUDE
Last reporter: 0.0.0.0
Group source-list: (Flags: S-Static, R-Remote)

Source address:	Uptime	Timer	Fwd	Flags
192.168.20.5	00:02:42	stopped	Yes	S
192.168.20.3	00:02:42	stopped	Yes	S
192.168.20.1	00:02:42	stopped	Yes	S

show ip igmp groups
Running this command will display the following message:

Interface	Group address	Uptime	Expires	Last Reporter	Flags
Ethernet0/0	239.255.255.250	00:01:08	00:02:05	192.168.20.141	R
Ethernet0/0	224.2.127.254	00:01:09	00:02:00	32.1.1.67	R
Ethernet0/0	224.1.1.1	00:01:24	stopped	0.0.0.0	S
Ethernet0/0	233.33.1.5	00:01:24	stopped	0.0.0.0	S
Ethernet0/0	233.33.1.3	00:01:24	stopped	0.0.0.0	S
Ethernet0/0	233.33.1.1	00:01:24	stopped	0.0.0.0	S

Interface	Group address	Uptime	Expires	Last Reporter	Flags
Loopback10	239.255.255.250	00:01:08	00:02:05	192.168.20.141	R
Loopback10	224.2.127.254	00:01:09	00:02:00	32.1.1.67	R

60.1.14 show ip igmp interface

You can use this command to see information on the current router's port where IGMP is activated.

Syntas

show ip igmp interface *interface*

Parameter

Parameter	Description
interface	The specified port to display information. If you don't add this parameter, all information on ports where IGMP is activated will be displayed.

Default

None

Command mode

Supervisor mode/global configuration mode/interface configuration mode

Explanation

You can use this command to display information on the port where IGMP is activated.

Example

show ip igmp interface e0/0

Running this command will display the following information:

Ethernet0/0 is up, line protocol is up
Internet address is 192.168.20.167
Current IGMP router version is 3
Router plays role of querier on the interface now
IGMP is enable on the interface
IGMP query-interval is 60 seconds
IGMP max query response time is 10 seconds
IGMP Last member query response time is 1000 milliseconds
IGMP querier timeout is 125 seconds
Multicast routing is enabled on the interface

60.1.15 show ip igmp-host

You can use this command to see IGMP host information on the port ofcurrent router.

Syntas

show ip igmph { ***interface*** } **detail**

Parameter

Parameter	Description
interface	The specified port to display information.
detail	Display igmp host detailed information.

Default

none

Command mode

Supervisor mode/global configuration mode/interface configuration mode

Explanation

You can use this command to display basic IGMP host information on the port.

Example

show ip igmph interface e0/0

Running this command will display the following information:

```
IGMP host Mode is IGMP_V3_ROUTER
  IGMP host Query Interval is 23 second
  IGMP host Query Response Interval is 125
  IGMP host Query Robustness Variable is 2
  IGMP host Last Query Interval is 0
  IGMP interface timer is 0
  IGMP host group joined(number of users):
    230.0.0.1(1)
```

Chapter 61 PIM-DM Configuration Commands

61.1 PIM-DM Configuration Commands

61.1.1 clear ip mroute pim-dm

Use the following command in supervisor mode to clear the (S,G) routing list items submitted by PIM-DM to mrouting:

Syntas

clear ip mroute pim-dm {***** | ***group*** [***source***]}

Parameter

Parameter	Description
*	Delete all multicast routing list items submitted by pim-dm.
group	Delete all list items submitted by pim-dm and satisfied in the specified group.
source	(optional) Delete all list items submitted by pim-dm and satisfied in the specified group's *source*.

Default

None

Command mode

Supervisor mode

Explanation

The command will delete all or part of table lists of local multicast router table,and it is possible to affect the normal multicast packet forwarding. This command can only delete the (S,G) items, whose upstream port is created by PIM-DM multicast routing protocol, and inform mrouting, then mrouting will determine if it should re-establish the corresponding (S,G).

Example

Example1:

Router#clear ip mroute pim-dm *

All (S,G) items, whose middlestream/upstream port is created by PIM-DM, on local MRT will be cleared.

Example2:

Router#clear ip mroute pim-dm 239.1.1.1

All (S,G) items with the group address 239.1.1.1, whose middlestream/upstream port is created by PIM-DM, on local MRT will be cleared.

Example3:

Router#clear ip mroute pim-dm 239.1.1.1 192.168.20.131

All (S,G) items with the address (192.168.20.138, 239.1.1.1), whose middlestream/upstream port is created by PIM-DM, on local MRT will be cleared.

61.1.2 clear ip pim-dm interface

Reset the multicast packet statistic value forwarded through (S,G) on PIM-DM port. You can use the command in supervisor mode:

Syntas

clear ip pim-dm interface {**count** | *type number{**count**}*}

Parameter

Parameter	Description
count	(optional) Delete all multicast packet statistic values on PIM-DM port.
type number	(optional) Delete multicast packet statistic values on the specified port.

Default

none

Command mode

supervisor mode

Explanation

This operation will reset the multicast packet number statistic values forwarded through PIM-DM port in local multicast routing list. This command can only reset the (S,G) items, whose upstream port is created by PIM-DM multicast routing protocol.

Example

Example1:

Router#clear ip pim-dm interface count

It will reset all multicast packet number statistic values forwarded by (S,G) items, whose upstream port is created by PIM-DM, on local MRT.

Example2:

Router#clear ip pim-dm interface Ethernet1/1 count

It will reset all multicast packet number statistic values forwarded by (S,G) items, whose upstream port is Ethernet1/1 and created by PIM-DM, on local MRT.

61.1.3 debug ip pim-dm

use this command to track input/output PIM packets and caused events. Set this command to “no” to stop tracking.

Syntas

debug ip pim-dm [**group**|**alert**]

Parameter

Parameter	Description
group	(optional) Track the specified group status.
alert	(optional) Track the alert status received from mrouting.

Default

none

Command mode

supervisor mode

Explanation

receive Alert from mrouting.

Send alert to other components.

Example

Example 1, the output information is as follows:

Hello packet prompt sent to each port.

Hello packet prompt received from each port.

A new neighbor is found.

Delete neighbor.

Port sending status refresh packet.

Port receiving status refresh packet.

Port is sending Assert packet.

Port is receiving Assert packet.

Port is sending prune packet.

Port is receiving prune packet.

Port is sending graft ack packet.

Port is receiving graft ack packet.

Port is sending graft packet.

Port is receiving graft packet.

Port is sending join/prune packet.

Port is receiving join/prune packet.

When a new (S,G) is created

When deleting (S,G)

Router#debug ip pim-dm

2003-3-26 11:45:17 received V2 hello packet on Ethernet2/1 from 192.168.20.133(GenID = 3539)

2003-3-26 11:45:17 Ethernet2/1 create new nbr 192.168.20.133

2003-3-26 11:45:25 send hello packet to 224.0.0.13 on Loopback1

2003-3-26 11:50:29 Ethernet2/1 delete nbr 192.168.20.133

2003-3-26 11:50:51 received V2 hello packet on Ethernet2/1 from 192.168.20.152

2003-3-26 11:50:51 send hello packet to 224.0.0.13 on Ethernet2/1

2003-3-26 12:04:37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success

2003-3-26 12:04:37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful

2003-3-26 12:04:39 PIM-DM: ignored V2 packet on Ethernet2/1 from 192.168.10.204 (validate source address failed)

2003-3-26 12:04:39 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream:192.168.20.132 Adding in MRT success

2003-3-26 12:04:39 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT

Example 2, output received alert message:

Router#debug ip pim-dm alert

2003-3-26 12:09:51 receive alert_rt_change alert from mroute

2003-3-26 12:09:54 receive alert_rt_change alert from mroute

2003-3-26 12:11:08 PIM-DM: send sg_deletion alert

2003-3-26 12:11:19 receive alert_sg_creation alert from mroute

2003-3-26 12:11:20 receive alert_sg_prune alert from mroute

2003-3-26 12:11:56 receive alert_group_report alert from mroute

2003-3-26 12:11:56 receive alert_sg_join alert from mroute

Example 3, track the specified group status:

Router#deb ip pim-dm 239.1.1.1

Router#2003-3-26 12:35:27 PIM-DM: clear (192.168.20.138, 239.1.1.1) forwd pkt count success

2003-3-26 12:35:37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success

2003-3-26 12:35:37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful

2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream: 192.168.20.132 Adding in MRT success

2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 1.1.1.1 create success

2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 192.167.20.132 create success

2003-3-26 12:35:42 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT

61.1.4 ip pim-dm

This command is used to run PIM-DM on the port. set this command to “no” to disable PIM-DM on the port.

Syntas

ip pim-dm

no ip pim-dm

Parameter

None

Default

None

Command mode

interface configuration mode

Explanation

1. If the “ip multicast-routing” is not configured before configuring this command, it will display the following warning: WARNING: "ip multicast-routing" is not configured, IP Multicast packets will not be forwarded

2. Once this function is disabled, PIMDM will no longer run on the port.but it will not affect other PIM-DM configurations. After rerun PIM-DM on the port, all PIM-DM configurations are still valid.

3. Enabling this function means it is available for forwarding multicast packet on the port, however, you have to enable the global multicast packet forwarding function first.

Example

Router_config#ip multicast-routing
Router_config#interface Ethernet1/1
Router_config_e1/1#ip pim-dm

Relevant command

ip multicast-routing

show ip pim-dm interface

61.1.5 ip pim-dm dr-priority

Set a router as the priority to specified router (DR). You can set this command to “no” to restore default DR priority on the port.

Syntas

ip pim-dm dr-prioirty *priority*

no pim-dm dr-prioirty

Parameter

Parameter	Description
priority	Port DR priority. The larger the value is, the higher the priority is. Its range is from 0 to 4294967294, and the default is 1.

Default

default DR priority on PIM port is 1.

Command mode

interface configuration mode

Explanation

1. If all PIM neighbors support DR Priority on the port, select the one with the highest priority as DR. If all have the same priority, just select the one with the highest port IP value as DR.

2. If router didn't advertise its priority in Hello packet and there are several routers have the same situation, just select the router with the highest port IP value as DR.

61.1.6 ip pim-dm hello-interval

This command is used to configure the interval of regularly sent PIM-Hello packets on the port. You can set this command to "no" to restore default interval.

Syntas

ip pim-dm hello-interval *interval*

no **ip pim-dm hello-interval**

Parameter

Parameter	Description
interval	The interval of regularly sent PIM-Hello packets. Its range is from 0 to 65535, and the default is 30 seconds.

Default

30 seconds

Command mode

interface configuration mode

Explanation

Regularly sending Hello packets can check if the neighbor exists. Generally, if Hello packets is not received after the 3.5 times hello-interval timeout configured by neighbor, the neighbor will be considered disappeared.

For IGMP v1, you can select the specified router (DR) through PIM-DM Hello packet.

Example

```
Router_config#interface Ethernet1/1
Router_config_e1/1#ip pim-dm hello-interval 30
```

Relevant command

ip igmp query-interval

61.1.7 ip pim-dm state-refresh origination-interval

It allows the router to generate original PIM-DM state refresh packet and configure the state refresh interval. To cancel the generation for original PIM-DM state refresh packet, set this command to “no”.

Syntas

ip pim state-refresh origination-interval [*interval*]

no ip pim state-refresh origination-interval

Parameter

Parameter	Description
interval	For the first port router connected with the source directly, it is the interval of regularly sending state refresh packet. For the following router, it is interval of allowed receiving and processing state refresh packet for the port. This parameter is configured optionally, and its range is from 4 to 100 seconds. The default is 60 seconds.

Default

This parameter is configured optionally.

The default is 60 seconds.

Command mode

interface configuration mode

Explanation

Configure this command on the first router’s, neighboring directly on the multicast source, incoming port. By default, it will generate original state refresh packet. During configuring this command on the following router’s port, you can use *interval* to limit the process for received state refresh packet interval. By default, all routers where is running PIM-DM can process and forward state refresh packet.

Example

Router_config_e1/1#ip pim-dm state-refresh origination-interval 80

Relevant command

ip pim-dm state-refresh disable

61.1.8 ip pim-dm neighor-filter

This command is used to prevent some routers from participating PIM-DM operation. Set this command to “no” to cancel the limit.

Syntas

ip pim-dm neighor-filter *acess-list-name*

no ip pim-dm neighor-filter *acess-list-name*

Parameter

Parameter	Description
access-list-name	Standard access-list, whose definition is to deny PIM packets from the specified source.

Default

No filter function.

Command mode

interface configuration mode

Explanation

You can use multiple filter lists. The router denied by anyone of the lists can’t be a neighbor of local PIM-DM.

Example

router_config_e1/1#ip pim-dm neighbor-filter nbr_filter
router_config#ip access-list standard nbr_filter
router_config_std_nacl#deny 192.167.20.132 255.255.255.255
router_config_std_nacl#permit 192.168.20.0 255.255.255.0

Relevant command

access-list

61.1.9 ip pim-dm state-refresh disable

It will not allow running router process for PIM-DM multicast protocol or forward PIM-DM state refresh control message. You can set this command to “no” to restore the forwarding function.

Syntas

ip pim-dm state-refresh disable

no ip pim-dm state-refresh disable

Parameter

none

Default

By default, it is allowed to run forwarding PIM dense mode state refresh control message.

Command mode

Supervisor mode

Explanation

After configuring this command to forbid processing and forwarding PIM-DM state refresh control message, the Hello message in PIM-DM will no longer contain state refresh control options and receive/send state refresh control packet.

Example

The following command forbids forwarding state refresh control message to downstream neighbors of PIM dense mode.

ip pim-dm state-refresh disable

Relevant command

ip pim-dm state-refresh origination-interval

61.1.10 show ip mroute pim-dm

Display PIM-DM multicast routing list information.

Syntas

s**how ip mroute pim-dm** *group-address* ***source***

Parameter

Parameter	Description
group-address	（optional）group address
source	（optional）source address

Default

none

Command mode

All modes except the user mode.

Explanation

It can display all (S,G) or specified (S,G) only in local MRT.

Example

Example1: Display all (S,G) in local MRT.

```
Router#show ip mroute pim-dm
PIM-DM Multicast Routing Table
Timers: Uptime/Expires
State: Interface state
RPF nbr: RPF neighbor address
(192.168.20.151, 224.1.1.1),       00:00:03 /00:03:27
  Incoming interface:
    Ethernet2/1      Forwarding          0.0.0.0
  Outgoing interface list:
    Loopback1        NoInfo    00:00:07 /00:00:00

(192.168.20.138, 239.1.1.1),       00:00:03 /00:03:27
  Incoming interface:
    Ethernet2/1      Forwarding          0.0.0.0
  Outgoing interface list:
```

Loopback1 NoInfo 00:00:07 /00:00:00
Ethernet1/1 NoInfo 00:02:43 /00:00:00

Example 2: Display the specified (S,G) in local MRT.

Router#show ip mroute pim-dm 224.1.1.1
PIM-DM Multicast Routing Table
Timers: Uptime/Expires
State: Interface state
RPF nbr: RPF neighbor address
(192.168.20.151, 224.1.1.1), 00:00:01 /00:03:29
Incoming interface:
Ethernet2/1 Forwarding 0.0.0.0
Outgoing interface list:
Loopback1 NoInfo 00:03:50 /00:00:00

Example3: Display the specified (S,G) in local MRT.

Router#show ip mroute pim-dm 224.1.1.1 192.168.20.131
PIM-DM Multicast Routing Table

61.1.11 show ip pim-dm neighbor

To display the PIM-DM neighbor and the selected DR, run the following command:

show ip pim-dm neighbor [***interface-type*** *interface-number*]

Parameter

Parameter	Description
interface-type *interface-number*	Type and ID of the interface, such as Ethernet1/1 and serial 11/0

Default

None

Command mode

All modes except the user mode

Explanation

This command is used to check on which LAN routers PIM-DM or PIM-SM is configured.

Example

Example 1:

```
Router#show ip pim-dm neighbor
        PIM-DM Neighbor Table
Neighbor          Interface         Uptime/Expires      Ver   DR Prior/Mode
Address
192.167.20.132    Ethernet1/1       03:13:34 / 00:00:00    v2    4/D      (DR)
1.1.1.1           Loopback1         03:52:30 / 00:00:00    v2    1/D      (DR)
192.168.20.132    Ethernet2/1       19:35:56 / 00:00:00    v2    1/D
192.168.20.152    Ethernet2/1       00:00:04 / 00:01:41    v2    1/D
192.168.20.204    Ethernet2/1       00:00:36 / 00:01:44    v2    20/D     (DR)
```

Example 2:

```
Router# show ip pim-dm neighbor Ethernet2/1
PIM-DM Neighbor Table
Neighbor          Interface         Uptime/Expires      Ver   DR Prior/Mode
Address
192.168.20.132    Ethernet2/1       19:39:22 / 00:00:00    v2    1/D
192.168.20.152    Ethernet2/1       00:00:30 / 00:01:15    v2    1/D
192.168.20.204    Ethernet2/1       00:00:04 / 00:02:16    v2    20/D     (DR)
```

Related command

ip pim-dm

ip pim-dm dr-priority

ip pim-dm hello-interval

ip pim version

ip pim-dm neighor-filter

show ip pim-dm interface

61.1.12 show ip pim-dm interface

To display the state of the PIM-DM interface, run the following command:

show ip pim-dm interface [***interface-type*** *interface-number*] [***count***][***detail***]

Parameter

Parameter	Description
interface-type *interface-number*	Type and ID of the interface, such as Ethernet1/1 and serial 11/0

Default

None

Command mode

All modes except the user mode

Explanation

Only the state of the PIM-DM interface can be displayed after this command is run. If the PIM-DM interface is not designated, the information about all PIM-DM interfaces' state will be displayed.

Example

Example 1:

```
Router#show ip pim interface
address          Interface          Ver/   Nbr     Hello   DR      DR
                                    Mode   Count   intvl   Prior
192.167.20.132   Ethernet1/1        v2/D   0       30      4       192.167.20.132
1.1.1.1          Loopback1          v2/D   0       30      1       1.1.1.1
192.168.20.132   Ethernet2/1        v2/D   2       30      1       192.168.20.204
```

Example 2:

```
Router#show ip pim interface Ethernet2/1
address          Interface          Ver/   Nbr     Hello   DR      DR
                                    Mode   Count   intvl   Prior
192.168.20.132   Ethernet2/1        v2/D   2       30      1       192.168.20.204
```

Related command

ip pim-dm

ip pim-dm dr-priority

ip pim-dm hello-interval

ip pim version

ip pim-dm neighor-filter

show ip pim-dm neighbor

61.1.13 show ip rpf pim-dm

To display how the multicast route conducts the Reverse Path Forwarding (RPF), run the following command:

show ip rpf pim-dm *source-address*

Parameter

Parameter	Description
source-address	Displays the RFP information of the designated source address.

Default

None

Command mode

All modes except the user mode

Explanation

The PIM-DM protocol can obtain the RPF information from multiple types of routing tables. This command tells you where the RPF information is obtained.

Example

Router#show ip rpf pim 4.1.1.1
RPF information for (4.1.1.1)
RPF interface: Ethernet2/1
RPF neighbor: 192.168.20.80
RPF route/mask: 192.168.20.0/24
RPF type: unicast
Metric preference: 120
Metric: 1

Related command

None

Chapter 62 PIM-SM Configuration Commands

62.1 PIM-SM Configuration Commands

62.1.1 ip pim-sm

Syntas

ip pim-sm

no ip pim-sm

Parameter

None

Default

Disable PIM-SM

Command mode

Interface configuration mode

Explanation

To enable PIM-SM function on an interface.You will enable PIM-SM when you configure the routers first in the router interface .you can cancle PIM-SM configure in the last interface to stop PIM-SM running .

Relevant command

None

62.1.2 ip pim-sm admin-scope

To configure the multicast administrator scope, run **ip pim-sm admin-scope *gaddr gmask***. The designated multicast address ranges between 239.0.0.0 and 239.255.255.255. This command is configured only on the edge routers which interlace other SZs.

ip pim-sm admin-scope *gaddr gmask*

no ip pim-sm admin-scope

Parameter

Name	English prompt	Description
admin-scope	admin-scope – pim-sm administrator scope	Only the C-BSRs and the ZBRs need to be configured to know about the existence of the scope zones. Other routers, including the C-RPs, learn of their existence from Bootstrap messages.
gaddr	A.B.C.D – private group address prefix	239.0.0.0 to 239.255.255.255
gmask	gmask – sz group mask	

Default value

The global domain is 224.0.0.0/4 by default.

Command mode

Port configuration mode

Instruction

This command is configured on the boundary of the PIM-SM administrator scope and used to check the BSM information which is received from the outside of the administrator scope. If the SZ scope of the received BSM information is smaller than or equal to the locally configured administrator scope, the received BSM information will be discarded. Otherwise, the received BSM information will enter the local administrator scope. When the BSM information is forwarded locally, the same principle is followed. At present, Huawei only supports the global domain and the private domain, but does not support the covering of the group address. RP in SZ1 will not notify the global SZ of the C-RP-ADV information. But the global BSM information can get in.

Example

The following example shows how to configure the boundary scope on routerA to **pim-sm sz1(239.1.1.1/24)**.

```
RouterA_config_f0/0#ip pim-sm admin-scope 239.1.1.1 255.255.255.0
RouterB_config_ps# c-bsr interface lo1
RouterB_config_ps# c-bsr admin-scope 239.1.1.1 255.255.255.0
```

Related command

ip pim-sm bsr-border

c-bsr intf_type intf_name

62.1.3 ip pim-sm asrt-hold

To configure the holdtime for the **assert** state on the port corresponding to PIM-SM, run the following command.

ip pim-sm asrt-hold *intvl*

no ip pim-sm asrt-hold *[*intvl*]*

Parameter

Name	English prompt	Description
pim-sm	pim-sm - Enable PIM sparse mode operatioin	
asrt-hold	***asrt-hold*** – assert status hold timer	
intvl	<7-65535> - time value (second)	The default value is 180 seconds.

Default value

180 seconds

Command mode

Port configuration mode

Instruction

Example

The following example shows how to configure the timeout time in **assert** state on port f0/0 to 200 seconds.

Router_config_f0/0#ip pim-sm holdtimer assert 200

62.1.4 ip pim-sm bsr-border

Syntas

ip pim-sm bsr-border

no ip pim-sm bsr-border

Parameter

None

Default

Non-BSR boundary.

Command mode

Global configuration mode

Explanation

This command can set interface to BSR boundary.in this interface didn't send/receive BSM message ;use "no"command to recovery default .

This command change difineition BSR boundary to make BSM message can not effect each other in different PIM-SM domain.

Relevant command

None

62.1.5 ip pim-sm dr-pri

Syntas

ip pim-sm dr-pri *pri-value*

no ip pim-sm dr-pri *pri-value*

Parameter

Name	English prompt
dr-pri	dr-pri - pim-sm interface DR priority
Pri-value	<0-4294967294> - DR priority, preference given to larger value

Default

DR priority is 1 by default in global mode.

Command mode

Interface configuration mode

Explanation

To change interface DR priority ,use “no”command to recovery default value.

The highest priority routers will be DR.if the priority is same,then the highest address is DR.

Relevant command

None

62.1.6 ip pim-sm hello-intvl

Syntas

ip pim-sm hello-intvl *seconds*

no pim-sm hello-intvl *[seconds]*

Parameter

Name	English prompt
hello-intvl	hello-intvl- pim-sm hello advertisement interval
seconds	<1-65535> - periodic pim hello message are sent(unit:s)

Default

The interval of sending Hello messages is 30s.

Command mode

Interface configuration mode

Explanation

To configure hello message sending interval ,use “no”command to renew default value.

To change the hold-time of neighbor router, hold-time is 3.5 times of hello message sending interval.

Relevant command

None

62.1.7 ip pim-sm holdtime

To configure the interval of the hello timer on the PIM-SM port, run the following first command. The value of the interval ranges between 4 and 65535.

ip pim-sm holdtime *seconds*

no pim-sm holdtime [*seconds*]

Parameter

Name	English prompt	Remarks
Holdtime ***seconds***	holdtime – keep alive time to neighbor <4-65535> - keep alive time value	

Default value

105 seconds

Command mode

Interface configuration mode

Instruction

This command is first run in port configuration mode and then in global configuration mode, or the default value is chosen. If the value of the holdtime is smaller than that of Hello interval, the configured value is then invalid. The value of the holdtime is **hello-intvl***3.5.

Example

The following example sets the holdtime value to 100 for interface pimsm configuration:

Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm holdtime *100*

Related command

ip pim-sm hold-intvl

intvl-time hello *hlo-intvl*

62.1.8 ip pim-sm horizon-split

To configure the horizon split strategy of the BSM packets on a port, run the following first command.

ip pim-sm horizon-split

no ip pim-sm horizon-split

Parameter

Name	English prompt	Remarks
horizon-split	Horizon-split – permit interface horizon split	

Default value

The horizontal split is disabled by default.

Command mode

Interface configuration mode

Instruction

After this command takes effect, you can set the corresponding label bit of the PIM-SM port. The BSM packets that are received from a port will not be transmitted from the port.

Example

The following example sets the DR priority value to 200 for the interface f0/0:

Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm ***horizon-split***

Related command

bsm policy

62.1.9 ip pim-sm jp-hold

To configure the holdtime for the **join-prune** state on the port corresponding to PIM-SM, run the following first command.

ip pim-sm jp-hold *intvl*

no ip pim-sm jp-hold *[intvl]*

Parameter

Name	English prompt	Remarks
pim-sm	pim-sm - Enable PIM sparse mode operation	
jp-hold	Join-prune –join-prune status hold timer	
intvl	<1-65535> - time value (second)	The default value is 210 seconds.

Default value

210 seconds

Command mode

Port configuration mode

Instruction

Example

The following example shows how to configure the timeout time in **join** state on port f0/0 to 200 seconds.

Router_config_f0/0#ip pim-sm jp-hold 200

62.1.10 ip pim-sm jp-intvl

To set the interval of transmitting the **join** or **prune** packets periodically, run the following first command. The interval, whose unit is second, ranges between 1 and 65535.

ip pim-sm jp-intvl [*seconds*]

***no* ip pim-sm jp-intvl**

Parameter

Name	English prompt	Remarks
pim-sm	pim-sm - Enable PIM sparse mode operatioin	
jp-intvl	jp-intvl – regular Join/Prune message interval (unit:s)	
Seconds	<1-65535> - time value (second)	The default value is 60 seconds.

Default value

60 seconds

Command mode

Port configuration mode

Instruction

*At each configuration the PIM-SM database must be entirely searched for the **(s, g)** pairs or the **(*, g)** pairs; if the configured port is an upstream one, the interval of the **jp** timer of the corresponding **(s, g)** or **(*, g)** pair should be reset. The interval in port configuration mode is prior to the **join/prune** interval in global mode.* If the **Join** packets from the downstream neighbor have not been received in three JP timeout periods, the downstream that corresponds to the multicast item will be shifted to the **prune** state. The default holdtime is 3 minutes. If this value is changed randomly, CPU shock and service-forwarding shock may be caused.

Example

The following example changes the PIM join message interval to 90 seconds:

Router_config_f0/0# ip pim-sm jp-intvl 90

Related command

ip pim-sm jp-hold

62.1.11 ip pim-sm lan-delay

To designate the prune delay time of the PIM-SM port, run the following first command.

ip pim-sm lan-delay *delay-intvl*

no pim-sm lan-delay

Parameter

Name	English prompt	Remarks
lan-delay	lan-delay - pim-sm prune delay	
delay-intvl	<1-32767> - prune delay time out interval(unit:ms)	The default value is 500 milliseconds.

Default value

500ms

Command mode

Interface configuration mode

Instruction

If the local port is the downstream port, the finally calculated prune delay time is based on all maximum values reported by downstream neighbors. In this case, the override timer of transmitting the **join** packets towards the upstream neighbors will be affected. If the **prune_delay** option is not supported by all downstream neighbors, the default value will be used as the overtime interval of the **prune pending** timer. If the interval of the **prune delay** timer is locally set, it will be reported to upstream neighbors through the HELLO packets.

Example

The following example sets the prune delay value to 200 ms for the pim-sm interface

f0/0:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm lan-delay 20
```

Related command

ip pim-sm override

62.1.12 ip pim-sm nbma-mode

If the following first command is configured on all NBMA interfaces, the central node will forward all information that is transmitted from the sub-nodes and the other sub-nodes can obtain the corresponding information. 。

ip pim-sm nbma-mode

no ip pim-sm nbma-mode

Parameter

Name	English prompt	Remarks
nbma-mode	nbma-mode - Use Non-Broadcast Multi-Access (NBMA) mode on interface	Currently our products do not support this function.

Default value

Disable

Command mode

Interface configuration mode

Instruction

Traditional NBMA networks (frame relay, ATM and SMDS) adopt the point-to-multipoint mode; when a sub-node need be pruned, it will report this information directly to the central node and other sub-nodes, however, can not receive this information. In this case, other sub-nodes cannot respond and the interface of the central node will be incorrectly pruned.

If the following first command is configured on all NBMA interfaces, the central node will forward all information that is transmitted from the sub-nodes and the other sub-nodes can obtain the corresponding information.

This command cannot be used in multicast LANs, such as Ethernet or FDDI.

Example

The following example configures an interface to be in NBMA mode:

Router_config#interface s1/0
Router_config_s1/0#ip address 10.0.1.2 255.255.255.0
Router_config_s1/0#ip pim-sm nbma-mode

Related command

62.1.13 ip pim-sm nbr-filter

To stop a device from being added to PIM, run the following first command; to cancel this function, run the following second command.

ip pim-sm nbr-filter *acl-name*

no ip pim-sm nbr-filter

Parameter

Name	English prompt	Remarks
nbr-filter	nbr-filter - PIM peering filter	
acl-name	WORD – ip stand access list name	

Default value

Disable

Command mode

Interface configuration mode

Instruction

If this command is configured, the neighbors need be filtered when Hello packets are received and then a new neighbor can be created. If it is in **deny** state, the corresponding new neighbor need not be created. Multiple neighbor access lists can be configured (New CISCO bin only allows to configure a neighbor access list; old bin allows to configure multiple neighbor access lists). Once a neighbor is filtered, the neighbor is then denied.

Example

The following example shows how to configure stub multicast routing on router A and how router B uses access list 1 to filter all PIM information from router A.

Router A Configuration

```
Router_config# ip multicast-routing
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.0.1 255.255.255.0
Router_config#interface f0/1
Router_config_f0/1# ip igmp-helper 10.0.0.2
```

Router B Configuration

```
Router_config# ip multicast-routing
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.0.2 255.255.255.0
Router_config_f0/0# ip pim-sm nbr-filter 1
Router_config#ip access-list standard 1
Router_config_std_nacl# deny 10.0.0.1
Router_config_std_nacl# permit any
```

Related command

ip pim-sm jp-intvl

62.1.14 ip pim-sm nbr-track

To forbid the limitation of the JOIN packets globally and enable neighbor tracking, run the following first command:

ip pim-sm nbr-track

no ip pim-sm nbr-track

Parameter

Name	Prompt	Remarks
nbr-track	nbr-track - pim-sm interface neighbor tracking	

Default value

If the global congfigration mode is not configured, neighbor tracking is forbidden.

Command mode

Interface configuration mode

Instruction

This command is used to forbid the limitation function of the **join** packets and enable neighbor tracking.

Example

The following example sets the DR priority value to 200 for the interface f0/0:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm nbr-track
```

Related command

None

62.1.15 ip pim-sm override

To designate the prune deny time of the PIM-SM port, run the following first command.

ip pim-sm override *override-intvl*

no ip pim-sm override

Parameter

Name	Prompt	Remarks
override	override - pim-sm override timer	
override-intvl	<1-65535> - override time out interval(unit:100ms)	

Default value

2.5s

Command mode

Interface configuration mode

Instruction

The finally calculated prune deny time is based on the maximum value among all the values reported by all neighbors. If some neighbor does not support prune deny, the default value is selected. If OT is enabled, the value can be random. If the interval of the **prune deny** timer is locally set, it will be reported to upstream neighbors through the HELLO packets.

Example

The following example sets the override value to 2000 ms for pim-sm interface f0/0 configuration:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm override 200
```

Related command

ip pim-sm lan-delay

62.1.16 router pim-sm

To enter the global PIM-SM view, under which there is common attributes, run the following first command:

router pim-sm

no router pim-sm

Parameter

None

Default value

The system will not generate the PIM-SM view by default.

Command mode

Global configuration mode

Instruction

If the **router pim-sm** command is configured globally or the PIM-SM related configuration is first configured on the port, the global PIM-SM view will be created. If there is some PIM-SM related configuration on the port, the global view cannot be deleted.

Example

The following command shows how to create the global PIM-SM view:
Router_config#router pim-sm
Router_config_ps#

Related command

ip pim-sm

62.1.17 hello-option

To configure in the global PIM-SM view, the global DR priority, the prune delay time, the transmission interval of HELLO packets, the prune deny time, neighbor tracking and neighbor timeout time, run the following command:

hello-option { dr-pri *pri-value* | lan-delay *delay-intvl* |

override *override-intvl* | nbr-track | holdtime *hold-intvl* }

no hello-option [dr-pri | lan-delay | override | nbr-track | holdtime]

Parameter

Name	Prompt	Remarks
dr-pri	dr-pri - pim-sm global DR priority	
pri-value	<0-4294967294> - DR priority, preference given to larger value	If this command is not configured, the default DR priority of this process is 1.
lan-delay	lan-delay - pim-sm prune delay time	Configures the prune delay time.
override	Override – override for rcvd prune	Configures the prune deny.
delay-intvl	**<0-32767>** – value for prune delay	The default prune delay time is 500ms.
override-intvl	**<0-65535>** – value for override delay	The default prune deny time is 2500ms.
nbr-track	**nbr-track – neighbor track enable**	If this command is configured, the JOIN packets will not be limited.

Name	Prompt	Remarks
holdtime ***hold-intvl***	**holdtime – neighbor keep alive timer** **<4-65535>** – value for neighbor timeout	In normal case, its value is 3.5 times larger than the Hello interval on a port. The default neighbor holdtime is 105 seconds.

Default value

See the table above.

Command mode

Global PIM-SM view

Instruction

If there is no corresponding configuration items on a port, the globally configured attributes will be used as the corresponding attributes on the port. The change of the global DR priority may affect the new DR selection.

The rules of DR selection are shown below:

1. The highest DR priority on a port will be selected as the DR of the network segment to which this port belongs; if there are many same DR values, the relatively large IP address among the main IP address on the local port and the main IP address of the neighbor will be selected as DR.

2. If there are neighbors on a port or the DR priority is not supported on a port, the relatively large mainaddress will serve as DR.

Example

The following example sets the DR priority value to 200 for global pimsm configuration:

```
Router_config#Router pim-sm
Router_config_ps#dr-priority 200
```

62.1.18 accept bsm-adv

You can run **accept bsm-adv** in global mode to set the filtration list. The filtration list settings is especially for filtrating specific BSM source addresses and receive the designated BSM source address. To cancel the filtration, you can run **no accept bsm-adv [*list* *std-acl*]**.

accept bsm-adv *list* *std-acl*

no accept bsm-adv [*list* *std-acl*]

Parameter

Name	Prompt	Remarks
accept	Accept – configure accept policy	
bsm-adv	bsm-adv - BSM packet source address accept filter	
list	list - IP access-list for bsm source-list	
std-acl	WORD -- stand access list name	It is used to limit the range of the BSM source address.

Default value

This filtration is disabled by default.

Command mode

pim-sm global view

Instruction

Only one filtration command can be set.

Example

The following example shows that the BSM notifications only from network segment 192.2.2.0/30 can be received.

```
Router_config#router pim-sm
Router_config_ps#accept bsm-adv list adv-src
Router_config_ps#exit
Router_config#ip access-list stand adv-src
Router_config_std_nacl#permit 192.2.2.0 255.255.255.252
```

62.1.19 accept crp-adv

To set the filtration list specially for filtrating the address range of specific groups, limiting to receive the C-RP-ADV packets from specific candidate rp unicast, and specifying the group address' range in the received packets through ACL. To cancel the filtration, you can run **no accept crp-adv *.*.*.*** *[std-acl]*.

accept crp-adv *.*.*.* *[std-acl]*

no accept crp-adv *.*.*.* *[std-acl]*

Parameter

Name	Prompt	Remarks
accept	Accept – configure accept policy	
c-rp-adv	crp-adv – C-RP-ADV accept filter	
	c	
A.B.C.D	A.B.C.D - IP address of candidate RP for group	
std-acl	WORD – ip stand access-list name for group	

Default value

Disable (not filtrating C-RP-ADV from c-rp)

Command mode

pim-sm global view

Instruction

After this command is set, BSR only processes C-RP-ADV from RP. Additionally, the range of the group address must be allowed by the standard ACL.

Example

The following example states that the router will accept c-rp messages RP address is 100.1.1.1 for the multicast group 224.2.2.2:

Router_config#router pim-sm
Router_config_ps#accept crp-adv 100.1.1.1 grp-acl
Router_config#ip access-list stand grp-acl
Router_config_std_nacl#permit 224.2.2.2 255.255.255.255

62.1.20 accept rp-addr

Run **accept-rp** in global configuration mode to set the filtration list to filter the specific group address range, deciding whether the join/prune of (*, G) is acceptable and responding to the registration information of specific destination group addresses. To cancel this setting above, run the “no” form of this command.

accept rp-addr *A.B.C.D [std-acl]*

no accept rp-addr *A.B.C.D*[*std-acl*]

Parameter

Name	Prompt	Remarks
accept	Accept – configure accept policy Accept – Configure the policy of packet reception.	
rp-addr	rp-addr - RP address accept filter rp-addr – Configure the acceptable RP address filter.	
A.B.C.D	A.B.C.D - IP address of RP for group A.B.C.D – Designate the RP address of a multicast group.	
std-acl	WORD – ip stand access-list name for group WORD – Stands for the standard access list that is used for multicast group filtration.	If omitting it, the router will process all the PIM-SM message to any group which is mapped to the RP.

Default value

Disable (All Join, Prune or Register packets will be processed)

Command mode

pim-sm global view

Instruction

After this command is set, the router processes only those Join packets which are mapped to the designated RP. Another point deserving attention is that the range of the group address must be allowed by the standard access list. The aggregation point of the corresponding group must be the calculated RP, and when the aggregation point matches up with the RP can the access filtration list be applied. If the group address is denied, RP will reject the Join and Register packets; after the Register packets are received, RP will return a Register Stop packet to the registration packet generator.

This command can be set many times if the **rp-addr** parameters in this command are different. If the RP that the group address is mapped to is not in the configured range, the RP will be denied directly.

Example

The following example states that the router will accept join or prune messages destined for the RP at address 100.1.1.1 for the multicast group 224.2.2.2:

```
Router_config#router pim-sm
Router_config_ps#accept rp 100.1.1.1 no-ssm-range
```

Router_config#ip access-list extended no-ssm-range
Router_config_std_nacl#permit 224.2.2.2

%PIM-6-INVALID_RP_JOIN: Received (, 238.1.1.1) Join from 192.17.20.173 for invalid RP 1.1.1.1*
Router#show ip mroute
(, 238.1.1.1), 00:02:52/00:00:07, RP 1.1.1.1, flags: S*
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
FastEthernet0/0, Forward/Sparse, 00:02:52/00:00:07
It can be seen that the previous address, *.238.1.1.1, ages after the filtration is set.

62.1.21 accept register

When the Register range list is set on C-RP, the selection is RP and the PIM-SM Register packet is received, the filtration list should be used to filter the Register packets. In this case, you should run **accept-register**, and if you want to cancel the filtration, run the “no” form of this command.

accept register *{**list ext-acl** | **route-map map-name**}*

no **accept register** [***list*** *ext-acl* **|** ***route-map*** *map-name*]

Parameter

Name	Prompt	Remarks
accept	Accept – configure accept policy	
	Accept – Configure the policy of packet reception.	
register	register - Registers accept filter	
	Register – Stands for the filter of receiving the Register message.	
list	list – access list	
	list – stands for the access list.	
route-map	Route-map – route map	
	route-map – stands for the route map list.	
ext-acl	WORD – IP extend access list name	
	WORD – stands for the name of the extensible IP access control list.	
map-name	WORD – route map name	
	WORD – stands for the name of the route map list.	

Default value

The access list filtration or the route-map filtration will not be conducted to the Register packets.

Command mode

pim-sm global view

Instruction

This command is used to prevent those unauthenticated data source from sending the Register packets to RP. If an unauthenticated data source sends a Register packet to RP, RP will return a Register Stop packet at once. This command takes effect only on the machine that runs as RP.

Example

The following example shows how to restrict the RP from allowing sources in the Source Specific Multicast (SSM) range of addresses to register with the RP.

```
Router_config#router pim-sm
Router_config_ps#accept register list no-ssm-range
Router_config#ip access-list extended no-ssm-range
Router_config_std_nacl#deny ip any 232.0.0.0 0.255.255.255
Router_config_std_nacl#permit ip any any
```

Related command

reg-src

62.1.22 anycast-rp

Through configuring **anycast-rp** and the corresponding neighbor address, you can specify the corresponding peer neighbor to share the load of RP. To cancel this setting above, run the “no” form of this command.

anycast-rp *A.B.C.D* **nbr *.*.*.***

no **anycast-rp** *A.B.C.D* **nbr *.*.*.***

Parameter

Name	Prompt	Remarks
anycast-rp	anycast-rp –anycast rp for pim-sm	

Name	Prompt	Remarks
A.B.C.D	*A.B.C.D – anycast rp address*	
nbr	nbr – anycast rp neighbor	
.*.*.	*A.B.C.D – anycast rp neighbor address*	

Default value

This command takes no effect by default.

Command mode

pim-sm global view

Instruction

PIM-SM only regulates the standards of the single RP, but a big data flow can cause single RP overload easily. In this case, this command will be used to solve the overload of RP in the PIM-SM domain.

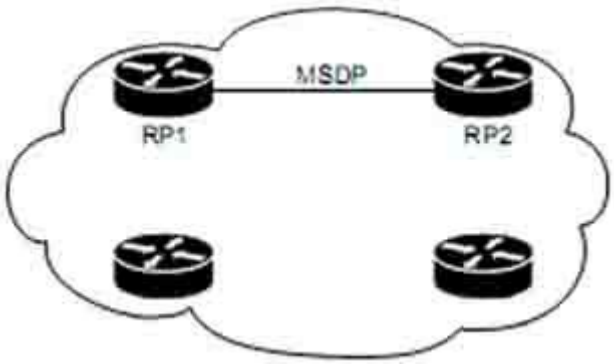
Note:

1. You'd better configure this command on the equipment with good connectivity in the PIM domain in the backbone network. That is, this command is not suitable to be set on the mute terminal router that connects other PIM equipments in the PIM domain through dial-up.

2. If the inside-domain MSDP is not used, the machine that specifies **anycast rp** must at the same time specify the address of a neighbor with the same RP address so as to facilitate the processing of the register.
3. The command, **anycast-rp A.B.C.D nbr**, is used on those devices that have no MSDP settings and provide an address as the static RP. All peer neighbors need be specified. The neighbors are reachable to one another.
4. If MSDP is set, the device, if it has provided the static RP address, need not specify **anycast rp nbr**.

Example

1. The following example shows how to set the **anycast-rp** address when MSDP is used.



RP1:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.1 255.255.255.255
I
ip msdp peer 10.1.1.2 connect-source loopback 1
ip msdp originator-id loopback 1

RP2:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.2 255.255.255.255
I
ip msdp peer 10.1.1.1 connect-source loopback 1
ip msdp originator-id loopback 1
Designate the static RP address on other devices, for example, do it on router Ra:
Ra:
router pim-sm
static-rp 10.0.0.1

2. The following example shows how to make settings when the MSDP is not used.

RP1:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.1 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2

static-rp 10.0.0.1

RP2:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.2 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2
static-rp 10.0.0.1
Designate the static RP address on other devices, for example, do it on router Ra:

Ra:
router pim-sm
static-rp 10.0.0.1

Related command

62.1.23 reg-rate-limit

As to (s, g), if you want to set the regeneration rate limit of the PIM-SM registration packets per second, you should use the **reg-rate-limit** command; to cancel this settings , you can run **no reg-rate-limit [*rate*]**.

reg-rate-limit *rate*

no reg-rate-limit [*rate*]

Parameter

Name	Prompt	Remarks
reg-rate-limit	reg-rate-limit - Rate limit for PIM data registers	
rate	<1-65535> Packets per second	

Default value

The regeneration rate of the registration packets of any (s,g) can be limited to one packet per second.

Command mode

pim-sm global view

Instruction

This command can be used to limit the regeneration rate of registration packets of (s.g) on the DR router. After this command is enabled, the load of the DR router will be limited. At the initial establishment of multicast path, the sudden eruption of large traffic of the multicast source may lead to packet loss due to the rate limit and the multicast receiver cannot receive all the multicast packets.

Example

The following example shows how to do the corresponding settings to let each (s.g) generate two registration packets per second.

Router_config#router pim-sm
Router_config_ps#reg-rate-limit 2

62.1.24 reg-src

To specify an IP address of a port to run as the source address for DR to transmit the PIM-SM registration packets, replacing the default port's address that connects the data source, run **reg-src**. If you use the **reg-src** command, the specified port must be active. To cancel this settings, you can run **no reg-src [***intf-type intf-number***]**.

reg-src *intf-type intf-number*

no reg-src [*intf-type intf-number***]**

Parameter

Name	Prompt	Remarks
reg-src	reg-src - Source address for PIM Register	
intf-type *intf-number*	Type of the designated port and its name	If a port has no main IP address or has no ID, the settings will take no effect. The L3 protocol of a designated port must be up.

Default value

By default, the port that connects DR and the data source will be used as the source address of the Register packet to conduct packet encapsulation.

Command mode

pim-sm global view

Instruction

When the default source address of the Register packet is not the only routable destination address for RP to return the Register Stop packet, you should use this command to set a new source address for the Register packet. For example, in cases that the source address of the Register packet will be filtered on RP by ACL or the source address is not the only IP address, the Register Stop packet returned by RP may not reach the corresponding DR correctly and then the PIM-SM registration finally may fail.

If the source address of the Register packet is not specified or the specified source address takes no effect, DR will choose the port, which connects the data source, as the source address of the Register packet. Therefore, it is recommended to set for the PIM-SM domain a unique routable address on the loopback port as the source address of the Register packet.

Example

The following example shows how to designate the address of the loopback3 port of DR as the source address of the Register packet.

```
Router_config#router pim-sm
Router_config_ps#reg-src loopback 3
```

62.1.25 spt-threshold

To set the traffic threshold for a flow to switch over to the shortest path tree, run **spt-threshold** in PIM-SM configuration mode. To resume the default settings, run **no spt-threshold**.

spt-threshold *{**infinity**/kbps} [stand-acl]*

no **spt-threshold**

Parameter

Name	Prompt	Remarks
spt-threshold	spt-threshold - Source-tree switching threshold	
infinity	Infinity - Never switch to source-tree	
kbps	<0-4294967> Traffic rate in kilobits per second	

Name	Prompt	Remarks
stand-acl	*stand-acl – ip standard access list name for group*	

Default value

There is no traffic limit for switchover. When the downstream receiver tries to join the data source, the data source will switch over to the SPT forwarding when it receives the data.

Command mode

pim-sm global view

Instruction

If the forwarding rate of a multicast source reaches or exceeds the designated threshold, the leaf node will send a (s,g) Join packet to the multicast source for constructing the source tree—the shortest path tree.

If the threshold is set to **infinity**, all multicast sources for the designated group take the sharing tree for packet forwarding. The group access list designates which groups use the configured threshold for SPT switchover. If the message flow from the data source is less than the designated threshold, the PIM-SM router of the leaf node will be switched back to the sharing tree after a period of time and then send the Prune message to the source tree.

Example

The following example sets a threshold of 4 kbps, above which traffic to a group from a source will cause the router to router to the shortest path tree to that source:

```
Router_config#router pim-sm
Router_config_ps# spt-threshold 4
```

Related command

None

62.1.26 ssm

To set the range of a specific multicast group, run **ssm {default | range** *std-acl}*. To cancel the designated SSM range, run **no ssm**.

ssm {default | range *std-acl}*

no **ssm**

Parameter

Name	Prompt	Remarks
ssm	ssm - Configure Source Specific Multicast	
Default	default - Use 232/8 group range for SSM	
Range	range - ACL for group range to be used for SSM	
std-acl	WORD - *ip standard access list name*	

Default value

disable

Command mode

pim-sm global view

Instruction

When PIM-SM is enabled, the default or configured range of the multicast group address can be used. If the multicast group is in the designated SSM range, the locally corresponding (,g) must be canceled. This requires the same strategic SSM shall be set in the whole PIM-SM.*

Note:

1. The same SSM strategy shall be set in the whole PIM-SM, otherwise the configured SSM will take no effect on preventing (*,g) Join for IGMPv3 can also specify the addition of (s,g) Join. Additionally, the (*,g) collision may be caused.
2. PIM-SM cannot be used together with other protocols. The configuration of SSM prevents the transmission of (*,g) Join and (*,*,rp) Join, and the PMBR device cannot send specific (s,g) Join to the upstream devices.
3. After SSM is set, MSDP cannot generate or receive SAs belonging to the designated range of the multicast group address. Our solution is that MSDP notification will be omitted if the group in the (S,G) items of PIM-SM is in the designated SSM group range,.
4. If the group range covers BIDIR group range, the previous configuration will be kept, and display error message to the later(not support now).

Example

The following example shows how to configure SSM service for the IP address range defined by access list 4:

Router_config#router pim-sm
Router_config_ps# ssm range grp_range
Router_config#ip access-list stand grp_range
Router_config_std_nacl# permit 224.2.151.141

Related command

None

62.1.27 c-bsr intf_type intf_name

To set a router to be a candidate BSR router, run the first of the following two commands; to cancel this settings, run the second one of the following two commands.

c-bsr *intf_type intf_name* [*hash-length* [*priority*]]

no **c-bsr** *[intf_type][intf_name][hash-length][priority]*

Parameter

Default value

Dynamic BSR selection is disabled.

Command mode

pim-sm global view

Instruction

After this command is set, the designated address of a port will be used as the BSR address and it will send BSM (bootstrap messages) to all PIM-SM neighbors on the local machine. Each neighbor will compare the previously received BSM with the currently received BSM, and if the BSR address in the current BSM is larger than or equal to that in the previously received BSM, the locally stored BSM will be updated and the current BSM will be forwarded; otherwise, the current BSM will be dropped directly. Before the candidate BSR receives the BSM with higher priority, it always regards itself as the BSM router in the corresponding management domain.

Note:

1. You'd better configure this command on the equipment with good connectivity in the PIM domain in the backbone network. That is, this command is not suitable to be set on the mute terminal router that connects other PIM equipments in the PIM domain through dial-up.
2. On accepting C-RP-Adv, BSR only accepts those contents that satisfy the SZ range; if the content exceeds the SZ range, it will be omitted.

3. You can specify only one port of a device as the BSR address; if multiple commands are set, the previously configured candidate BSRs will be replaced.
4. The condition for this command to be effective is that the IP address of the designated port is in PIM-SM state and the protocol is up.

Example

The following example configures the IP address of the router on Ethernet interface 0 to be a candidate BSR with priority of 10:

```
Router_config# router pim-sm
Router_config_ps# c-bsr f0/0 10 100
```

Related command

c-bsr admin-scope {global |*gaddr gmask***} [*hash-length* [*priority*]]**

62.1.28 c-bsr admin-scope

To set a candidate BSR in the administration domain, run the first one of the following two commands.

c-bsr admin-scope {global |*gaddr gmask***} [*hash-length* [*priority*]]**

no **c-bsr *admin-scope***

Parameter

Name	Prompt	Remarks
c-bsr	c-bsr –Candidate bootstrap router (candidate BSR)	
admin-scope	admin-scope – pim-sm administrator scope	
global	global – global range	224.0.0.0/255.0.0.0
gaddr	gaddr – sz group address	239.0.0.0 to 239.255.255.255
gmask	gmask – sz group mask	
hash-length	<0-32> - Hash Mask length for RP selection	
Priority	<0-255> - Priority value for candidate bootstrap router	

Default value

The global domain is 224.0.0.0/4 by default.

Command mode

pim-sm global view

Instruction

This command is used to set the candidate BSR in the administration domain. This command corresponds to the **admin-scope** command in the domain boundary and is used to specify the range of the administration domain.

Note:

1. If the command, c-bsr intf type intf name, is not configured, this command takes no effect.
2. It is recommended to set this command in the administration range (239.0.0.0--239.255.255.255).

Example

The following example shows that C-BSR only takes effect in the administration domain 239.1.1.0/24:

```
Router_config# router pim-sm
Router_config_ps#c-bsr f0/0 10 250
Router_config_ps#c-bsr admoni-scope 239.1.1.1 255.255.255.0
```

Related command

c-bsr *intf_type intf_name* [*hash-length* [*priority*]]

62.1.29 bsm-policy

To set the BSM reception policy, run the first one of the following two commands in PIM-SM configuration mode. To resume the default settings, run the other command.

bsm-policy { unicast *{rcvd* | *send}*| *forward-all* | *backward}*

no **bsm-policy** { unicast ***{rcvd* | *send}* |** *forward-all }*

Parameter

Name	Prompt	Remarks
bsm	bsm –bsm packet received	
policy	Policy – the policy for BSM receive and forward	
unicast	unicast –unicast bsm packet	The default value allows the reception of the unicast BSM packets. The backward compatibility supports the transmission of unicast BSM.
rvd	*rcvd*-permit receive bsm message	
forward-all	***forward-all – forward all bsm packet***	The horizontal division port will not forward all BSM packets, including unicast or no-forward-bit reset packets.
backward	***backward -*** backwards compatibility support send unicast BSM.	

Default value

There is no BSM reception or transmission policy.

Command mode

pim-sm global view

Instruction

Refer to the description of this command.

Example

The following example configures the local router can receive bsm unicasted from neighbor:

Router_config# router pim-sm
Router_config_ps# ***bsm-policy unicast rcvd***

Related command

None

62.1.30 static-rp

To set the static RP of PIM-SM, run the first one of the following two commands; to resume the default settings, run the other command.

static-rp ***rp-addr*** **[*std-acl*] [override][bidir]**

no **static-rp** *rp-addr*

Parameter

Name	Prompt	Remarks
static	static - configure static rp-address for pim-sm	
rp-addr	A.B.C.D – pim-sm rp-address (Rendezvous Point)	
std-acl	WORD – IP stand access list	
override	override –If conflict,the static rp prevails over the dynamic RP	When static RP goes against dynamic RP, if the parameter is not designated, the dynamic RP will be chosen first, and if no dynamic RP exists or dynamic RP takes no effect can static RP take effect.
bidir	bidir - Group range treated in bidirectional shared-tree mode	It is not supported currently.

Default value

disable

Command mode

pim-sm global view

Instruction

The designated IP address of static RP must be legal unicast address and cannot be the loopback address (127.0.0.0/8). If ACL is designated, the configured static RP will serve the matched multicast group; if ACL is not designated, the configured static RP will serve all multicast groups (224.0.0.0/4). When static RP goes against dynamic RP, the former will be first chosen.

In PIM-SM or BIDIR mode, each group will be provided with an RP. All routers in the same administration domain must follow the identical rule to set RP for the group. RP can be obtained through two mechanisms: static configuration of the RP address or the BSR mechanism's dynamic learning of RP address. The **static rp-address** command can be used to set an RP to be the aggregation point of multiple groups. The ACL configured by static RP defines the RP application range. If the standard ACL is not set, the designated static RP will be applied to all groups. One PIM router can use multiple RPs, but it can use the only RP for a specific group.

If multiple **static rp-address** commands are set, the matchup rules of group-to-rp are listed below:

1. If a group matches up with multiple static RP rules, suitable RPs can be chosen according to the longest matchup principle specified by the standard ACL. As to the static configuration without designated ACL, it can be applied to all groups, but the entries in the ACL must be first set.
2. If a group and multiple ACLs accord to the longest matchup principle, the IP addresses of RPs must be compared and those RPs with big IP addresses come prior in choice.
3. If the static RP configuration is adopted, the reachability test will not be conducted to the designated RP. If an RP is selected, the RP with a comparatively low RP will not be chosen even though the route of the selected RP does not exist locally.
4. Each command can be used to specify a static RP address. If the designated static RP address or ACL rule is same during configuration, the new configuration will replace the previous configurations.

In case static RP and dynamic RP are used together, the rules of group-to-rp are listed below:

1. When the override is not specified, the RPs, dynamically learned through the BSR mechanism, come prior to static RPs.
2. If dynamic RP is used, the **c-rp intf_type intf_name** command must be set.

Note:

1. The same RP cannot be used simultaneously on BIDIR and PIM-SM.
2. The statically configured RP only supports global SZ or provides support even if global SZ has not yet created.

Example

The following example shows how to designate 198.92.37.33 to be the static RP address.

Router_config#router pim-sm
Router_config_ps#static-rp 198.92.37.33

Related command

c-rp intf_type intf_name

62.1.31 c-rp intf_type intf_name

To set a port to be C-RP and to send the unicast notification periodically to a designated BSR router in the PIM-SM domain, run the first one of the following two commands. To resume the default settings, run the other command.

c-rp *intf-type intf-name* **[group-list** *std-acl***] [bidir][intvl** ***seconds*****][pri** ***pri-value*****]**

no **c-rp** *intf-type intf-name*

Parameter

Name	Prompt	Remarks
c-rp	c-rp - To be a PIMv2 RP candidate	
intf-type intf-name	Designating the interface type and the interface's name	PIM-SM must be enabled on C-RP.
group-list	group-list – ip access list for group-list	It is the prefix of the group address.
std-acl	WORD – ip stand access list	
bidir	bidir - Group range treated in bidirectional shared-tree mode	It is not supported currently.
intvl	Interval - RP candidate advertisement interval	
Seconds	<1-32767> - number of seconds	
pri	pri – RP priority	
pri-value	<0-255> - RP priority value	The smaller the value is, the higher the priority is. The default value is 192.

Default value

Dynamic RP selection is disabled.

Command mode

pim-sm global view

Instruction

This command is used to notify all BSRs on C-RP. The range of the group address is listed in a form of the standard ACL.

Note:

1. PIM-SM must be enabled on the port that serves as C-RP.
2. You'd better set C-RP on the main PIM-SM domain to avoid static configuration on similar routers or the on-demand dialup stub routers.
3. If C-RP is not specified with a multicast group range, C-RP will serve all multicast groups.
4. If you want to set a router to be C-RP for multiple group ranges, you need to represent multiple group ranges with multiple rules when configuring STD-AC1 that group-list corresponds to.
5. One port can only be set to one C-RP and the following configuration will replace the previous configuration, including the replacement of STD-AC1.
6. You can set C-RP for multiple ports on the same PIM-SM router.
7. Multiple C-RPs can use the same standard ACL.
8. If this command is run many times on a same interface, the previous configuration will be replaced.
9. If multiple SZs are known on C-RP, unicast C-RP-Adv will be sent to the BSR of each SZ. It is noted that the established group range cannot exceed the group range of the destination SZ.
10. If C-RP itself is the ZBR of an SZ, the Admin Scope Bit in the C-RP-Adv packet must be reset; otherwise, this bit will not be reset. At present, it is used for BSR to record logs but possible to be used for protocol expansion.

Example

The following example shows how to designate lo172 and lo173 to be C-RP ports, the former limiting to provide RP to the group of prefix 239.1/16.

```
Router_config#router pim-sm
Router_config_ps# c-rp loopback172 group-list grp-range
Router_config# ip access-list standard grp-range
Router_config_std_nacl# permit 239.1.0.0 255.255.0.0
Router_config_ps# c-rp loopback173
```

Related command

None

62.1.32 intvl-time

To enable the periodical transmission of join/prune packets and set the interval of periodically transmitting the Hello, BSM or C-RP-Adv packets, run the first of the following two commands:

intvl-time { join-prune *jp-intvl* | *hello hlo-intvl* | *c-bsr cbsr-intvl* |*crp-adv crp-intvl*| *spt-check [spt-intvl]}*

no **intvl-time** {**join-prune** [*jp-intvl*] **| *hello* [*hlo-intvl]* |*c-bsr[**cbsr-intvl**]*| *crp-adv* [*crp-intvl*] | *spt-check [**spt-intvl**]}***

Parameter

Name	Prompt	Remarks
join-prune	**join-prune -** pim-sm regular join/prune packet periodic	
jp-intvl	<1-65535> - value for JP timer	The default interval of transmitting Join/Prune packets is 60 seconds.
Hello	hello – pim-sm hello advertisement interval	Sets the interval of transmitting the Hello packets.
hlo-intvl	<1-65535> - value for JP timer	The default interval of transmitting Hello packets is 30 seconds.
c-bsr	c-bsr –Candidate bootstrap router (candidate BSR)	
cbsr-intvl	<1-65535> - value for c-bsr timer	The default interval of self selecting packets is 60 seconds.
crp-adv	crp-adv – pim-sm C-RP-ADV interval	Sets the interval of transmitting the C-RP-Adv packets.
crp-intvl	<1-65535> - value for CRP timer	The default interval of transmitting Report packets is 60 seconds.
spt-check	Spt-check – spt switch timer	
spt-intvl	<1-65535> - value for spt switch query timer	

Default value

See the above-mentioned table.

Command mode

pim-sm global view

Instruction

If the holdtime of Join-prune packet is not set and the **Join** packets from the downstream neighbor have not been received in three JP timeout periods, the downstream that corresponds to the multicast entry will be shifted to the **prune** state. The default holdtime is 3 minutes. The interval in port configuration mode is prior to the **join/prune** interval in global mode.

Example

The following example sets the join/prune advertisement interval value to 30 for global pimsm configuration:

Router_config#Router pim-sm
Router_config_ps#timer join-prune 30

Related command

holdtime

62.1.33 holdtime

To set the interval of the timeout timer of PIM-SM, run the first one of the following two commands. To resume the default settings, run the other command.

holdtime {join-prune *jp-hold* | assert *asrt-hold* | c-bsr *cbsr-**hold*** | **crp-adv *crp-hold* | sz *sz-hold*}**

no **holdtime {join-prune** [*jp-hold*] **| assert** [*asrt-hold*] **| c-bsr** [*cbsr-hold*] **| crp-adv** [*crp-hold*] **| *sz*** [*sz-hold*]**}**

Parameter

Name	Prompt	Remarks
holdtime	holdtime – hold timer for keep the status	
join-prune	Join-prune –join-prune status hold timer	

Name	Prompt	Remarks
jp-hold	<1-65535> - time value (second)	The default value is 210 seconds.
assert	assert – assert status hold timer	
asrt-hold	<7-65535> - time value (second)	The default value is 180 seconds.
c-bsr	c-bsr –Candidate bootstrap router (candidate BSR)	
cbsr-hold	<1-65535> - time value (second)	By default, it is as follows: holdtime timeout time= holdtime's interval*2+10 By default, the holdtime's interval is 60 seconds and the holdtime's timeout time is therefore 130 seconds.
c-rp	c-bsr –Candidate bootstrap router (candidate BSR)	
crp-hold	<1-65535> - time value (second)	The default value is 150 seconds. Because non-BSR updates its timeout time through the BSR's holdtime packets, the timeout time of C-RP must not be less than the interval of holdtime packet transmission. It is best when the former is 2.5 intervals or beyond.
sz	sz –scope zone timer	
sz-hold	<10-4294967295> - time value (second)	The default value is 1300 seconds.

Default value

See the above-mentioned table.

Command mode

pim-sm global view

Instruction

If the holdtime is set on a port, first comes the configuration of this port and then the global configuration; finally, if neither configuration is done, the default configuration will be chosen.

Note:

- When configuring the holdtime of C-RP, you should set the timeout time of C-RP to 2.5 holdtime transmission intervals or beyond to prevent the C-RP loss in the BSR holdtime packet.
- The timeout time of SZ must be longer than the BSR timeout time and you'd better set it to be 10 BSR timeout times.

Example

The following example shows how to set the holdtime of C-RP to 150 seconds, among which C-RP and C-BSR are not set on Ra.

Ra_config# router pim-sm
Ra_config_ps# holdtime c-rp 200

Related command

intvl-time

62.1.34 log

To enable the log switch to record DR's change, neighbor's up or down, address conflict and abnormal packets, run the first one of the following two commands:

log { nbr-change | ipaddr-conflict | pkt-conflict }

no **log** ***{ nbr-change | ipaddr-conflict | pkt-conflict }***

Parameter

Name	Prompt	Remarks
Log	log - To log conflict	
nbr-change	nbr-change – neighbor up/donw or DR changes	
ipaddr-conflict	ipaddr-conflict –secondary ip address is conflict with the another neighbor	

Name	Prompt	Remarks
pkt-conflict	pkt-conflict – pim-sm mroute items conflict in the pimsm pkt	

Default value

The log function is disabled.

Command mode

pim-sm global view

Instruction

If there is the log server, the corresponding logs will be recorded to the log server.

Example

The following example configures the router to log the conflict when the exist secondary ip address is also contained in hello packet when receivd from another neighbor.

```
Router_config_ps# log nbr-change
```

Related command

None

62.1.35 show running-configure

To display the global PIM-SM information and the main configuration information about a port, run the following command:

show running-configure

Parameter

None

Default value

None

Command mode

EXEC

Instruction

According to the output information, you can check the configuration information about the current PIM-SM.

Example

62.1.36 show ip pim-sm bsr-router

Syntas

show ip pim-sm bsr

Parameter

None

Default

None

Command mode

Management mode

Explanation

Display PIM-SM router BSR message .

Example

```
R142#show ip pim-sm bsr-router
PIMv2 BSR information:
I am BSR!
  Address of BSR: 192.166.100.142
  BSR Priority: 201 Hash Mask Length: 30 Uptime: 00:10:56
  Next BSM will be sent in 00:00:04
Candidate-RP: 192.166.100.142(Loopback0)
  Interval of Advertisements: 60 seconds
  Next Advertisement will be sent in 00:00:04
```

Relevant command

None

62.1.37 show ip pim-sm interface

Syntas

show ip pim-sm interface [**type** *number*]

Parameter

Parameter	Description
type	Port type
number	Port number

Default

None

Command mode

Management mode

Explanation

Display PIM-SM router port imformation .

Example

```
R142#show ip pim-sm interface
Address         Interface    Ver/   Nbr    Query   DR      DR
                             Mode   Count  Intvl   Prior
192.168.21.142  Serial2/0    v2/S   1      30      1       192.168.21.144
192.168.100.142 Ethernet1/1  v2/S   1      30      100     192.168.100.142
192.166.100.142 Loopback0    v2/S   0      30      1       192.166.100.142
```

Relevant command

None

62.1.38 show ip pim-sm neighbor

Syntas

show ip pim-sm neighbor [**type** *number*]

Parameter

Parameter	Description
type	Port type
number	Port number

Default

None

Command mode

Management mode

Explanation

Display PIM-SM router neighbor information.

Example

```
R142#show ip pim-sm neighbor
PIM Neighbor Table
Neighbor          Interface      Uptime/Expires      Ver     DR
Address                                              Prio
192.168.21.144    Serial2/0      00:03:53/00:01:22   v2      1
192.168.100.143   Ethernet1/1    00:03:34/00:01:41   v2      1
```

Relevant command

None

62.1.39 show ip pim-sm rp

Syntas

show ip pim-sm rp [**mapping**|**metric**]

Parameter

Parameter	Description
mapping	Displays RP—GROUP mapping relation.
metric	Displays each RP simple-cast route metric.

Default

None

Command mode

Management

Explanation

Display PIM-SM router RP mapping information .

Example

R144#show ip pim-sm rp
GROUP: 225.1.1.10, RP: 9.1.1.1, Version2 Uptime: 1d01h07m, Expires in 00:02:16

Relevant command

None

62.1.40 show ip pim-sm rp-hash

Syntas

show ip pim-sm rp-hash [*group-address*]

Parameter

Parameter	Description
group-address	Group address.

Default

None

Command mode

Management mode

Explanation

Display specify multicast address hash accout value.

Example

R142#show ip pim-sm rp-hash 225.1.1.10
RP: 192.166.100.142
Info Source: 192.166.100.142, via BSR
Uptime: 00:00:08, Expires: 00:02:22

Relevant command

None

62.1.41 show ip mroute pim-sm

Syntas

show ip mroute pim-sm [*group-address*|*source-address*] [**type** *number*] [**summary**|**count**] [**active** *kbps*]

Parameter

Parameter	Description
group-address	Group address.
source-address	source-address
type	Port type
number	Port number
summary	Display table PIM-SM entry
count	Display (S,G) stat information
active	Activity sending data speed

Default

None

Command mode

Management mode

Explanation

Display PIM-SM multicast route information.

Example

```
R142#show ip mroute pim-sm
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir group, s - SSM group,
I - IGMP report, R - RP-bit set, F - Register flag, T - SPT-bit set,
J - Join Needed, P - Pruned,
Timers: Uptime/Expires
(*, 225.1.1.10), 00:15:14/00:02:37, RP 9.1.1.1, flags: SRJ
Incoming interface: Ethernet1/1, RPF nbr 192.168.100.143
Outgoing interface list:
Serial2/0, Forward/Sparse, 00:13:23/00:02:37
```

(192.166.1.253, 225.1.1.10), 00:15:14/00:02:46, flags: STJ
Incoming interface: Ethernet1/1, RPF nbr 192.168.100.143
Outgoing interface list:
Serial2/0, Forward/Sparse, 00:15:14/00:02:46
(192.168.20.141, 225.1.1.10), 00:15:14/00:02:46, flags: STJ
Incoming interface: Ethernet1/1, RPF nbr 192.168.100.143
Outgoing interface list:
Serial2/0, Forward/Sparse, 00:15:14/00:02:46

Relevant command

None

62.1.42 show ip rpf pim-sm

Syntas

show ip rpf pim-sm {*source-address*} **metric**

Parameter

Parameter	Description
source-address	Source address.
metric	Simple-cast route Metric

Default

None

Command mode

Management mode

Explanation

Display specify source address converse forwarding information.

Example

R142#show ip rpf pim-sm 192.166.1.143
RPF information for 192.166.1.143
RPF interface: Ethernet1/1
RPF neighbor: 192.168.100.143
RPF route/mask: 192.166.1.0/24
RPF type: unicast (rip)
RPF recursion count: 0
Doing distance-preferred lookups across tables

Relevant command

None

62.1.43 debug ip pim-sm alert

To display the alert information from mrouting or IP, run the first one of the following two commands.

debug ip pim-sm alert

no debug ip pim-sm alert

Parameter

None

Default value

None

Command mode

EXEC

Instruction

VTY will be exported if the alart information from mrouting or aged (s,g).

Example

The following example shows that the route event of RIP is monitored.

router# debug ip rip database
RIP-DB: Adding summary route 192.1.1.0/24 <metric 0> to RIP database

The fields in the previous example are explained in the following table:

Domain	Description
summary	Route type which is added to the routing table
192.1.1.0/24	Route which is added to the routing table
<metric 0>	Value of the route's metric

62.1.44 debug ip pim-sm assert

To monitor the Assert event of PIM-SM, run the first one of the following two commands:

debug ip pim-sm assert [packet | state- machine | A.B.C.D **]**

no debug ip pim-sm assert [packet | state- machine | A.B.C.D **]**

Parameter

Name	Prompt	Remarks
state- machine	Show state machine activity debug information	
packet	Trace information about packet	
A.B.C.D	Group address for stm and packet output	

Default value

None

Command mode

EXEC

Instruction

According to the output information, you can check the current assert event of PIM-SM.

Result

- Show (S,G) Assert State-machine Actions
- Show (*,G) Assert Message State Machine actions
- Show activity after timer timerout
- Show packet activity

62.1.45 debug ip pim-sm bsr

To monitor the BSM event of PIM-SM, the C-RP-ADV event or the BSR state machine, run the first one of the following two commands:

debug ip pim-sm assert [packet | state- machine**]**

no debug ip pim-sm assert [packet | state- machine**]**

Parameter

Name	Prompt	Remarks
state- machine	Show state machine activity debug information	
packet	Trace information about packet	

Default value

None

Command mode

EXEC

Instruction

According to the output information, you can check the BSM event of PIM-SM, the C-RP-ADV event or the BSR state machine.

Example

62.1.46 debug ip pim-sm rp

To monitor the related events and packets about PIM-SM-RP-SET change, run the first one of the following two commands:

debug ip pim-sm rp

no debug ip pim-sm rp

Parameter

None

Default value

None

Command mode

EXEC

Instruction

This command is used to export the reception and transmission of C-RP-ADV and the RP-SET change. As to the change of static RP, no debugging information will be exported at present.

Example

62.1.47 debug ip pim-sm entry

To export the creation and update of (*,*,rp), (*,g), (s,g,rpt) and (s,g,spt) and their simultaneous change of them at the time of RP change, run the first one of the following two commands.

debug ip pim-sm entry

no debug ip pim-sm entry

Parameter

None

Default value

None

Command mode

EXEC

Instruction

According to the output information, you can browse the information about PIMSM creation and update of multicast routing entries.

Example

62.1.48 debug ip pim-sm event

To export all events that PIMSM main task receives, run the first one of the following two commands.

debug ip pim-sm event

no debug ip pim-sm event

Parameter

None

Default value

None

Command mode

EXEC

Instruction

According to the output information, you can browse all events of current PIMSM.

Example

62.1.49 debug ip pim-sm hello

To display the Hello packet received or transmitted by PIM-SM for debugging the neighbor's information, run the first one of the following two commands.

debug ip pim-sm hello

no debug ip pim-sm hello

Parameter

Name	Prompt	Remarks
pim-sm	Show state machine activity debug information	
hello	Show information about packet sending and receiving	

Default value

None

Command mode

EXEC

Instruction

According to the output information, you can browse the Hello packets, including those received or transmitted by PIM-SM, to know what's going on the local machine or the neighbors.

Results

- The ports, source addresses and genid of the currently received or transmitted Hello packets can be displayed.

Example

62.1.50 debug ip pim-sm jp

To trace the Join/Prune event of (*,g) or (s,g), run the first one of the following two commands.

debug ip pim-sm jp [packet | state- machine | A.B.C.D **]**

no debug ip pim-sm jp [packet | state- machine | A.B.C.D **]**

Parameter

Name	Prompt	Remarks
state- machine	Show state machine activity debug information	
packet	Trace information about packet	
A.B.C.D	Group address for stm and packet output	

Default value

None

Command mode

EXEC

Instruction

Example

62.1.51 debug ip pim-sm nbr

To trace the related events of a neighbor, such as the addition of neighbor, aging deletion or DR selection, run the first one of the following two commands.

debug ip pim-sm nbr

no debug ip pim-sm nbr

Parameter

None

Default value

None

Command mode

EXEC

Instruction

According to the output information of this command, you can browse neighbor change, neighbor refreshment, GENID change and DR selection.

Example

62.1.52 debug ip pim-sm packet

To trace the protocol control packets received or transmitted by PIM-SM, run the following command.

debug ip pim-sm packet

Parameter

None

Default value

None

Command mode

EXEC

Instruction

After this command is run, the PIM-SM packet's type will be displayed.

Example

62.1.53 debug ip pim-sm register

To display the registration packet and register state event of PIM-SM, run the first one of the following two commands.

debug ip pim-sm register [packet | state- machine | A.B.C.D **]**

no debug ip pim-sm register [packet | state- machine | A.B.C.D **]**

Parameter

Name	Prompt	Remarks
state- machine	Show state machine activity debug information	
packet	Trace information about packet	
A.B.C.D	Group address for stm and packet output	

Default value

None

Command mode

EXEC

Instruction

According to the output information, you can check the register event of PIM-SM.

Example

62.1.54 debug ip pim-sm timer

To display the change of all PIM-SM timers, including creation, deletion, stop and timeout, run the first one of the following two commands.

debug ip pim-sm timer

no debug ip pim-sm timer

Parameter

None

Default value

None

Command mode

EXEC

Instruction

The PIM-SM timers include the Hello timer, the neighbor timeout timer, the Join/Prune timer, the override timer, the prune pending timer, the keepalive timer, the assert timer, the register timer, the register limit timer, the BSM timer, and so on.

Example

Chapter 63 Multicast VPN Settings

The MVPN functionality is supported on the routers.

63.1.1 **Ip multicast-routing vrf** *vpn-instance-name*

To enable the multicast on VRF, run the following command:

Ip multicast-routing vrf vpn-instance-name

Parameter

Parameter	Description
vpn-instance-name	Enables the VPN instance of multicast.

Default value

None

Command mode

EXEC mode

Instruction

After this command is run, the system enters the MVPN configuration mode.

If you run the “no” form of this command, the related VPN multicast will be disabled.

Example

The following example shows how to enable the multicast on VRF.

```
R4_config#ip multicast-r vrf RED
R4_config_mvpn_(RED)#
```

Related command

Ip vrf vpn-instance

Before enabling the VPN multicast, you have to configure related VPN.

63.1.2 **mdt share-group** group-address **binding mtunnel** number

To designate the share group address of this VPN multicast and the bound Mtunnel ID, run the following command:

mdt share-group 232.1.1.1 **binding mtunnel** 0

Parameter

Parameter	Description
Number	Stands for the Mtunnel ID, which is an indispensable parameter and disabled by default. One Mtunnel is bound to only one MVPN.
group-address	Stands for the share group's address, which is an indispensable parameter and disabled by default.

Default value

None

Command mode

MVPN configuration mode

Instruction

This command can be regarded as the switch of global MVPN.

If you want to cancel the share-group settings and the Mtunnel binding, you shall run **no mdt share-group**.

Before you want to modify the share group's address or bind other Mtunnel, you have to cancel the previous binding through the **no mdt share-group** command.

Example

The following example shows how to set the share group and bind Mtunnel.

R4_config_mvpn_(RED)#mdt share-group 232.1.1.1 binding mtunnel 0

Related command

63.1.3 mdt connect-src interface

To designate the connect-source address of VPN multicast, run the following command:

mdt connect-src interface

Parameter

Parameter	Description
Interface	Stands for the currently existent port, such as loopback0.

Default value

None

Command mode

MVPN configuration mode, which can be entered through the ip **multicast-routing vrf vpn-instance** command

Instruction

This command can be used to bind the address of the Mtunnel port. When the Mtunnel obtains its binding address, the Mtunnel is up and then receives or transmits the packets.

It is recommended that the Mtunnel address should be the same as the connect-src address of BGP and that the loopback port should be used as the binding port of Mtunnel.

Example

以下示例将 loopback0 指定为该 mvpn 的绑定地址

R4_config_mvpn_(RED)#mdt connect-src loopback0

Related command

63.1.4 mdt switch-group-pool group-address group-mask threshold

To designate the range of the switch pool, run the following command:

mdt switch-group-pool 238.1.1.1 255.255.255.0 **threshhold** number

Parameter

Parameter	Description

number	Designates the value of threshold, whose unit is packet/second. The default threshold is 10 packets/second.
Group-address group-mask	Designates a switch pool on the condition that the group mask must be between 225.225.225.0 and 225.255.255.255.

Default value

None

Command mode

MVPN configuration mode, which can be entered through the ip **multicast-routing vrf vpn-instance** command

Instruction

This command is used to designate the range of the switch pool and then the switch pool is used for data MDT switchover.

Example

The following example shows how to designate 238.1.1.1/24 as the switch pool and how to set the switchover threshold to 10 packets/second.

R4_config_mvpn_(RED)#-group-pool 238.1.1.1 255.255.255.0 threshhold 10

Related command

63.1.5 mdt mdt switch-delay

To set how long the system switches over to data MDT after the switchover conditions are ready and the JointLV packet is transmitted, run the following command:

mdt mdt switch-delay number

Parameter

Parameter	Description
Number	INTEGER<3-60> Value of multicast-domain switch-delay(second)

Default value

5 seconds

Command mode

MVPN configuration mode, which can be entered through the ip **multicast-routing vrf vpn-instance** command

Instruction

This command is used to designate the switchover time of data MDT.

Example

The following example shows how to set the switchover time to 4 seconds.

R4_config_mvpn_(RED)#mdt switch-delay 4

Related command

63.1.6 mdt hold-down

To designate the hold-down timer of data MDT, run the following command.

mdt hold-down number

Parameter

Parameter	Description
Number	INTEGER<0-180> Value of multicast-domain holddown-time(second)

Default value

60 seconds

Command mode

MVPN configuration mode, which can be entered through the ip **multicast-routing vrf vpn-instance** command

Instruction

This command is used to designate the hold-down time of data MDT to prevent the twitter. Before the hold-down time times out, the data MTD mapping cannot be deleted.

Example

The following example shows how to set the hold-down time to 70 seconds.

R4_config_mvpn_(RED)#mdt holddown-time 70

Related command

63.1.7 mdt rd-list

To set the RD of the peer VRF, run the following command:

mdt rd-list rd

Parameter

Parameter	Description
rd	ASN:nn or IP-address:nn -- VPN Route Distinguisher

Default value

None

Command mode

MVPN configuration mode, which can be entered through the ip **multicast-routing vrf vpn-instance** command

Instruction

Example

The following example shows how to make settings to enable VRF RED to accept the multicast flow of VRF BLUE.

```
ip vrf RED
 rd 100:1

ip vrf BULE
 rd 200:1

R4_config_mvpn_(RED)#mdt rd-list 200:1
```

Related command

63.1.8 show ip mroute vrf vpn-instance pim-s jointlv

To browse the Join Tlv options of VPN, run this command.

Parameter

Parameter	Description
Vpn-instance	Browses the name of VPN instance.

Default value

None

Command mode

Instruction

Example

R4#show ip mroute vrf RED pim-s joint
(1.1.1.160 239.1.1.1) p sg:(10.0.1.1 232.2.1.1) couter:0 flag:R
mi:00:00:00 dd:00:00:00 hd:00:00:00 dt:00:02:51

In this example, **psg** stands for the sg address peer encapsulated by the public network, **flag** stands for the local distribution when it is **a**, or the remote distribution if it is **r**.

The second line shows 4 related timers.

Related command

63.1.9 debug ip pim-s mvpn

To trace the events related to MVPN and PIM-SM, run **debug ip pim-s mvpn**. To resume this default settings, run **no debug ip pim-s mvpn**.

Parameter

Parameter	Description
None	

Default value

None

Command mode

Instruction

Example

R4#show ip mroute vrf RED pim-s joinatb

(20.0.4.4 232.1.1.1) assigner:0.0.0.0 proxy:172.16.34.4

atb_t:00:00:00 rd: 100:1

In this example, the assigner address is the address of the JINATB releaser. If the assigner address is 0.0.0.0, it means the local distribution.

The proxy address stands for the agent address for this flow to send the Join packet.

If it is the remote distribution, **atb_t** will time out.

Related command

63.1.10 debug ip multicast mvpn

To trace and observe the MVPN-related events, run this command.

Parameter

Parameter	Description
None	

Default value

None

Command mode

Instruction

Example

Related command

Chapter 64 IPv6 Configuration Commands

64.1 IPv6 Configuration Commands

IPv6 configuration commands include the following ones:

- ipv6 address
- ipv6 address anycast
- ipv6 address autoconfig
- ipv6 address eui-64
- ipv6 address link-local
- ipv6 enable
- show ipv6 interface

64.1.1 ipv6 address

To set an IPv6 address in port configuration mode and meanwhile enable IPv6 on a port, run **ipv6 address {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}.** To delete the IPv6 address on a port, run **no ipv6 address [*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*]**.

ipv6 address { *ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length* **}**

no ipv6 address [*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length* **]**

Parameter

Parameter	Description
ipv6-address	Means the to-be-added IPv6 address.
/prefix-length	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.
Prefix-name	Means a general prefix, defining the network part of the IPv6 address.
Sub-bits	Means the host part of the IPv6 address. It combines with the prefix, which is defined by prefix-name, to form an IPv6 address. This parameter must support the IPv6 address format regulated in RFC2373.

Default value

No default IPv6 address exists on the VLAN port.

Command mode

Interface configuration mode

Instruction

If you run **no ipv6 address**, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted.

Example

The following example shows how to set an IPv6 address in VLAN port configuration mode and meanwhile enable IPv6 on the VLAN port.

```
Switch_config_v1# ipv6 address 2001:0:0:0:0DB8:800:200C:417A/64
```

Related command

ipv6 address anycast

ipv6 address eui-64

ipv6 address link-local

show ipv6 interface

64.1.2 ipv6 address anycast

To set an anycast address and enable IPv6 on the VLAN port, run the first one of the following two commands:

ipv6 address *ipv6-prefix/prefix-length* **anycast**

no ipv6 address [*ipv6-prefix/prefix-length* **anycast]**

Parameter

Parameter	Description
Ipv6-prefix	Means the network part of the IPv6 address.
/prefix-length	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.

Default value

It is set as an anycast address on the VLAN port by default.

Command mode

Interface configuration mode

Instruction

If you run **no ipv6 address**, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted.

Example

Switch_config_v1# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast

Related command

ipv6 address aui-64

ipv6 address link-local

show ipv6 interface

64.1.3 ipv6 address autoconfig

To use the stateless auto-configuration protocol to set an IPv6 address, run **ipv6 address autoconfig** in VLAN port configuration mode.

Ipv6 address autoconfig

no ipv6 address autoconfig

Parameter None

Default value

By default, IPv6 address auto-configuration is not used.

Command mode

Interface configuration mode

Example

Switch_config_v1# ipv6 address autoconfig

64.1.4 ipv6 address eui-64

To set an IPv6 address in VLAN port configuration mode, run **ipv6 address eui-64**.

ipv6 address *ipv6-prefix/prefix-length* **eui-64**

ipv6 address [*ipv6-prefix/prefix-length* **eui-64]**

Parameter

Parameter	Description
Ipv6-prefix	Means the network part of the IPv6 address.
/prefix-length	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.

Default value

The IPv6 address in the eui-64 form is not configured on the VLAN port.

Command mode

Interface configuration mode

Instruction

If you run **no ipv6 address**, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted.

If the **prefix-length** parameter is bigger than 64 bits, the prefix-length is prior to the length of the VLAN port ID.

Example

Switch_config_v1# ipv6 address 2001:0:0:0:0DB8::/64 eui-64

Related command

ipv6 address link-local
show ipv6 interface

64.1.5 ipv6 address link-local

To set a link-local address in VLAN port configuration mode and meanwhile enable IPv6 on the VLAN port, run the first one of the following two commands:

ipv6 address *ipv6-address* **link-local**

no ipv6 address [*ipv6-address* **link-local]**

Parameter

Parameter	Description

ipv6-address	Means the to-be-added IPv6 address. The format of this address must abide by the definition in RFC 4291 strictly.
link-local	Means a link-local address. The link-local address designated by the **ipv6-address** command will automatically replace the automatically configured link-local address.

Default value

No default IPv6 link-local address exists on the VLAN port.

Command mode

Interface configuration mode

Instruction

If you run **no ipv6 address**, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted. If you run **ipv6 enable**, a link-local address will be automatically set. Of course you can set the link-local address manually, the command you will use is **ipv6 address link-local**.

Example

The following example shows how to set a link-local address manually on the VLAN port:

```
Switch_config_v1# ipv6 address FE80::A00:3EFF:FE12:3457 link-local
```

Related command

ipv6 address eui-64

show ipv6 interface

64.1.6 ipv6 enable

If the IPv6 address is not set on the VLAN port but users want to enable the IPv6 protocol on this port, run **ipv6 enable**.

ipv6 enable

no ipv6 enable

Parameter

Parameter	Description

Default value

The IPv6 protocol is forbidden on the VLAN port.

Command mode

Interface configuration mode

Instruction

After the **ipv6 enable** command is run, the system will add a link-local address on the VLAN port automatically. At the same time, the communication range of the IPv6 protocol on the VLAN port is confined to the links that the VLAN port connects. If the IPv6 address has already configured on the VLAN port explicitly, you cannot forbid IPv6 processing on the VLAN port even though you use the **no ipv6 enable** command.

Example

```
Switch_config# interface vlan 1
Switch_config_v1# ipv6 enable
```

Related command

ipv6 address link-local

ipv6 address eui-64

show ipv6 interface

64.1.7 show ipv6 interface

To show the information about the VLAN port on which the IPv6 protocol is enabled, run the following command:

show ipv6 interface [*interface-type interface-number* **] | [brief]**

Parameter

Parameter	Description
interface-type	Stands for the type of the VLAN port.
interface-number	Stands for the ID of the VLAN port.

Default value

Those VLAN ports on which the IPv6 protocol is enabled will all be displayed.

Command mode

Global configuration mode

Instruction

This command can be used to display the state of IPv6 on the VLAN port, the configured IPv6 address and other IPv6 related parameters.

Example

The following example shows how to display the IPv6 state on port vlan1:

```
Switch# show ipv6 interface vlan 1

Vlan1 is up, line protocol is down
  IPv6 is enabled, link-local address is FE80::A00:3EFF:FE12:3457 [TENTATIVE]
  Global unicast address(es):
    5678::111, subnet is 5678::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF12:3457
    FF02::1:FF00:111
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are enabled
```

Field	Description
Vlan1 is up(down/administratively down)	Indicates whether the physical layer of the VLAN port is accessible or whether it can be shut down manageably.
line protocol is up(down)	Indicates whether the line protocol (the software layer) is accessible.
IPv6 is enabled	Enables the IPv6 protocol.
link-local address	Displays the link-local address of a port.
Global unicast address(es)	Displays the unicast address of a port.
Joined group address(es)	Displays the multicast address of a port.
MTU	Displays the MTU of a port.
ICMP error messages	Displays the transmission frequency of ICMPv6 error packets (the minimum interval).
ICMP redirects	Displays whether the redirection packet will be sent or not.

ICMP unreachables	Displays whether the destination unreachable packet will be enabled or shut down.

Related command

Chapter 65 IPv6 Configuration Commands

65.1 IPv6 Configuration Commands

IPv6 configuration commands include the following ones:

- clear ipv6 traffic
- debug ipv6 packet
- ipv6 cur-hoplimit
- ipv6 icmp6-ratelimit
- ipv6 mtu
- ipv6 redirect
- ipv6 source-route
- show ipv6 pmtu
- show ipv6 traffic

65.1.1 clear ipv6 traffic

To delete the statistics information about the IPv6 flow, run the following command:

clear ipv6 traffic

Parameter

Parameter	Description

Command mode

EXEC

Instruction

This command is used to delete all the statistics information about IPv6 flow.

Example

The following example shows how to delete the statistics information about IPv6 flow:

```
Switch# clear ipv6 traffic
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 badhdrs, 0 badvers
         0 tooshort, 0 toosmall, 0 toomanyhdrs
         0 source-routed, 0 badscope
         0 badopts, 0 unknowopts, 0 exthdrtoolong
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  0 generated, 0 forwarded, 0 cant forwarded
         0 fragmented into 0 fragments, 0 failed
         0 no route
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd:  0 total, 0 format errors, 0 checksum errors
         0 unreachable, 0 packet too big
         0 time exceeded, 0 parameter problem
         0 echos, 0 echo replies
         0 membership query, 0 membership report, 0 membership reduction
         0 Switch solicitations, 0 Switch advertisements
         0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
  Sent:  0 total, 0 bandwidth limit
         0 unreachable, 0 packet too big
         0 time exceeded, 0 parameter problem
         0 echos, 0 echo replies
         0 membership query, 0 membership report, 0 membership reduction
         0 Switch solicitations, 0 Switch advertisements
         0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
```

Related command

show ipv6 traffic

65.1.2 debug ipv6 packet

To display the debug information about the IPv6 packet, run the first one of the following two commands:

debug ipv6 packet [*interface-type interface-number* | **access-list** [access-list-namae] **]**

no debug ipv6 packet

Parameter

Parameter	Description
Interface-type	Type of the interface (optional)
Interface-number	ID of an interface (optional)
access-list-namae	Name of ACL (optional)

Default value

The debug information is closed in default settings.

Command mode

EXEC

Example

The following example shows how to export the IPv6 debug information:

```
Switch# debug ipv6 packet
2002-1-1 05:07:16
IPv6: source FE80::A00:3EFF:FE12:3459, dest FF02::1
      plen 32, proto 58, hops 255
      sending on Ethernet1/0
```

Field	Description
source	Source address in the IPv6 packet
dest	Destination address in the IPv6 packet
plen	Load length in the IPv6 packet
proto	Protocol for the next header encapsulation, which is presented by next-header in the IPv6 packet
hops	Value of hop-limit in the IPv6 packet
sending (receving , forwarding) on Ethernet	Displays packet transmission, reception and forwarding on an interface.

Related command

65.1.3 ipv6 cur-hoplimit

To configure the maximum hop-limit value in the RA packet and the hop-limit value which is applied in the IPv6 header of all transmitted packets, run the first one of the following two commands:

ipv6 cur-hoplimit *values*

no ipv6 cur-hoplimit *values*

Parameter

Parameter	Description
values	Stands for the maximum value of hop-limit (1-255).

Default value

The default hop-limit is 64.

Command mode

Interface configuration mode

Example

The following example shows how to set the maximum hop-limit value in the RA packet and the hop-limit value which is applied in the IPv6 header of all transmitted packets.

Switch_config_v1# ipv6 cur-hoplimit 16

65.1.4 ipv6 general-prefix

To define a general IPv6 prefix, run the first one of the following two commands:

ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

no ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

Parameter

Parameter	Description
Prefix-name	Stands for the name of a general prefix.
Ipv6-prefix	Stands for the general IPv6 prefix (that is, the network part of the IPv6 address). This parameter must support the IPv6 address format regulated in RFC2373.
/Prefix-length	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.

Default value

There is no default general prefix.

Command mode

Global configuration mode

Example

The following example shows how to set a general IPv6 prefix:

Switch_config# ipv6 general-prefix my-prefix 2001:DB8:2222::/48

65.1.5 ipv6 icmp-ratelimit

To set the minimum interval of ICMPv6 error packet transmission, run the first one of the following two commands:

ipv6 icmp-ratelimit *us*

no ipv6 icmp-ratelimit

Parameter

Parameter	Description
us	Stands for the minimum interval (unit: milisecond).

Default value

1000 miliseconds

Command mode

Global mode

Instruction

This command can be used to set the transmission frequency of ICMPv6 error packets.

Example

Switch_config# ipv6 icmp6-ratelimit 2000

65.1.6 ipv6 mtu

To set the MTU of the VLAN port, run the first one of the following two commands:

ipv6 mtu *bytes*

no ipv6 mtu *bytes*

Parameter

Parameter	Description
bytes	Stands for MTU, whose unit is byte.

Default value

The default value depends on the port type, but the minimum value of any port is 1280 bytes.

Command mode

Interface configuration mode

Instruction

When MTU is the default value, RA has the MTU option.

When a switch forwards packet, a packet will not be fragmented just because the MTU of the egress is smaller than the packet's length. But it will be fragmented only when the transmitted packet is generated.

Example

The following example shows how to set the MTU of a port:

Switch_config_v1# ipv6 mtu 2000

Related command

show ipv6 interface

65.1.7 ipv6 redirects

To control whether to transmit a redirection packet after the packet is forwarded, run **ipv6 redirects**.

ipv6 redirects

no ipv6 redirects

Parameter

Parameter	Description

Default value

The redirection packet will be transmitted by default.

Command mode

Interface configuration mode

Instruction

The redirection packets are transmitted through the ICMPv6 protocol.Because of the limitation of the ipv6 icmp-ratelimit command, the redirection packet may not be transmitted.

Example

The following example shows how to shut down a port to transmit the redirection packet.

Switch_config_v1# no ipv6 redirects

Related command

ipv6 icmp-ratelimit

show ipv6 interface

65.1.8 ipv6 source-route

To enable a switch to process the packets with type0 source route, run **ipv6 source-route**.

ipv6 source-route

no ipv6 source-route

Parameter

Parameter	Description

Default value

The type 0 source route is handled in default settings.

Command mode

Global configuration mode

Instruction

If you want to forbid a switch to handle the source routes of type 0, you can use the **no ipv6 source-route** command. After the running of this command, the switch will drop this kind of packets if they are received, and send an ICMPv6 unreachable packet.

Because of the limitation of **ipv6 icmp-ratelimit**, ICMPv6 error packets may not be transmitted.

Example

The following example shows how to disable the processing of soure routes of type 0.

Switch_config# no ipv6 source-route

Related command

ipv6 icmp-ratelimit

65.1.9 ipv6 traffic-filter

To filter the received or transmitted packets on an interface, run the first one of the following two commands:

ipv6 traffic-filter *access-list-name* **{ in | out }**

no ipv6 traffic-filter { in | out }

Parameter

Parameter	Description
access-list-name	Stands for the name of the ACL.
In	Filters the incoming packets.
Out	Filters the outgoing packets.

Default value

The filtration function is not set by default.

Command mode

Interface configuration mode

Instruction

Example

The following example shows how to use the ACL to filter packets when interface vlan1 receives the packets.

Switch_config_v1# ipv6 traffic-filter in

Related command

Ipv6 access-list

Show ipv6 interface

65.1.10 ipv6 unreachables

To enable an interface to generate and transmit the ICMPv6 unreachable packets, run **ipv6 unreachable**.

ipv6 unreachables

no ipv6 unreachables

Parameter

Parameter	Description

Default value

The unreachable packets are transmitted by default.

Command mode

Interface configuration mode

Instruction

The unreachable packets are transmitted through the ICMPv6 protocol. Because of the limitation of **ipv6 icmp-ratelimit**, unreachable packets may not be transmitted.

Example

The following example shows how to disable the VLAN interface to transmit the unreachable packets.

Switch_config_v1# no ipv6 unreachables

Related command

65.1.11 show ipv6 general-prefix

To display the detailed information about the general prefix of IPv6, run the following command:

show ipv6 general-prefix

Parameter

Parameter	Description

Command mode

EXEC

Example

Switch_config#show ipv6 general-prefix

IPv6 Prefix my-prefix, acquired via manual

2002::/64

Vlan1 (Address command)

Field	Remarks
IPv6 Prefix	Stands for the name of the general IPv6 prefix defined by user.
Acquire via	Stands for the configuration method of the general prefix. At present, the manual configuration and the automatic DHCP obtainment are supported.
Vlan1 (Address command)	Stands for a list of ports that use this general prefix.

Related command

ipv6 general-prefix

65.1.12 show ipv6 pmtu

To display the cache options of path MTU, run the following command:

show ipv6 pmtu

Parameter

Parameter	Description

Command mode

EXEC

Example

Switch_config#show ipv6 pmtu

PMTU Expired Destination Address

1300 00:04:00 2002:1::1

1280 00:01:00 2001:2::2

The cache of path MTU stores the path MTU which is applied to reach a destination address. If the to-be-transmitted packets generated by routers or switches are bigger than the path MTU, they will be fragmented during being transmitted.

The switch will create a path MTU record when receiving an ICMPv6 too-big packet.

Field	Remarks
MTU	Stands for the value of the path MTU. It is this MTU that is contained in the received ICMPv6 too-big packet.
Expired	It means expiration. The expiration time starts counting when the ICMPv6 “too-big” packet is received. When the **expired** parameter is 0, this path MTU record will be deleted.
Destination Address	Stands for the destination address. It is this destination address that is contained in the received ICMPv6 too-big packet.

Related command

ipv6 mtu

65.1.13 show ipv6 traffic

To display the statistics of IPv6 flow, run the following command:

show ipv6 traffic

Parameter

Parameter	Description

Command mode

EXEC

Example

```
Switch#show ipv6 traffic
IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 badhdrs, 0 badvers
         0 tooshort, 0 toosmall, 0 toomanyhdrs
         0 source-routed, 0 badscope
         0 badopts, 0 unknowopts, 0 exthdrtoolong
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  25 generated, 0 forwarded, 0 cant forwarded
         0 fragmented into 0 fragments, 0 failed
         0 no route
  Mcast: 0 received, 25 sent

ICMP statistics:
```

```
Rcvd:   25 total, 0 format errors, 0 checksum errors
        0 unreachable, 0 packet too big
        0 time exceeded, 0 parameter problem
        0 echos, 0 echo replies
        0 membership query, 0 membership report, 0 membership reduction
        0 Switch solicitations, 0 Switch advertisements
        0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
Sent:   0 total, 0 bandwidth limit
        0 unreachable, 0 packet too big
        0 time exceeded, 0 parameter problem
        0 echos, 0 echo replies
        0 membership query, 0 membership report, 0 membership reduction
        0 Switch solicitations, 0 Switch advertisements
        0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
```

Related command

clear ipv6 traffic

Chapter 66 ND Commands

Neighbor Detection (ND) commands include the following ones:

- debug ipv6 nd
- show ipv6 neighbors
- clear ipv6 neighbors
- ipv6 neighbor
- ipv6 nd dad attempts
- ipv6 nd managed-flag
- ipv6 nd ns-interval
- ipv6 nd other-flag
- ipv6 nd prefix
- ipv6 nd ra-interval-range
- ipv6 nd ra-interval
- ipv6 nd ra-lifetime
- ipv6 nd reachable-time
- ipv6 nd router-preference
- ipv6 nd suppress-ra

66.1.1 debug ipv6 nd

To enable the switch of printing ND debugging information, run the following command:

debug ipv6 nd [*entry* | *timer* | *X:X:X:X::X*]

Parameter

Parameter	Description
entry	Stands for the switch of neighbor cache entry changes.
timer	Stands for the switch of neighbor cache timer changes.
X:X:X:X::X	Stands for the IPv6 address of neighbor cache.

Default value

By default, the switch of printing ND debugging information is in disabled state.

Command mode

EXEC

Explanation

If the command carries with no extension parameters, all debugging switches are enabled.

Example

N/A

Related command

N/A

66.1.2 show ipv6 neighbors

To display the current switch's neighbor cache, run the following command:

show ipv6 neighbors [**vlan** *vlanid*]

Parameter

Parameter	Description
vlanid	Stands for the Vlan ID.

Default value

N/A

Command mode

EXEC

Explanation

N/A

Related command

N/A

66.1.3 clear ipv6 neighbors

To cancel on a switch all neighbor caches that are not configured manually, run the following command:

clear ipv6 neighbors

Parameter

Parameter	Description
N/A	

Default value

N/A

Command mode

EXEC

Explanation

This command can only cancel all those neighbor caches automatically obtained by a switch itself, not those manually configured by the **ipv6 neighbor** command.

Related command

ipv6 neighbor

66.1.4 ipv6 neighbor

To set neighbor caches of a switch, run the following command globally:

ipv6 neighbor *address6* **vlan** *vlanid mac*

Parameter

Parameter	Description
address6	Means the IPv6 address of the neighbor.
vlanid	Stands for the ID of the VLAN port.
mac	Means the link-layer address of a neighbor.

Default value

N/A

Command mode

Global configuration mode

Explanation

You can use this command to set neighbor caches of a switch. These neighbor caches never times out and are always reachable until **no ipv6 neighbor** is run.

Example

IPv6_config#ipv6 neighbor 1::1 vlan 1 00:e0::4c:5a:78:eb

The above-mentioned example shows how to set on port e1/1 a neighbor whose IPv6 address is 1::1 and whose link-layer address is 00:e0:4c:5a:78:eb.

Related command

show ipv6 neighbors

66.1.5 ipv6 nd dad attempts

To set the number of transmitted NSs when ND performs DAD on a port, run the following command:

ipv6 nd dad attempts *num*

Parameter

Parameter	Description
num	Stands for the number of NSs transmitted during DAD.

Default value

1

Command mode

Interface configuration mode

Explanation

You can use the “no” form of this command to resume the default value.

Related command

N/A

66.1.6 ipv6 nd managed-flag

To set the M flag in the RA message transmitted by the local port, run the following command.

ipv6 nd managed-flag

Parameter

Parameter	Description
N/A	

Default value

The M flag is 0 by default.

Command mode

Interface configuration mode

Explanation

This command can be used to set to 1 the M flag in the RA message transmitted by the local port, and its “no” form can be used to cancel this settings and resume its value to 0.

Related command

N/A

66.1.7 ipv6 nd ns-interval

To set the NS transmission interval of the local port and configure the **retrans-timer** field in the RA message, run the following command:

ipv6 nd ns-interval *milliseconds*

Parameter

Parameter	Description
milliseconds	Stands for the NS transmission interval, whose unit is millisecond.

Default value

The default interval of transmitting NS is 1000 ms, that is, 1 second. The **retrans-timer** field in the RA message is 0 by default, which means uncertainty.

Command mode

Interface configuration mode

Explanation

This command can be used to set the NS transmission interval of the local switch on the local port and at the same time the **retrans-timer** field in the RA message on the local port.

You can use the “no” form of this command to resume the default value.

Related command

N/A

66.1.8 ipv6 nd other-flag

To set the O flag in the RA message transmitted by the local port, run the following command.

ipv6 nd other-flag

Parameter

Parameter	Description
N/A	

Default value

The O flag in the transmitted RA message is 0 by default.

Command mode

Interface configuration mode

Explanation

This command can be used to set the O flag in the RA message, which is transmitted by the local port, to 1, and its “no” form can be used to cancel this settings and resume the default settings.

Related command

N/A

66.1.9 ipv6 nd prefix

To set the prefix of the RA message, run the first one of the following two commands:

ipv6 nd prefix {*ipv6-prefix***/***prefix-length* | **default**} [**no-advertise** | [*valid-lifetime preferred-lifetime* [**off-link** | **no-autoconfig**]] | **infinite**]

Parameter

Parameter	Description
Ipv6-prefix	Stands for the prefix of IPv6.
Prefix-length	Stands for the length of the prefix.
Valid-lifetime	Stands for the valid time.
Preferred-lifetime	Stands for the most privileged time.

Default value

The default valid-lifetime is 2592000 seconds and the default preferred-lifetime is 604800 seconds.

Command mode

Interface configuration mode

Explanation

no-advertise means that the prefix is not contained in the RA message.

off-link means that the ON-Link flag in the prefix of the RA message is 0, and **no-autoconfig** means that the AUTO-CONFIG in the prefix of the RA message is 0.

You can run **ipv6 nd prefix *ipv6-prefix/prefix-length …*** to set a prefix under this port and run the negative form of this command to remove this prefix.

You can set the default value of the prefix by using the **ipv6 nd prefix default …** command and cancel this settings by running the “no” form of this command.

Example

1. IPv6_config_v1#ipv6 nd prefix 1::/64

The prefix “1::0/64” is added on a port and the other fields will be attributed with default values. The following RA messages will all be added with this prefix.

2. IPv6_config_v1#ipv6 nd prefix 2::/64 off-link

The prefix “2::/64” is added, the ON-LINK flag is 0, and other protocols are their default values.

3. IPv6_config_v1#ipv6 nd prefix default no-autoconfig

The default value on this port is changed to NO-AUTOCONFIG, and other protocols are their default values. If the two commands are used successfully, the third command will not influence the prefix “2::/64” configured by the second command but the prefix “1::/64” configured by the first command will change to NO-AUTOCONFIG.

Related command

N/A

66.1.10 Ipv6 nd ra-interval-range

To set the maximum or minimum interval of RA transmission, run the following command:

ipv6 nd ra-interval-range *max [min]*

Parameter

Parameter	Description
max	Sets the maximum interval of RA transmission, whose unit is second.
Min	Sets the minimum interval of RA transmission, whose unit is second.

Default value

The default maximum interval is 600 seconds and the default minimum interval is only 1/3 of the default maximum interval.

Command mode

Interface configuration mode

Explanation

This command is always used to set the range of the RA transmission interval.

You can use the “no” form of this command to resume the default value.

Related command

ipv6 nd ra-interval

ipv6 nd ra-lifetime

66.1.11 ipv6 nd ra-interval

To set the interval of RA transmission on the local port, run the following command:

ipv6 nd ra-interval *seconds*

Parameter

Parameter	Description
seconds	Sets the interval of RA transmission, whose unit is second.

Default value

The interval for the local port to transmit the first three messages cannot be more than 16 seconds, while that to transmit the following messages varies between the maximum interval (600 seconds) and the minimum interval (200 seconds).

Command mode

Interface configuration mode

Explanation

This command is always used to set the range of the RA transmission interval for the local port.

As to the first three RA messages transmitted by the local port, if their transmission interval is less than 16 seconds, the time will be used as the transmission interval. Otherwise, the transmission interval for the first three messages is 16 seconds. The following RA messages' transmission interval is the just configured time.

You can use the “no” form of this command to resume the default value.

Related command

ipv6 nd ra-interval-range

66.1.12 ipv6 nd ra-lifetime

To set the router-lifetime field in the RA message transmitted by the local port, run the following command.

ipv6 nd ra-lifetime *seconds*

Parameter

Parameter	Description
seconds	Stands for the value in the router-lifetime field in the RA message, whose unit is second.

Default value

1800 seconds or triple of the maximum RA transmission interval configured by **ipv6 nd ra interval *max***

Command mode

Interface configuration mode

Explanation

You can use the “no” form of this command to resume the default value.

Related command

ipv6 nd ra-interval-range

66.1.13 ipv6 nd reachable-time

To set the reachable-time field of the RA message and the reachable time of all automatically configured neighbor caches on the local port, run the following command:

ipv6 nd reachable-time *milliseconds*

Parameter

Parameter	Description
milliseconds	Stands for the time, whose unit is second.

Default value

The reachable-time is 0 by default and the default reachable time for the neighbor cache is a value between 15 seconds and 45 seconds.

Command mode

Interface configuration mode

Explanation

You can use the “no” form of this command to resume the default value.

Related command

N/A

66.1.14 ipv6 nd router-preference

To set the value of the switch preference in the RA message, run the following command:

ipv6 nd router-preferenc *preference*

Parameter

Parameter	Description
Preference	Stands for the preference of a switch, which can be one of the three values: high, medium and low.

Default value

medium。

Command mode

Interface configuration mode

Explanation

You can use the “no” form of this command to resume the default value.

Related command

N/A

66.1.15 ipv6 nd suppress-ra

To stop a port to be the notification port of a switch, run the following command:

ipv6 nd suppress-ra

Parameter

Parameter	Description
N/A	

Default value

The port works as the notification port of the switch.

Command mode

Interface configuration mode

Explanation

You can use the “no” form of this command to resume the default value.

Related command

N/A

Chapter 67 Ripng Commands

67.1 aggregate-address

To designate the aggregation route of the RIPNG instances, run the following first one of the commands:

aggregate-address *X:X:X::X****/<0-128>***

no aggregate-address *X:X:X::X****/<0-128>***

Parameter

*X:X:X::X****/<0-128>***	Designates the prefix of IPv6 aggregation network.

Default value

There is no aggregation route.

Command mode

RIPNG configuration mode

Instruction

None

Example

The following example shows how to aggregate the sub-route of 2006:4:5::/35：

Router_config_ripng_r1#aggregate-address 2006:4:5::/35

Related command

None

67.2 debug ipv6 rip

To open the RIPNG debug switch, run the first one of the following two commands:

debug ipv6 rip [word] **[** events | send | receive |database | all **]**

no debug ipv6 rip

Parameter

word	Stands for the name of the RIPNG instance.

events

Displays the RIP event.

send	Displays the transmitted RIP packets.
receive	Displays the received RIP packets.
database	Displays the detailed change of the RIPNG route.
all	Opens all debug items.

Default value

All debug items are disabled.

Command mode

EXEC

Instruction

This command can be used to trace the main procedures of RIPNG.

Example

router# debug ipv6 rip r1 event

The example shows how to enable the debugging switch of the RIPNG event.

Related command

None

67.3 default-information

To notify the default route, run the following command:

default-information {only | originate} [metric_value]

no default-information {only | originate} [metric_value]

Parameter

metric_value	It is an optional parameter, which is used to specify the default metric value of the default route.

Default value

There is no default route and the default metric value is 1.

Command mode

RIPNG configuration mode

Instruction

No matter whether a default route exists in the main routing table, another default route will be generated in the RIPNG routing table; and if the following parameters exist, you have to know their meaning respectively:

only: only the default route is notified.

originate: both the current route and the default route are notified.

Example

The following example shows how to generate the default route and how to notify only the default route:

Router_config_ripng_r1# default-information only

Related command

None

67.4 default-metric

To designate the default metric of the forward-route, run the first one of the following commands:

default-metric value

no default-metric

Parameter

value

It is used to specify the default metric value of the forward-route, which ranges between 1 and 15. .

Default value

The default metric of the forward-route is 1.

Command mode

RIPNG configuration mode

Instruction

The metric ranges between 1 and 15 and it is used to specify the default metric when RIPNG forwards other protocols and RIPNG instances.

Example

Router_config_ripng_r1#default-metric 3

The above-mentioned example shows how to set the metric of route forwarding to 3.

Related command

redistribute

67.5 connect-metric

To specify the default metric of the directly-connected route, run the first one of the following commands:

connect-metric value

no connect-metric

Parameter

value

It is used to specify the default metric value of the directly-connected route, which ranges between 1 and 15. .

Default value

The default metric the directly-connected route is 1.

Command mode

RIPNG configuration mode

Instruction

The metric ranges between 1 and 15 and is used to specify the default metric of the RIPNG directly-connected route.

Example

Router_config_ripng_r1#connect-metric 3

The above-mentioned example shows how to set the metric of the directly-connected route to 3.

Related command

redistribute

67.6 distance

To set the management distance, run the first one of the following two commands:

distance *weight* [*X:X:X:X::X/*<0-128> [Acc-list_name]

no distance *weight* [*X:X:X:X::X/*<0-128> [Acc-list_name]

Parameter

Parameter	Remarks
Weight	Stands for the management distance, ranging between 1 and 255. It is recommended to set it to a value between 10 and 255. If the parameter is used alone, the router will take it as the default management distance if the router does not have relative regulations about a routing information. When the management distance of a route is 255, this route will not be added to the routing table.
X:X:X:X/<0-128>	This parameter is optional. It stands for the prefix of the source IPv6.
Acc-list_name	This parameter is optional. It stands for the IP access control list.

Default value

The default RIPNG management distance is 120.

Command mode

RIPNG configuration mode

Instruction

The management distance is an integer from 0 to 255. In general, the bigger the value is, the more incredible the value is. If the optional parameter, **access-list-name**, is used in the command, the access control list is applied when a one-hop route is added to the routing table. In this way, you can filter the paths of some network according to the address of the router provided by the routing information.

Example

The following example shows that the distance of the route received from network **af::/64** is set to 100.

```
router ripng r1

distance 100 af::/64
```

Related command

None

67.7 filter

To set the filtration for RIPNG route reception and transmission, run the first one of the following two commands.

filter *interface-type interface-number* **{in | out}** access-list | gateway | prefix-list

no filter *interface-type interface-number* **{in | out}** access-list | gateway | prefix-list

Parameter

Parameter	Remarks
interface-type	Designates the interface type.
interface-number	Designates the port ID.
in	Filters the input RIPng routes.
out	Filters the output RIPng routes.
access-list	Uses the ACL to filter routes.
gateway	Uses the ACL to filter gateways.
prefix-list	Uses the prefix list to filter routes.

Default value

None

Command mode

RIPNG configuration mode

Instruction

This command is used to filter those received and to-be-transmitted RIPng routes.

Example

The following example shows how the routes, received by the RI instance from interface e1/1, are filtered by ACL and added to the routing table if they meet the already configured condition or deleted if they do not meet the above-mentioned condition.

Router_config_ripng_r1#filter e1/1 in acc acc-name

Related command

None

67.8 ipv6 rip enable

To enable a RIPng instance on a port, run the first one of the following two commands:

ipv6 rip *word* **enable**

no ipv6 rip *word* **enable**

Parameter

word

It stands for the name of the routing process instance.

Default value

None

Command mode

Port configuration mode

Instruction

This command is used to enable a RIPng instance on a port. If no RIPng instance exists and the number of the current instances is less than the maximum, a new instance will be generated and then be enabled.

Example

Router_config# int e2/1

Router_config_e2/1# ipv6 rip r1 enable

Related command

Show ipv6 rip

67.9 ipv6 rip passive

To set the passive port and cancel route update on a port, run the first one of the following two commands:

ipv6 rip passive

no ipv6 rip passive

Parameter

None

Default value

None

Command mode

Port configuration mode

Instruction

If a port is set to be a passive one, the transmission of update packets will be canceled on this port and the update packets will continually be transmitted out from other ports.

Example

The following example shows how to set port e2/1 to be the passive port to receive updated routes but not to transmit them.

R142_config_e2/1# ipv6 rip passive

Related command

None

67.10 ipv6 rip poision-reverse

To apply poison reverse on a port, run the first one of the following two commands:

ipv6 rip poision-reverse

no ipv6 rip poision-reverse

Parameter

word

It stands for the name of the routing process instance.

poision-reverse

It means to enable poison reverse on a port.

Default value

The poison reverse is disabled by default.

Command mode

Port configuration mode

Instruction

This command is used to enable the **word** RIPng instance to enable poison reverse on this port.

Example

The following example shows that the R1 RIPng instance enables poison reverse on port e2/1:

R142_config_e2/1# ipv6 rip poision-reverse

Related command

None

67.11 ipv6 rip split-horizon

To apply horizontal split on a port, run the first one of the following two commands:

ipv6 rip split-horizon

no ipv6 rip split-horizon

Parameter

word	Standing for the name of the routing process instance
split-horizon	Meaning to apply horizontal split on a port

Default value

The horizontal split is enabled by default.

Command mode

Port configuration mode

Instruction

In the default settings, all instances enable the horizontal split.

Example

The following example shows that the R1 RIPng instance enables the horizontal split on port e2/1:

R142_config_e2/1# ipv6 rip split-horizon

Related command

None

67.12 router ripng

To set a RIPng instance globally, run the first one of the following two commands:

router ripng *word*

no router ripng *word*

Parameter

Word	Standing for the name of the RIPng instance

Default value

None

Command mode

Global configuration mode

Instruction

In the default settings, up to 4 RIPng instances can be generated.

After the configuration command is entered, the router prompt changes to **Router_config_ripng_r1#**.

Example

Router_config#router ripng r1

Router_config_ripng_r1#

Related command

ipv6 rip word enable

67.13 max-path

To set the number of equivalent routes allowed by the RIPng instance, run the first one of the following two commands:

max-path *value*

no max-path

Parameter

Value

Setting the number of equivalent routes allowed by the RIPng instance

Default Value

4

Command mode

RIPNG configuration mode

Instruction

This command is used to set the maximum of equivalent routes in a RIPng instance and the maximum of equivalent routes is 6.

Example

The following example shows how to set the maximum of equivalent routes in the R1 RIPng instance to 5.

Router_config_ripng_r1#max-path 5

Related command

None

67.14 neighbor

To specify a neighbor and transmit updates to this specified neighbor, run the first one of the following two commands:

neighbor *ipv6-addr interface interface-number*

no neighbor *ipv6-addr interface interface-number*

Parameter

ipv6-addr	Standing for the IPv6 address
interface	Designating an interface
interface-number	Standing for a port ID

Default value

None

Command mode

RIPNG configuration mode

Instruction

You can use this command to specify an address to be the neighbor of a specific interface and then the routing information transmitted from this port will be sent in the unicast form to the neighbor.

Example

The following example shows how to set neighbor **fe::2** on port f0/0.

Router_config# router ripng r1

Router_config_ripng_r1#neighbor fe::2 f0/0

Related command

None

67.15 offset

To set the in/out metric of a RIPng instance on a port, run the first one of the following two commands:

offset *interface-type interface-number* **{in | out}** acl-name *value*

no offset *interface-type interface-number* **{in | out}**

Parameter

Parameter	Remarks
interface-type	Designates the interface type.
interface-number	Designates the port ID.
in	Adds the metric for an incoming RIPng route.
out	Adds the metric for an outgoing RIPng route.
acl-name	**Stands for the IP access control list.**
value	**Adds the specified metric for the received RIPng route.**

Default value

The default value of the **in** parameter is 1.

The default value of the **out** parameter is 0.

Command mode

RIPNG configuration mode

Instruction

This command is used to specify the metric for those received and to-be-transmitted RIPng routes.

Example

The following example shows that the routes received by the R1 instance from port e1/1 are added with a metric, 8, after ACL filtration and then added to the routing table.

Router_config_ripng_r1#offset e1/1 in acc 8

Related command

None

67.16 port

To set a specific UDP port for the RIPng instance, run the following command:

port *port-number*

Parameter

port-number

Standing for the UDP port ID, which is a value between 521 and 65535

Default value

521

Command mode

RIPNG configuration mode

Instruction

You can use this command to specify the UDP port of the Ripng instance. The default value of the UDP port ID is 521.When two instances are enabled on a same port, the UDP port cannot be the same.

Example

The following example shows how to set the ID of the UDP port of the R1 instance to 555:

Router_config# router ripng r1

Router_config_rip_r1# port 555

Related command

None

67.17 redistribute

To enable other routing domains to forward routes to RIPng, run the first one of the following two commands:

redistribute protocol [*protocol-id* | *instance name]* [**route-map** *map-name*]

no redistribute protocol [*protocol-id* | *instance name]* [**route-map** map-name]

Parameter

Protocol	Standing for the type of the forwarded protocol
protocol-id	Standing for the ID of the forwarded process
instance name	Standing for the name of the forwarded RIPng instance

Default value

disable

Command mode

RIPNG configuration mode

Instruction

This command is used to forward the routes from other routing domains and other RIPng instances. The metric of a forwarded route is set by the **default-metric** command and its default value is 1.

Example

The following example shows how to forward the BGP route whose AS ID is 4.

Router_config_ripng_r1#redis bgp 4 route-map rm

Related command

None

67.18 show ipv6 rip

To display the RIPng related information, run the following command:

show ipv6 rip [name] [**database** | **summary | interface**]

Parameter

Name	Standing for the name of the RIPng instance
Database	Displaying the detailed information about the routes of a designated RIPng instance
summary	Displaying the detailed statistics information about the routes of a designated RIPng instance
interface	Displaying where the RIPng instance is enabled

Default value

None

Command mode

Any non-user mode

Instruction

None

Example

The following example shows on which port the R1 instance is enabled:

router#sho ipv6 rip r1 interface

ripng instance r1/1 enable on: FastEthernet0/0 , FastEthernet0/1

Related command

None

67.19 timers

To adjust the timeout value in each clocks in RIPng, run the first one of the following two commands:

timers *update/holddown/garbage value*

no timers *update/holddown/garbage*

Parameter

Update	Standing for the interval of regular updates
Holddown	Standing for the timeout time of the invalid timer
Garbage	Standing for the waiting time of route deletion

Default value

Update	30s
Holddown	180s
Garbage	120s

Command mode

RIPNG configuration mode

Instruction

Do not adjust the value of each timer randomly. If necessary to do so, you have to note the relationships between 3 timers.

Example

None

Related command

None

Chapter 68 OSPFv3 Configuration Commands

68.1 OSPFv3 Configuration Commands

The OSPFv3 configuration commands include:

- area default-cost
- area nssa
- area range
- area stub
- area virtual-link
- debug ipv6 ospf
- debug ipv6 ospf events
- debug ipv6 ospf ifsm
- debug ipv6 ospf lsa
- debug ipv6 ospf nfsm
- debug ipv6 ospf nsm
- debug ipv6 ospf packet
- debug ipv6 ospf route
- default-information originate
- default-metric
- filter
- ipv6 ospf area
- ipv6 ospf cost
- ipv6 ospf database-filter all out
- ipv6 ospf dead-interval
- ipv6 ospf hello-interval
- ipv6 ospf mtu-ignore
- ipv6 ospf neighbor

- ipv6 ospf network
- ipv6 ospf priority
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay
- passive-interface
- redistribute
- router ospfv3
- router-id
- show ipv6 ospf
- show ipv6 ospf database
- show ipv6 ospf interface
- show ipv6 ospf neighbor
- show ipv6 ospf route
- show ipv6 ospf virtual-link
- summary-prefix
- timers delay
- timers hold

68.1.1 **area** default-cost

To specify the cost of the default summary route in the NSSA or STUB area, run the first one of the following two commands:

area *area-id* **default-cost** ***cost***

no area *area-id* **default-cost**

Parameter

Parameter	Description
area-id	Means the ID of the NSSA or STUB area.
cost	Means the cost of the default summary route.

Default value

The default value is 1.

Command mode

Routing configuration mode

Instruction

The command is helpful only when it is used on the boundary router connecting the NASSA area or the STUB area.

After the **area stub default-information-originate** command is configured, the cost configured by this command will be used in LSA to set the corresponding cost.

Example

The following example shows how to set the default cost of stub domain 36.0.0.0 to 20:

```
interface vlan 1
    ipv6 enable
    ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
    router-id 2.2.2.2
    area 36.0.0.0 stub
    area 36.0.0.0 default-cost 20
```

Related command

area nssa

area stub

68.1.2 **area** nssa

To configure a NSSA area, run the first one of the following two commands**:**

area *area-id* **nssa** [**default-information-originate** [**metric** *value*] [**metric-type** {1 | 2}]] [**interval** *value*] [**no-redistribute**] [**no-summary**] [**range** {*ipv6-prefix/prefix-length*} [advertise | not-advertise]] [**translator** {always|candidate}]

no area *area-id* **nssa** [**default-information-originate** [**metric** *value*] [**metric-type** {1 | 2}]] [**interval** *value*] [**no-redistribute**] [**no-summary**] [**range** {*ipv6-prefix/prefix-length*} [advertise | not-advertise]] [**translator** {always|candidate}]

Parameter

Parameter	Description
area-id	Sets the ID of the NSSA area. It can be a decimal number or an IP address.

default-informatio n-originate	Means to send the default route to the NSSA area.
metric *value*	Stands for the cost of the default route, which ranges from 1 to 16777214.
metric-type {1 | 2}	Means the cost type of the default route.
interval *value*	Means the stable time of the NSSA translator role, which ranges from 1 to 65535.
no-redistribute	Means not to redistribute a route to the NSSA area.
no-summary	Forbids the ABR router to send the summary link to the NSSA area.
range	Means to conduct summary when type-7 LSA is translated into type-5 LSA.
translator	Stands for the NSSA translator role; if the parameter “always” is used, it means it is always the translator, and if it is the parameter “candidate”, it means it can be chosen as a translator.

Default value

Non-NSSA area

Command mode

Routing configuration mode

Instruction

All routers and access servers in the NSSA area will be configured by the **area nssa** command.

To decrease the number of LSA’s, you can run **no summary** on the ABR router to forbid the summary LSA to enter the NSSA area.

The parameter “no-distribute” is always used for ABR and its purpose is to stop redistributed routes from being sent to the NSSA area.

Example

The following example shows how to set the NSSA area of 36.0.0.0:

```
interface vlan 1
    ipv6 enable
    ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
    router-id 2.2.2.2
    area 36.0.0.0 nssa
!
```

Related command

area stub

68.1.3 **area** range

To summarize the routes at the field boundary, run **area *area-id* range {*ipv6-prefix /prefix-length*} [advertise | not-advertise]**. To cancel the previous settings, run **no area range**.

area *area-id* **range {***ipv6-prefix /prefix-length***} [advertise | not-advertise]**

no area *area-id* **range {***ipv6-prefix /prefix-length***} [advertise | not-advertise]**

Parameter

Parameter	Description
area-id	Means the fields where the fields will be summarized. It can be a decimal number or an IPv6 address.
ipv6-prefix	Means the prefix of the IPv6 address.
prefix-length	Means the length of the IPv6 address' prefix.
advertise	Means that the routes are released after they are summarized.
not-advertise	Means that the routes are not released after they are summarized.

Default value

The command has no effect by default.

Command mode

Routing configuration mode

Instruction

The **area range** command is not run on the ABR router, enabling ABR to be broadcast to other routers through a summary route. In this way, the route of the field boundary is miniatured. As to the outside of the area, each address range has only one summary route.

The command can be configured on the routers in multiple areas, and OSPF, hence, can summarize many address ranges.

Example

The following example shows how to set the prefix of the summarized IPv6 address in area 1, 2001:0DB8:0:1::/64:

```
interface vlan 1
    no ip address
    ipv6 enable
    ipv6 ospf 1 area 1
!
router ospfv3 1
    router-id 192.168.255.5
    log-adjacency-changes
    area 1 range 2001:0DB8:0:1::/64
```

68.1.4 **area** stub

To configure a STUB area, run the first one of the following two commands. To cancel the configuration, run the other command.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter

Parameter	Description
area-id	Sets the ID of the STUB area. It can be a decimal number or an IP address.
no-summary	Forbids the ABR router to send the summary link to the STUB area.

Default value

Non-stub area

Command mode

Routing configuration mode

Instruction

All routers and access servers in the STUB area will be configured by the **area stub** command. The ABR router adopts the **default-cost** option to set the cost from the internal router to the STUB area.

To decrease the number of LSA's, you can run **no summary** on the ABR router to forbid the summary LSA to enter the STUB area.

Example

The following example shows how to set the STUB area of 36.0.0.0:

```
interface vlan 1
```

```
    ipv6 enable
    ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
    router-id 2.2.2.2
    area 36.0.0.0 stub
!
```

Related command

area nssa

68.1.5 area virtual-link

To configure a virtual link, run the first one of the following two commands.

area *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transmit-delay** *dly-value*]

no area *area-id* **virtual-link** *neighbor-ID*

Parameter

Parameter	Description
area-id	Specifies the transit-area of the virtual link.
neighbor-id	OSPF router ID of the peer router of virtual link
dead-value	Stands for the interval for the local router to regard that the neighbor dies, whose unit is second. The values configured at the two terminals of the virtual link must be same.
hello-value	Stands for the interval for the router to transmit the HELLO packet on the virtual link, whose unit is second. The values configured at the two terminals of the virtual link must be same.
retrans-value	Interval for the router to transmit the **re-transmit** packet on the virtual link, whose unit is second The values configured at the two terminals of the virtual link must be same.
dly-value	Delay value which is reported by the router to LSA on the virtual link, whose unit is second The values configured at the two terminals of the virtual link must be same. The values configured at the two terminals of the virtual link must be same.

Default value

The virtual link is not configured.

The default values of other parameters are shown in the following:

Hello-value: 10s, Dead-value : 40s, Retrans-value : 5s, dly-value : 1s

Command mode

Routing configuration mode

Instruction

In order to create a virtual link, you have to perform configuration at the two terminals of the virtual link. If only one terminal need be configured, the virtual link cannot function.

The **area-id** parameter cannot be zero because the transit area of the virtual link must not be the backbone area. The area-id configured at the two terminals of the virtual link must be same.

Parameters configured at the two terminals of the virtual link must be same.

After the virtual link is created (the neighborhood is in the FULL state), the virtual link works in the Demand Circuit mode, that is, the periodical Hello packet and the LSA refresh packet are not transmitted.

You can run no **area *area-id* virtual-link *neighbor-ID*** to cancel the previous configuration of the virtual link.

You also can run **show ip ospf virtual-link** to check the state of the virtual link.

Example

The following example shows how to create a virtual link between router A and router B.

Configuration on router A (router-id: 200.200.200.1) :

```
!
interface vlan 1
    no ip address
    ipv6 enable
    ipv6 ospf 1 area 1
!
router ospfv3 1
    router-id 200.200.200.1
    area 1 virtual-link 200.200.200.2
!
```

Configuration on router B (router-id: 200.200.200.2) :

```
!
interface vlan 1
    no ip address
    ipv6 enable
    ipv6 ospf 1 area 1
```

```
!
router ospfv3 1
    router-id 200.200.200.2
    area 1 virtual-link 200.200.200.1
!
```

Related command

show ipv6 ospf virtual-link

68.1.6 **debug** ipv6 ospf

To open all debugging switches of the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf

no debug ipv6 ospf

Parameter

None

Default value

None

Command mode

EXEC

Instruction

This command can be used to collect all debugging information about the OSPFv3 for the R&D engineers and technical support staff.

Example

```
Router# debug ipv6 ospf
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Intra-Area-Prefix-LSA(0x38110c0) originated
VLINK[VLINK1]: local address is 101::1VLINK[VLINK1]: peer 200.200.200.2 link upLSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Install Link-LSA to Link FastEthernet0/0
```

LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Link-LSA(0x381ec40) originated

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x381ec20) originated

IFSM[FastEthernet0/0]: Down (InterfaceUp)

IFSM[FastEthernet0/0]: Status change Down -> Waiting

SPF[0.0.0.0]: Calculation timer scheduled [delay 5 secs]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[VLINK1]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x38297e0) originated

IFSM[VLINK1]: Down (InterfaceUp)

IFSM[VLINK1]: Status change Down -> Point-To-Point

ROUTER[1]: Change status to ABR

IFSM[FastEthernet0/0]: Hello timer expire

Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5)

OSPFv3 Header

Version 3 Type 1 (Hello) Packet length 36

Router ID 200.200.200.1

Area ID 0.0.0.1

Checksum 0x0000 Instance ID 0

OSPFv3 Hello

Interface ID 4

RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)

HelloInterval 10 RtrDeadInterval 40

DRouter 0.0.0.0 BDRouter 0.0.0.0

Neighbors 0

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

……

68.1.7 **debug** ipv6 ospf events

To enable the event debug switch of the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf events {abr|asbr|vlink|os|router}

no debug ipv6 ospf events { abr|asbr|vlink|os|router }

Parameter

Parameter	Description
abr	Opens the state change debug switch of ABR.
asbr	Opens the state change debug switch of ASBR.
vlink	Opens the state change debug switch of the virtual link.
os	Opens the state change debug switch of socket.
router	Opens the debug switch of OSPF.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can check the OSPF port and the neighbor trigger event.

Example

Router# **debug** ip ospf events
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
ROUTER[1]: Change status to ABR
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
VLINK[VLINK1]: peer 200.200.200.2 link downROUTER[1]: Change status to non-ABR
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
ROUTER[Process:1]: GC timer expire
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
ROUTER[Process:1]: GC timer expire
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
join AllDRouters on FastEthernet0/0OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
……

68.1.8 **debug** ipv6 ospf ifsm

To enable the state machine's debug switch of the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf ifsm {status|events|timers}

no debug ipv6 ospf ifsm {status|events|timers}

Parameter

Parameter	Description
status	Opens the state debug switch of the interface state machine.
events	Opens the event debug switch of the interface state machine.
timers	Opens the timer debug switch of the interface state machine.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can check the whole process of the state machine of the OSPF interface.

Example

```
Router# debug ipv6 ospf ifsm
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point
IFSM[FastEthernet0/0]: Down (InterfaceUp)
IFSM[FastEthernet0/0]: Status change Down -> Waiting
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[VLINK1]: Hello timer expire
IFSM[VLINK1]: ifsm_ignore called
IFSM[VLINK1]: Point-To-Point (NeighborChange)
IFSM[FastEthernet0/0]: ifsm_ignore called
IFSM[FastEthernet0/0]: Waiting (NeighborChange)
IFSM[VLINK1]: LS ack timer expire
IFSM[VLINK1]: LS ack timer expire
IFSM[VLINK1]: Point-To-Point (InterfaceDown)
IFSM[VLINK1]: Status change Point-To-Point -> Down
IFSM[VLINK1]: ifsm_ignore called
IFSM[VLINK1]: Down (NeighborChange)
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: Wait timer expire
IFSM[FastEthernet0/0]: DR-Election[1st]: Backup 200.200.200.2
IFSM[FastEthernet0/0]: DR-Election[1st]: DR         200.200.200.2
IFSM[FastEthernet0/0]: Waiting (WaitTimer)
IFSM[FastEthernet0/0]: Status change Waiting -> DROther
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point
IFSM[FastEthernet0/0]: DR-Election[1st]: Backup 200.200.200.1
IFSM[FastEthernet0/0]: DR-Election[1st]: DR         200.200.200.2
IFSM[FastEthernet0/0]: DR-Election[2nd]: Backup 200.200.200.1
IFSM[FastEthernet0/0]: DR-Election[2nd]: DR         200.200.200.2
```

IFSM[FastEthernet0/0]: DROther (NeighborChange)
IFSM[FastEthernet0/0]: Status change DROther -> Backup
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: LS ack timer expire
IFSM[VLINK1]: Hello timer expire
IFSM[FastEthernet0/0]: LS ack timer expire
IFSM[VLINK1]: Point-To-Point (InterfaceDown)
IFSM[VLINK1]: Status change Point-To-Point -> Down
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point
IFSM[FastEthernet0/0]: LS ack timer expire
IFSM[VLINK1]: Hello timer expire
……

68.1.9 **debug** ipv6 ospf lsa

To enable the LSA-related debug switch of the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf lsa { flooding|install|maxage|refresh}

no debug ipv6 ospf lsa { flooding|install|maxage|refresh}

Parameter

Parameter	Description
flooding	Opens the debug switch of LSA exchange.
install	Opens the debug switch of LSA installation.
maxage	Opens the debug switch of LSA timeout.
refresh	Opens the debug switch of LSA-Refresh.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can browse the operation that OSPF performs to LSA and related events.

Example

```
router# debug ipv6 ospf lsa
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Intra-Area-Prefix-LSA(0x3824ba0) originated
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding to neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x3819be0) originated
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Install Link-LSA to Link FastEthernet0/0
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Link-LSA(0x3819bc0) originated
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x3824740) originated
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: instance(0x380bf60) created with Link State Update
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: instance(0x38246c0) created with Link State Update
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: flood started
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: consider flooding through interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: consider flooding to neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: neighbor is not Full state
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: flood started
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: consider flooding through interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: consider flooding to neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: neighbor is not Full state
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: Install Inter-Area-Prefix-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding to neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: added to neighbor[200.200.200.2]'s retransmit-list
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: sending update to interface[VLINK1]
```

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA refreshed
OSPFv3 LSA Header
LS age 0
LS type 0x2001 (Router-LSA)
Advertising Router 200.200.200.1
Link State ID 0.0.0.0
LS sequence number 0x80000002
LS checksum 0x5ff7
length 40
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[VLINK1]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA refreshed
OSPFv3 LSA Header
LS age 0
LS type 0x2001 (Router-LSA)
Advertising Router 200.200.200.1
Link State ID 0.0.0.0
LS sequence number 0x80000002
LS checksum 0x5382
length 24
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Intra-Area-Prefix-LSA refreshed
OSPFv3 LSA Header
LS age 0
LS type 0x2009 (Intra-Area-Prefix-LSA)
Advertising Router 200.200.200.1
Link State ID 0.0.0.1
LS sequence number 0x80000002
LS checksum 0x3631
length 64
……

68.1.10 **debug** ipv6 ospf nfsm

To enable the state machine's debug switch of the OSPFv3 neighbor, run the first one of the following two commands:

debug ipv6 ospf nfsm {status|events|timers}

no debug ipv6 ospf nfsm {status|events|timers}

Parameter

Parameter	Description
status	Opens the state debug switch of the neighbor state machine.
events	Opens the event debug switch of the neighbor state machine.
timers	Opens the timer debug switch of the neighbor state machine.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can check the whole process of the OSPF neighbor's state machine.

Example

router# debug ipv6 ospf nfsm
NFSM[200.200.200.2-00000004]: Full (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore calledNFSM[200.200.200.2-00000004]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: Down (HelloReceived)
NFSM[200.200.200.2-00000004]: Status change Down -> Init
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Init (1-WayReceived)
NFSM[200.200.200.2-00000004]: Init (HelloReceived)
NFSM[200.200.200.2-00000004]: Init (2-WayReceived)
NFSM[200.200.200.2-00000004]: Status change Init -> 2-Way
NFSM[200.200.200.2-00000004]: 2-Way (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: 2-Way (2-WayReceived)
NFSM[200.200.200.2-00000004]: 2-Way (AdjOK?)
NFSM[200.200.200.2-00000004]: Status change 2-Way -> ExStar
tNFSM[200.200.200.2-00000004]: ExStart (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: ExStart (2-WayReceived)
NFSM[200.200.200.2-00000004]: DD Retransmit timer expire
NFSM[200.200.200.2-00000004]: ExStart (NegotiationDone)
NFSM[200.200.200.2-00000004]: Status change ExStart -> Exchange
NFSM[200.200.200.2-00000004]: Exchange (ExchangeDone)
NFSM[200.200.200.2-00000004]: Status change Exchange -> Loading

NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Loading (LoadingDone)
NFSM[200.200.200.2-00000004]: Status change Loading -> Full
NFSM[200.200.200.2-80000001]: Down (HelloReceived)
NFSM[200.200.200.2-80000001]: Status change Down -> Init
NFSM[200.200.200.2-80000001]: Init (2-WayReceived)
NFSM[200.200.200.2-80000001]: Status change Init -> ExStart
NFSM[200.200.200.2-80000001]: ExStart (NegotiationDone)
NFSM[200.200.200.2-80000001]: Status change ExStart -> Exchange
NFSM[200.200.200.2-80000001]: Exchange (ExchangeDone)
NFSM[200.200.200.2-80000001]: Status change Exchange -> Loading
NFSM[200.200.200.2-80000001]: nfsm_ignore called
NFSM[200.200.200.2-80000001]: Loading (LoadingDone)
NFSM[200.200.200.2-80000001]: Status change Loading -> Full
NFSM[200.200.200.2-00000004]: Full (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: Full (AdjOK?)
NFSM[200.200.200.2-00000004]: LS update timer expire
NFSM[200.200.200.2-80000001]: LS update timer expire
NFSM[200.200.200.2-00000004]: LS update timer expire
NFSM[200.200.200.2-80000001]: LS update timer expire
NFSM[200.200.200.2-80000001]: Full (HelloReceived)
NFSM[200.200.200.2-80000001]: nfsm_ignore called
NFSM[200.200.200.2-80000001]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: Full (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: LS update timer expire
NFSM[200.200.200.2-80000001]: LS update timer expire
……

68.1.11 **debug** ipv6 ospf nsm

To open the debug switch of information transmission between the IPv6 routing table's management module and the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf nsm { redistribute | interface }

no debug ipv6 ospf nsm { redistribute | interface }

Parameter

Parameter	Description
redistribute	Opens the debug switch of routing information forwarding.
interface	Opens the debug switch of interface events.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by this command, you can browse information exchange between OSPF and routing management module.

Example

```
router# debug ipv6 ospf nsm
Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
Sep 17 16:43:53 OSPFv3: Receive [NSM_MSG_GLBL_ENAIPV6] message
……
```

68.1.12 **debug** ipv6 ospf packet

To enable the debug switch of OSPFv3 transmission and reception, run the first one of the following two commands:

debug ipv6 ospf packet { hello|dd|ls-request|ls-update|ls-ack }

no debug ipv6 ospf packet { hello|dd|ls-request|ls-update|ls-ack }

Parameter

Parameter	Description
hello	Opens the debug switch of Hello packets.
dd	Opens the debug switch of DD packets.
ls-request	Opens the debug switch of IS-REQUEST packets.
ls-update	Opens the debug switch of IS-Update packets.
ls-ack	Opens the debug switch of IS-Ack packets.
detail	Observes the details of packets.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can check the exchange of the OSPF packets.

Example

```
router# debug ipv6 ospf packet
Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5)
OSPFv3 Header
  Version 3   Type 1 (Hello)   Packet length 40
  Router ID 200.200.200.1
  Area ID 0.0.0.1
  Checksum 0x0000   Instance ID 0
OSPFv3 Hello
  Interface ID 4
  RtrPriority 1   Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10   RtrDeadInterval 40
  DRouter 200.200.200.2   BDRouter 200.200.200.1
  # Neighbors 1
    Neighbor 200.200.200.2
Packet[RECV]: src(101::2) -> dst(101::1)
OSPFv3 Header
  Version 3   Type 1 (Hello)   Packet length 40
  Router ID 200.200.200.2
  Area ID 0.0.0.0
  Checksum 0x5774   Instance ID 0
OSPFv3 Hello
  Interface ID 2147483649
  RtrPriority 1   Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10   RtrDeadInterval 40
  DRouter 0.0.0.0   BDRouter 0.0.0.0
  # Neighbors 1
    Neighbor 200.200.200.1
RECV[Hello]: Neighbor(200.200.200.2) declare 0.0.0.0 as DR, 0.0.0.0 as Backup
Packet[SEND]: src(101::1) -> dst(101::2)
OSPFv3 Header
  Version 3   Type 1 (Hello)   Packet length 40
```

```
  Router ID 200.200.200.1
  Area ID 0.0.0.0
  Checksum 0x0000   Instance ID 0
OSPFv3 Hello
  Interface ID 2147483649
  RtrPriority 1   Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10   RtrDeadInterval 40
  DRouter 0.0.0.0   BDRouter 0.0.0.0
  # Neighbors 1
    Neighbor 200.200.200.2
Packet[RECV]: src(fe80::2e0:fff:fe26:a8) -> dst(ff02::5)
OSPFv3 Header
  Version 3   Type 1 (Hello)   Packet length 40
  Router ID 200.200.200.2
  Area ID 0.0.0.1
  Checksum 0xa8a8   Instance ID 0
OSPFv3 Hello
  Interface ID 4
  RtrPriority 1   Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10   RtrDeadInterval 40
  DRouter 200.200.200.2   BDRouter 200.200.200.1
  # Neighbors 1
    Neighbor 200.200.200.1
RECV[Hello]: Neighbor(200.200.200.2) declare 200.200.200.2 as DR, 200.200.200.1 as Backup
Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5)
OSPFv3 Header
  Version 3   Type 1 (Hello)   Packet length 40
  Router ID 200.200.200.1
  Area ID 0.0.0.1
  Checksum 0x0000   Instance ID 0
OSPFv3 Hello
  Interface ID 4
  RtrPriority 1   Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10   RtrDeadInterval 40
  DRouter 200.200.200.2   BDRouter 200.200.200.1
  # Neighbors 1
    Neighbor 200.200.200.2
    ……
```

68.1.13 **debug** ipv6 ospf route

To enable the debug switch of OSPFv3 routing information, run the first one of the following two commands:

debug ipv6 ospf route { ase|install|spf|ia }

no debug ipv6 ospf route { ase|install|spf|ia }

Parameter

Parameter	Description
ase	Opens the debug switch of exterior routing calculation.
install	Opens the debug switch of routing installation procedure.
spf	Opens the debug switch of SPF calculation.
ia	Opens the debug switch of between-domain routing calculation.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can browse the calculation, deletion and addition of OSPF routes.

Example

router# debug ipv6 ospf route

Route[IA:0.0.0.0]: No SPF tree, schedule SPF calculationSPF[0.0.0.1]: SPF calculation timer expire

SPF[0.0.0.1]: SPF calculation (1st STAGE)

SPF[0.0.0.1]: Vertex[200.200.200.1-0.0.0.0]

SPF[0.0.0.1]: SPF calculation (2nd STAGE)

SPF[0.0.0.1]: SPF calculation (END)

Route[IA:0.0.0.1]: Cleanup IA route because of no ABRsRoute[IA:0.0.0.1]: Cleanup IA route because of no ABRsSPF[0.0.0.1]: Calculation completed [0.170000 sec]

SPF[0.0.0.1]: Calculation timer scheduled [delay 9 secs]

SPF[0.0.0.1]: SPF calculation timer expire

SPF[0.0.0.1]: SPF calculation (1st STAGE)

SPF[0.0.0.1]: Vertex[200.200.200.1-0.0.0.0]

SPF[0.0.0.1]: SPF calculation (2nd STAGE)

SPF[0.0.0.1]: SPF calculation (END)

Route[IA:0.0.0.1]: Cleanup IA route because of no ABRsSPF[0.0.0.1]: Calculation completed [0.180000 sec]

SPF[0.0.0.1]: Calculation timer scheduled [delay 10 secs]

SPF[0.0.0.0]: Calculation timer scheduled [delay 5 secs]

Route[IA:0.0.0.1]: 888::/64 calculating Network routeRoute[IA:0.0.0.1]: 888::/64 Can't find route to ABR (200.200.200.2)Route[IA:0.0.0.0]: No SPF tree, schedule SPF calculationSPF[0.0.0.0]: SPF calculation timer expire

SPF[0.0.0.0]: SPF calculation (1st STAGE)

SPF[0.0.0.0]: Vertex[200.200.200.1-0.0.0.0]

SPF[0.0.0.0]: Link[0] (200.200.200.2-128.0.0.1): Virtual-Link

SPF[0.0.0.0]: Calculate nexthop for (200.200.200.2-0.0.0.0)

Route[0.0.0.0:SPF]: ADD Stub Route for (200.200.200.2)SPF[0.0.0.0]: Vertex[200.200.200.2-0.0.0.0]

SPF[0.0.0.0]: Link[0] (200.200.200.1-128.0.0.1): Virtual-Link

SPF[0.0.0.0]: LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *] is already in SPF tree

SPF[0.0.0.0]: SPF calculation (2nd STAGE)

SPF[0.0.0.0]: SPF calculation (END)

SPF[0.0.0.0]: Calculation completed [0.580000 sec]

……

68.1.14 **default-information** originate

To introduce the default route to the OSPFv3 routing domain, run the following command:

default-information originate [always | metric *value* **| metric-type** {1 | 2} **| tag** *tag***]**
no default-information originate

Parameter

Parameter	Description
Always	Generates and releases an ASE-LSA, which describes the default route, or just releases it out if the default route exists in the routing table.
metric *value*	Stands for the cost of the default route, which ranges from 1 to 16777214.
metric-type	Means the cost type of the default route.
tag *tag*	Means the routing identifier, which ranges from 0 to 4294967295.

Default value

No default route is introduced.

Command mode

Routing configuration mode

Instruction

The redistribute command cannot introduce the default route, and if you want to introduce the default route, you can use this command.
If the **always** parameter is set, no matter whether the default route exists in the current routing table, ASE-LSA, describing the default route, will be released out; if the **always** parameter is not set, ASE-LSA will be released out only when the default route exists in the current routing table.

Example

The following example shows how to introduce the default route from the OSPFv3 autonomous system.

```
router ospfv3 1
  router-id 2.2.2.2
  default-information originate always
```

Related command

redistribute

68.1.15 default-metric

To set the default weight of the introduced route, run the first one of the following two commands:

default-metric *value*

no default-metric

Parameter

Parameter	Description
value	Stands for the to-be-set route weight, ranging between 1 and 16777214.

Default value

The default route weight is 10.

Command mode

Routing configuration mode

Instruction

The **default-metric** command is used to set the default routing weight when the route of other routing protocol is guided into the OSPF packet. When the **redistribute** command is used to guide the route of other routing protocol, the default routing weight designated by the **default-metric** command will be guided the specific routing weight will not be specified.

Example

The following example shows how to introduce the static route and set the default route weight of other routing protocol to 3:

```
interface vlan 1
  ipv6 enable
```

```
    ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
    router-id 2.2.2.2
    default-metric 3
    redistribute static
```

Related command

redistribute

68.1.16 filter

To set the routing filtration table, run **filter {*interface-type interface-number* | *} {in | out } {access-list *access-list-name* | gateway *access-list-name* | prefix-list *prefix-list-name*}**. To resume the default settings, run **no filter {interface-type interface-number | *} {in | out } {access-list access-list-name | gateway access-list-name | prefix-list prefix-list-name}**.

filter {**interface-type** *interface*-number | ***}** {**in | out** } {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

no filter {**interface-type** *interface*-number | ***}** {**in** | out} {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

Parameter

***interface*-type**	Interface type
interface-number	Interface number
*****	All interfaces
In	Filtrates the received OSPF routes.
out	Filters the transmitted routes, which is not for a specific interface but for all interfaces.
access-list-name	Name of the IP access control list
access-list-name	Name of the IP access control list
prefix-list-name	Name of the prefix list

Default value

None

Command mode

Routing configuration mode

Example

The following example shows how to filter the received routes according to the **mylist** ACL.

```
router ospfv3 1
    filter * in access-list mylist
```

Related command

None

68.1.17 **ipv6** ospf area

To enable the OSPFv3 protocol on an interface and specify an area for this interface, run the first one of the following two commands:

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

Parameter

Parameter	Description
process-id	Stands for the OSPF process.
area-id	Stands for the OSPF area ID, which is specified by the interface.
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

None

Command mode

Interface configuration mode

Example

The following example shows how to enable OSPFv3 process 1 for interface vlan1 and set its area ID to 0.

```
interface vlan 1
    ipv6 enable
    ipv6 ospf 1 area 0
!
router ospfv3 1
    router-id 2.2.2.2
```

Related command

None

68.1.18 **ipv6** ospf cost

To designate the cost for the OSPFv3 protocol running on the interface, run **ipv6 ospf cost *cost***. To resume the default settings, run **no ipv6 ospf cost**.

ipv6 ospf cost *cost* [**instance** *instance-id*]

no ipv6 ospf *cost* *cost* [**instance** *instance-id*]

Parameter

Parameter	Description
cost	Cost for the OSPF protocol, which is an integer between 1 and 65535
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

The default cost for the OSPFv3 protocol running on the interface is obtained based on the rate of the port.

Command mode

Interface configuration mode

Example

The following example shows how to set the cost for the OSPFv3 protocol running on interface vlan1 to 2:

```
interface vlan 1
  ipv6 ospf cost 2
```

Related command

None

68.1.19 **ipv6** ospf database-filter all out

To designate an interface to filter those to-be-transmitted LSA, run the first one of the following two commands:

ipv6 ospf database-filter all out [**instance** *instance-id*]

no ipv6 ospf database-filter all out [**instance** *instance-id*]

Parameter

Parameter	Description
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

The interface does not filter those to-be-transmitted LSAs.

Command mode

Interface configuration mode

Example

The following example shows how to set interface vlan 1 to filter those to-be-transmitted LSAs:

```
interface vlan 1
  ipv6 ospf database-filter all out
```

Related command

None

68.1.20 **ipv6** ospf dead-interval

To designate the dead interval of the neighboring router, run **ipv6 ospf dead-interval *seconds***. To resume the default value, run **ipv6 ospf dead-interval**.

ipv6 ospf dead-interval *seconds* [**instance** *instance-id*]

ipv6 ospf dead-interval *seconds* [**instance** *instance-id*]

Parameter

Parameter	Description
seconds	Value of the dead interval for the neighboring router, which ranges from 1 to 2147483647 seconds
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

The dead interval for the neighboring router is four times of hello-interval by default.

Command mode

Interface configuration mode

Instruction

The value of the **dead-interval** parameter will be written to the HELLO packet and will be transmitted along with the HELLO packet. It must be ensured that the **dead-interval** parameter must be identical with that between the neighboring routers and the value of the **dead-interval** parameter must be four times of the value of the **hello-interval** parameter.

Example

The following example shows how to set the dead interval of the neighboring router on interface vlan1 to 60 seconds.

```
interface vlan 1
  ipv6 ospf dead-interval 60
```

Related command

None

68.1.21 **ipv6** ospf hello-interval

To designate the interval for transmitting the HELLO packet on the interface, run **ipv6 ospf hello-interval *seconds***. To resume the default settings, run **no ipv6 ospf hello-interval**.

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

Parameter

Parameter	Description
seconds	Transmission interval of the HELLO packet, ranging from 1 to 65535 seconds
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

The interval for the P2P or Broadcast interface to send Hello packets is 10 seconds, while the interval for the P2MP or NBMA interface to send Hello packets is 30 seconds.

Command mode

Interface configuration mode

Instruction

The value of the **dead-interval** parameter will be written to the HELLO packet and will be transmitted along with the HELLO packet. The smaller the hello-interval is, the sooner the change of the network topology will be found. However, much more path cost will be paid. It must be ensured that the parameter must be identical with that between the neighboring routers.

Example

The following example shows that the interval for transmitting the HELLO packet on interface vlan1 is set to 20 seconds.

```
interface vlan 1
  ipv6 ospf hello-interval 20
```

Related command

ipv6 ospf dead-interval

68.1.22 **ipv6** ospf mtu-ignore

To set the MTU value of the transmitted DD packet to 0 on an interface and meanwhile omit the checkup of the MTU domain of the received DD packet, run the first one of the following two commands:

ipv6 ospf mtu-ignore [**instance** *instance-id*]

no ipv6 ospf mtu-ignore [**instance** *instance-id*]

Parameter

Parameter	Description
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

The value of the MTU domain of the DD packet is set to be the MTU value of this interface and MTU checkup is not omitted.

Command mode

Interface configuration mode

Instruction

OSPF judges whether the MTU value of the network segment, where an interface belongs, is consistent by checking the MTU value of the exchanged DD packet.If the MTU value of the received DD packet is bigger than the MTU value of this interface, the OSPF neighborhood cannot be set up.

Example

The following example shows how to set interface vlan1 to omit MTU checkup.

```
interface vlan 1
  ipv6 ospf mtu-ignore
```

Related command

None

68.1.23 **ipv6** ospf neighbor

To set the OSPF neighbor on the non-broadcast network interface, run the first one of the following two commands:

ipv6 ospf neighbor *router-id* *ipv6-address* [**cost** *number*] [**database-filter all out**] [**poll-interval** *seconds*] [**priority** *number*] [**instance** *instance-id*]

no ipv6 ospf neighbor *router-id* *ipv6-address* [**cost** *number*] [**database-filter all out**] [**poll-interval** *seconds*] [**priority** *number*] [**instance** *instance-id*]

Parameter

Parameter	Description
router-id	Means the router ID of a neighbor.
ipv6-address	Means the local address of the neighbor's link.
cost *number*	Means the neighbor’s cost, whose value ranges from 1 to 65535.
database-filter all out	Filters the transmitted LSAs.
poll-interval *seconds*	Means the query interval of a neighbor.
priority *number*	Means the neighbor’s priority, whose value ranges from 0 to 255.
instance *instance-id*	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

No neighbors are set.

Command mode

Interface configuration mode

Instruction

You shall specify a neighbor manually on the non-broadcast network. If neighbors invalidates, the Hello packet should be sent to this neighbor in poll interval.

Example

The following example shows how to set the neighbor of interface vlan1.

```
interface vlan 1
  ipv6 ospf neighbor 1.1.1.1 fe80::1
```

Related command

None

68.1.24 **ipv6** ospf network

To set the network type for the interface, run the first one of the following two commands.

ipv6 ospf network { **broadcast | non-broadcast | point_to_multipoint | point-to-point**} [**instance** *instance-id*]

no ip ospf network { **broadcast | nonbroadcast | point_to_multipoint | point-to-point**} [**instance** *instance-id*]

Parameter

Parameter	Description
broadcast	Sets the network type of the interface to **broadcast**.
nonbroadcast	Sets the network type of the interface to **NBMA**.
point-to-multipoint	Sets the network type of the interface to **point-to-multipoint**.
point-to-point	Sets the network type of the interface to **point-to-point**.
instance *instance-id*	Specifies the OSPF instance ID of the interface, whose default value is 0.

Command mode

Interface configuration mode

Instruction

The interface in the broadcast network without multi-address access should be set to NBMA. In the NBMA network, the network should be set to **point-to-multipoint** if any two routers cannot be ensured to be directly reachable.

Example

The following example shows how to set interface vlan1 to NBMA.

```
interface vlan 1
  ipv6 ospf network non-broadcast
```

Related command

None

68.1.25 **ipv6** ospf priority

To configure the priority for the interface to choose the router, run **ipv6 ospf priority** ***priority***. To resume the default value, run **no ipv6 ospf priority**.

ipv6 ospf priority ***priority*** [**instance** *instance-id*]

no ipv6 ospf priority [**instance** *instance-id*]

Parameter

Parameter	Description
priority	Priority to choose the router, ranging between 0 and 255
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

The default priority for the interface to choose the routers is 1.

Command mode

Interface configuration mode

Instruction

When two routers in the same network segment want to be the selection router, the router with higher priority will be selected. If the priority of the two routers is the same, the router with a larger ID is selected. When the priority of a router is 0, the router cannot be selected as the designated router or the standby designated router. The priority is effective only on the networks except the nonpoint-to-point network.

Example

The following example shows how to set the priority to 8 when interface vlan1 selects the selection router.

```
interface vlan 1
  ipv6 ospf priority 8
```

Related command

None

68.1.26 **ipv6** ospf retransmit-interval

To designate the retransmission interval for transmitting LSA between the interface and the neighboring router, run **ipv6 ospf retransmit-interval seconds**. To resume the default value, run **no ipv6 ospf retransmit-interval**.

ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]

Parameter

Parameter	Description
seconds	Transmission interval for transmitting the link state broadcast between the interface and the neighboring router, ranging between 1 and 3600 seconds
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

The default interval for transmitting the link state broadcast between the interface and the neighboring router is 5 seconds.

Command mode

Interface configuration mode

Instruction

When a router transmits the link-state broadcast to its neighbor, the command will maintain the link-state broadcast until the peer receives the acknowledgement. If the link-state broadcast is not received during the transmission interval, it will be retransmitted. The value of the **seconds** parameter must be larger than the round-trip time for a packet transmitting between two routers.

Example

The following example shows how the default interval for transmitting the link-state broadcast between interface vlan1 and the neighboring router is set to 8 seconds.

```
interface vlan 1
  ipv6 ospf retransmit-interval 8
```

Related command

None

68.1.27 **ipv6** ospf transmit-delay

To set the delay for the link-state broadcast to be transmitted on the interface, run **ipv6 ospf transit-delay time**. To resume the default value, run **no ipv6 ospf transit-delay**.

ipv6 ospf transit-delay *time* [**instance** *instance-id*]

no ipv6 ospf transit-delay *time* [**instance** *instance-id*]

Parameter

Parameter	Description
time	Means the delay of link state broadcast transmission on an interface, which ranges from 1 to 3600 seconds.
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

The default delay for the link-state broadcast to be transmitted on the interface is 1 second.

Command mode

Interface configuration mode

Example

The following example shows how to set the delay for transmitting the link-state broadcast on interface vlan1 to 3 seconds.

```
interface vlan 1
  Ipv6 ospf transit-delay 3
```

Related command

None

68.1.28 passive-interface

To forbid a designated interface to transmit or receive the OSPFv3 packets, run the first one of the following two commands:

passive-interface { *interface-type* *interface-number* **| all }**

no passive -interface { *interface-type* *interface-number* **| all }**

Parameter

Parameter	Description
interface-type *interface-number*	Means the interface type and the interface ID.
all	Means all interfaces.

Default value

The interface is allowed to transmit or receive the OSPFv3 packets.

Command mode

Routing configuration mode

Instruction

Different processes can forbid a same interface to transmit or receive the OSPFv3 packets, but the passive-interface command takes effect only on the OSPFv3 interface.

Example

The following example shows how to forbid interface vlan1 to receive and transmit the OSPFv3 packets in the OSPFv3 process.

```
router ospfv3 100
  passive –interface vlan 1
```

Related command

None

68.1.29 redistribute

To configure the route where OSPF forwards other routing protocols, run **redistribute**. To resume the default settings, run **no redistribute**.

redistribute *protocol* [*as-number*] [**route-map *map-tag***]

no redistribute *protocol* [*as-number*] [**route-map *map-tag***]

Parameter

Parameter	Description
protocol	Means to forward the learned original protocol.
as_number	Means the number of the autonomous system which is not for the **connect**, **rip** or **static** parameter.
map-tag	Means the name of the route map.

Default value

Not forward

Command mode

Routing configuration mode

Instruction

None

Example

The following example shows how to forward the static route in OSPF process 1:

```
interface vlan 1
    ipv6 enable
    ipv6 ospf 1 area 0
!
router ospfv3 1
    router-id 2.2.2.2
redistribute static
```

68.1.30 **router** ospfv3

To enable OSPFv3 and enter the OSPFv3 configuration view, run the first one of the following two commands:

router ospfv3 *process-id*

no router ospfv3 *process-id*

Parameter

Parameter	Description
process-id	Identifies the OSPF process. It is a positive integer distributed by the local router.

Default value

None

Command mode

Global configuration mode

Instruction

One router may have multiple OSPFv3 processes.

Example

The following example shows how to set an OSPFv3 process, whose process ID is 109:

router ospfv3 109

Related command

ipv6 ospf area

68.1.31 router-id

To set the router ID in the autonomous system for the router on which the OSPFv3 protocol is running, run the first one of the following two commands:

router-id *router-id*

no router-id *router-id*

Parameter

Parameter	Description
router-id	Means the identifier of the router, which is in the IPv4 address format.

Default value

If an IPv4 address has already configured on a router before OSPFv3 is enabled, the router will automatically choose an IPv4 address as its ID.

Command mode

Routing configuration mode

Instruction

The router ID is the unique identifier of a OSPFv3-running router in the autonomous system, so the router IDs of two routers in the autonomous system are different. If a router has no router ID, the OSPFv3 process cannot go on.

Example

The following example shows how to set the router ID of OSPFv3 process 1 to 2.2.2.2:

```
router ospfv3 1
  router-id 2.2.2.2
```

68.1.32 show ipv6 ospf

To display the main OSPFv3 information, run the following command:

show ipv6 ospf [*process-id*]

Parameter

Parameter	Description
process-id	Means the OSPF process ID.

Default value

None

Command mode

EXEC

Instruction

The information exported by the command can help checking the OSPFv3 faults. If the **process-id** parameter follows the command, the information about the global configuration of the OSPFv3 process is displayed.

Example

The following example shows that the configuration information about all OSPFv3 processes will be displayed.

```
router# show ipv6 ospf
```

Routing Process "OSPFv3 0" with ID 1.2.3.4
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 3. Checksum Sum 0x2CD6F
Number of areas in this router is 1
Area BACKBONE(0)
Number of interfaces in this area is 1
SPF algorithm executed 3 times
Number of LSA 4. Checksum Sum 0x2A6AC
router#

Relative fields are explained in the following table:

Domain	Description
Routing Process "OSPFv3 0"	ID of the process
with ID 1.2.3.4	ID of the router
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs	Two timer values relative with OSPF
Number of areas is 1	Number of the currently-configured fields, and parameters configured in each field
Number of LSA 4	Quantity of LSAs in the database
Number of external LSA 3	Quantity of ASE LSAs in the database
SPF algorithm executed 3 times	SPF algorithm execution statistics

68.1.33 **show** ipv6 ospf database

To display the database information about the OSPFv3 connection state, run the following command:

show ipv6 ospf database { router | network | inter-prefix | inter-router | external | link | intra-prefix **} [** ADVROUTER **]**

Parameter

Parameter	Description
router	Means the LSA type is the router.
network	Means the LSA type is the network.
inter-prefix	Means the LSA type is the inter-domain route.
inter-router	Means the LSA type is the inter-domain router.
external	Means the LSA type is the exterior route.
link	Means the LSA type is the link.

intra-prefix	Means the LSA type is the inside-domain route.
ADVROUTER	Means to declare the router ID.

Default value

None

Command mode

EXEC

Instruction

The information exported by the command can help to check the database information about the OSPFv3 connection state and to find the reason of the faults.

Example

router#
router#show ipv6 ospf database
Link-LSA (Interface eth0)
Link State ID ADV Router Age Seq# CkSum Prefix
0.0.0.3 1.2.3.4 104 0x80000004 0x889e 0
0.0.0.5 5.6.7.8 142 0x80000003 0xab70 2
Router-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum Link
0.0.0.1 1.2.3.4 94 0x80000014 0xeaea 1
0.0.0.1 5.6.7.8 105 0x80000019 0x8a32 1
Network-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum
0.0.0.5 5.6.7.8 105 0x80000001 0xa441
Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum Prefix Reference
0.0.0.1 5.6.7.8 104 0x80000001 0x8d4f 2 Network-LSA
AS-external-LSA
Link State ID ADV Router Age Seq# CkSum
0.0.0.1 5.6.7.8 1229 0x80000002 0xe92d
0.0.0.2 5.6.7.8 1229 0x80000002 0xef25
0.0.0.3 5.6.7.8 1229 0x80000002 0xf51d
router#

Relative fields are explained in the following table:

Domain	Description
AREA: 1	Current area
Router Link	LSA type

States/Net Link States/Summary Net Link States	
Link ID	LSA ID
ADV Router	Releases the router.
Age	Releases the age.
Seq #	Generates the sequence ID.
Checksum	Means the checksum.

68.1.34 **show** ipv6 ospf interface

To display the information about the OSPFv3 interface, run the following command:

show ipv6 ospf interface [type] [index]

Parameter

Parameter	Description
type	Port type
index	Port number

Default value

None

Command mode

EXEC

Instruction

According to the information displayed by the command, you can check the OSPFv3 configuration and its running state, which helps you to detect the OSPFv3 faults.

Example

router#**show ipv6 ospf interface**
ethernet0/1 is up, line protocol is up
Interface ID 3, Instance ID 0, Area 0.0.0.0
IPv6 Link-Local Address fe80::248:54ff:fec0:f32d/10
Router ID 1.2.3.4, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State Backup, Priority 1
Designated Router (ID) 5.6.7.8
Interface Address fe80::203:47ff:fe4c:776e

Backup Designated Router (ID) 1.2.3.4
Interface Address fe80::248:54ff:fec0:f32d
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Neighbor Count is 1, Adjacent neighbor count is 1
router#

Relative fields are explained in the following table:

Domain	Description
IPv6 Link-Local Address	Address of port **IPv6 link-local**
Nettype	Network type of the OSPF interface
OSPF process is	ID of the OSPF process
AREA	Current area
Router ID	ID of the router where the process belongs
Cost	Cost of the OSPF interface of the router
Transmit Delay is	Transmission delay
Priority	Priority for the interface of the router
Hello interval	Transmission interval of the Hello packet
Dead timer	Dead time
Retransmit	Retransmission interval
OSPF INTF State is	State of the OSPF port
Designated Router id	ID of the designated router and the IP address of its port
Backup Designated router id	ID of the backup designated router and the IP address of its port
Neighbor Count is	Number of the neighboring routers
Adjacent neighbor count is	Number of neighbors that have established the neighborhood relation
Adjacent with neighbor	Neighbor lists that have established the neighborhood relation

68.1.35 **show** ipv6 ospf neighbor

To display the information about OSPFv3 neighbor, run the following command.

show ipv6 ospf neighbor [interface_type interface_number | router-id | detail]

Parameter

Parameter	Description
interface_type	Port type

interface_number	Port number
router-id	Router ID
detail	Displays the detailed information.

Default value

None

Command mode

EXEC

Instruction

The information displayed by the command can help you to check whether the OSPFv3 neighbor configuration is right and to detect the OSPFv3 faults.

Example

router#**show ipv6 ospf neighbor**

OSPFv3 Process 1

Area 1

Neighbor ID Pri State Dead Time Interface Instance ID

5.6.7.8 1 Full/DR 00:00:38 eth0 0

Relative fields are explained in the following table:

Domain	Description
OSPFv3 process	ID of the OSPF process
AREA	Local area
Neighbor	ID of a neighbor
Pri	Priority of a neighbor
State	Connection state related with the neighbor
DeadTime	Time of neighbor invalidation
Address	IP address of the neighbor
Interface	Interface used by a router to reach its neighbor

68.1.36 **show** ipv6 ospf route

To display the information about the OSPFv3 routing table, run the following command:

show ipv6 ospf route

Parameter

None

Default value

None

Command mode

EXEC

Instruction

The information displayed by the command can help you browse the OSPFv3 routing table and confirm whether the OSPFv3 trouble diagnosis is correctly carried out.

Example

router#**show ipv6 ospf route**
Destination Metric
Next-hop Interface
3ffe:1:1::/48 10
-- eth0
3ffe:2:1::/48 10
-- eth0
3ffe:2:2::/48 10
-- eth0
3ffe:3:1::/48 10
-- eth0
3ffe:3:2::/48 10
-- eth0
3ffe:3:3::/48 10
-- eth0
E2 3ffe:100:1::1/128 10/20
fe80::203:47ff:fe4c:776e eth0
E2 3ffe:100:2::1/128 10/20
fe80::203:47ff:fe4c:776e eth0
E2 3ffe:100:3::1/128 10/20
fe80::203:47ff:fe4c:776e eth0
IA 3ffe:101:1::/48 20
fe80::203:47ff:fe4c:776e eth0
IA 3ffe:101:2::/48 20
fe80::203:47ff:fe4c:776e eth0
IA 3ffe:101:3::/48 20
fe80::203:47ff:fe4c:776e eth0

Relative fields are explained in the following table:

Domain	Description
Destination	Destination network segment
Metric	Cost of a route
Next-hop	Address of the next hop
Interface	Interface of the next hop

68.1.37 show ipv6 ospf virtual-link

To display the information about the OSPFv3 virtual link, run the following command:

show ipv6 ospf virtual-link

Parameter

None

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can check the state of the OSPFv3 virtual link.

You can run **show ipv6 ospf neighbor** to check the detailed information about the adjacent neighbor.

Example

router#show ipv6 ospf virtual-link

Virtual Link VLINK1 to router 5.6.7.8 is up

Transit area 0.0.0.1 via interface eth0, instance ID 0

Local address 3ffe:1234:1::1/128

Remote address 3ffe:5678:3::1/128

Transmit Delay is 1 sec, State Point-To-Point,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:01

Adjacency state Up

Relative fields are explained in the following table:

Domain	Description
neibhbor ID	Neighbor ID of the peer
邻居状态	Neighborhood state for the neighbor
TransArea	Transmission area
cost	Minimum cost for reaching the peer in the transmission area If the value of the cost is 0, it means that the peer is unreachable.
Hello Interval	Current transmission interval for the Hello packet
DeadTime	Time of neighbor invalidation
Retrans	Retransmission interval
Adjacency state	State of the virtual link interface

Related command

area vritual-link

show ipv6 ospf neighbor

68.1.38 summary-prefix

To configure the address for OSPFv3 to create the route aggregation, run **summary-prefix**. To cancel the address of route aggregation, run **no summary-prefix**.

summary-prefix *ipv6-prefix /prefix-length*

no summary-prefix *ipv6-prefix /prefix-length*

Parameter

Parameter	Description
ipv6-prefix	Aggregation address with the designated address range
prefix-length	Subnet mask of the aggregation route

Default value

None

Command mode

Routing configuration mode

Instruction

Multiple groups of addresses are summarized. Routes learned from other routing protocols can also be summarized. After the aggregation, all covered networks cannot be transmitted to other routing fields. The cost of the summary route is the minimum value among the cost values of all summary routes. The command cannot be used to reduce the size of the routing table.

The command is used by OSPFv3 to enable the ASBR to notify an external route of being an aggregation route to replace all external routes. The command is only used to aggregate the OSPFv3 routes of other routing protocols. You can run **area range** in OSPFv3 to summarize the routes.

Example

In the following example, the summary address 2001::/64 stands for addresses such as 2001::/80, 2001::1/64 and so on, and only address 2001::/64 is broadcasted.

summary-address 2001::/64

Related command

area range

68.1.39 **timers** delay

To designate a delay interval between OSPF receiving a topology change and starting a shortest path priority calculation, run **timers delay *spf-delay***. To resume the default settings, run **no timers delay**.

timers delay *spf-delay*

no timers delay

Parameter

Parameter	Description
spf-delay	Delay between the topology change and calculation start Its default value is 5 seconds. If the value is 0, there is no delay. That is, the calculation will be promptly started if changes occur.

Default value

spf-delay: 5 seconds

Command mode

Routing configuration mode

Instruction

The smaller value the delay is set to, the faster the network change is reflected. However, it will take the processor more time.

Example

The following example shows how to set the time for OSPF to start calculating the delay is 10 seconds.

timers delay 10

68.1.40 **timers** hold

To set the interval between two continuous SPF calculations, run **timers hold**. To resume the default settings, run **no timers hold**.

timers hold *spf-holdtime*

no timers hold

Parameter

Parameter	Description
spf-holdtime	Minimum value between two continuous calculations It ranges between 0 to 65535 seconds. Its default value is 10 seconds; when it is 0, there is no interval between the two continuous calculations.

Default value

spf-holdtime: 10 seconds

Command mode

Routing configuration mode

Instruction

The smaller value the delay is set to, the faster the network change is reflected. However, it will take the processor more time.

Example

The following example shows how to set the interval between two successive SPF calculations to 20 seconds:

timers hold 20

Chapter 69 BFD Configuration Commands

BFD configuration commands are shown as follows:

- bfd init-mode
- bfd slow-timers
- bfd demand enable
- bfd echo enable
- bfd enable
- bfd neighbor
- bfd min_echo_rx_interval
- bfd authentication-mode
- show bfd

69.1.1 bfd init-mode

To enable the initial BFD mode, run the following command:

bfd init-mode *[active | passive]*

no bfd init-mode

Parameter

Parameter	Description
active	Means that the BFD neighbor sends the control packets actively to establish the BFD connection.
passive	Means that the BFD neighbor won't send any BFD packets when BFD neighbor is down.

Default value

The value of the **init-mode** parameter is **active**.

Command mode

Global configuration mode

Explanation

The BFD connection requires one terminal to be active in its initial mode, or the BFD connection cannot be set up.

Example

The following example shows how to set the BFD mode of local system to **passive**.

Switch#

Switch#conf

Switch_config#bfd init-mode passive

Related command

bfd slow-timers

69.1.2 bfd slow-timers

To set the slow timer of BFD, run **bfd slow-timers**; to resume the default settings, run **no bfd slow-timers**.

bfd slow-timers <*value*>

no bfd slow-timers

Parameter

Parameter	Description
value	It ranges between 1000ms and 30000ms.

Default value

The default value of slow-timers is 1.

Command mode

Global configuration mode

Explanation

This command is used to set the BFD slow-timers, which is 1 second by default. The BFD neighbor transmits control packets at an interval of this configured time before it is up. This is mainly to prevent those not-up sessions from consuming too much bandwidth.

When the echo function is activated, echo packets are responsible for conducting real connectivity checkup. Hence, BFD control packets are not frequently forwarded and

the system takes this configured slow-timers as the interval for transmitting control packets.

Example

The following example shows how to set the slow-timers of BFD to 2 seconds:

Switch#

Switch#conf

Switch_config#bfd slow-timers 2000

Related command

bfd init-mode

69.1.3 bfd demand enable

To activate the BFD query mode, run **bfd demand enable**; to disable the BFD query mode, run **no bfd demand enable**.

bfd demand enable

no bfd demand enable

Parameter

N/A

Default value

The BFD query mode is not activated by default.

Command mode

Interface configuration mode

Explanation

In query mode, we suppose that each system has an independent method to confirm its connection with other systems. Once a BFD session is conducted, the system stops transmitting BFD control packets unless a certain system requires explicit connectivity checkup. In a system where explicit connectivity checkup is required, the system transmits short-sequence BDF control packets and claims the session is down if it doesn't receive the response packets in the checkup period.

Example

The following example shows how to enable the VLAN1 BFD query mode.

Switch_config#

Switch_config# interface vlan 1
Switch_config_v1#bfd enable
Switch_config_v1#bfd demand enable

Related command

bfd enable

69.1.4 bfd echo enable

To activate BFD echo, run **bfd echo enable**; to disable BFD echo, run **no bfd echo enable**.

bfd echo enable <*cr*>|<*number*>

no bfd echo enable

Parameter

Parameter	Description
number	Stands for the allowable maximum number of dropped echo packets, which is 3 by default and ranges from 3 to 10.

Default value

The BFD echo is not activated by default.

Command mode

Interface configuration mode

Explanation

After BDF echo is activated, connectivity checkup is conducted by the echo packets.

Example

The following example shows how to activate VLAN1 BFD echo and set the allowable maximum number of echo packet losses to **4**.

Switch_config#
Switch_config#int vlan1
Switch_config_v1#bfd enable
Switch_config_v1#bfd echo enable 4

Related command

bfd enable

bfd min_echo_rx_interval

69.1.5 bfd enable

To activate BFD on a port, run **bfd enable**; to disable BFD on a port, run **no bfd enable**.

bfd enable *<cr> | [**min_tx_interval** <tx_value> **min_rx_interval** <rx_value> **multiplier** <m_value>]*

no bfd enable

Parameter

Parameter	Description
tx_value	Sets the minimum interval of transmitting control packets, which ranges from 10ms to 999ms and the default value of which is 50ms.
rx_value	Sets the minimum interval of receiving control packets, which ranges from 10ms to 999ms and the default value of which is 50ms.
m_value	Sets the checkup coefficient of BFD control packets, which ranges from 3 to 50 and the default value of which is 3.

Default value

The BFD function is not activated on ports.

Command mode

Interface configuration mode

Explanation

The precondition for activating BFD on a port is that the IP address of this port must exist.

Note:

Both **min_tx_interval** and **min_rx_interval** are used as references for the local BFD and the peer BFD. They are not real intervals of packet reception and transmission. The multiplier has no role in the local BFD, but is used for the peer BFD to calculate the checkup time.

Example

The following example shows how to enable VLAN1 BFD, set the minimum intervals of both transmitting and receiving control packets to **80ms** and the checkup coefficient to **5**.

Switch_config#

Switch_config#int vlan1

Switch_config_v1#bfd enable min_tx 80 min_rx 80 multi 5

Related command

ip address

69.1.6 bfd neighbor

To set the static BFD neighbor, run **bfd neighbor**; to delete the static BFD neighbor, run **no bfd neighbor**.

bfd neighbor <*ip-add*>

no bfd neighbor <*ip-add*>

Parameter

Parameter	Description
Ip-add	Stands for the to-be-configured IP address.

Default value

No static BFD neighbor exists on the port.

Command mode

Interface configuration mode

Explanation

BFD is a two-way checkup protocol. If it is used to check the unidirectional paths such as static route, a problem may arise that no BFD neighbor exists on the peer end. Hence you have to use this command to set a static neighbor. Of course, you can solve this problem through dynamic protocol.

Example

The following example shows how to set static BFD 172.16.1.100 on interface vlan1.

Switch_config#

Switch_config#int vlan1

Switch_config_v1#bfd enable

Switch_config_v1#bfd neighbor 172.16.1.100

Related command

bfd enable

69.1.7 bfd min_echo_rx_interval

To set the minimum interval of receiving BFD echo packets, run **bfd min_echo_rx_interval**; to resume the default settings, run **no bfd min_echo_rx_interval**.

bfd min_echo_rx_interval <*value*>

no bfd min_echo_rx_interval

Parameter

Parameter	Description
value	<10-999>, unit: millisecond

Default value

The default value of **min_echo_rx_interval** is 50ms.

Command mode

Interface configuration mode

Explanation

This command is used to set the minimum interval of receiving BFD echo packets. Because echo packets are locally transmitted and locally received, the echo packet transmission interval in the local system is also set via this command.

Example

The following example shows how to activate BFD echo on interface vlan1 and set the minimum interval of receiving BFD echo packets to 80ms.

```
Switch_config#
Switch_config#int vlan1
Switch_config_v1#bfd enable
Switch_config_v1#bfd echo enable
Switch_config_v1#bfd min_echo_rx_interval 80
```

Related command

bfd enable

bfd echo enable

69.1.8 bfd authentication-mode

To set the authentication of BFD packets, run **bfd authentication-mode**; to disable the authentication of BFD packets, run **no authentication-mode**.

bfd authentication-mode *[**md5** | **meticulous md5** | **simple**]* <*key id*> <*key*>

no bfd authentication-mode

Parameter

Parameter	Description
md5	MD5 authentication
meticulous md5	Securer MD5 authentication
simple	Simple password authentication
key id	Authentication ID
key	Authentication password (up to 16 characters)

Default value

The authentication function is not enabled.

Command mode

Interface configuration mode

Explanation

After BFD authentication is configured, BFD will transmit control packets with the authentication field. Normal link checkup can be performed only when two BFD terminals have the same authentication configuration.

Note: Those BFD neighbors in UP state are not subject to authentication changes.

Example

The following example shows how to enable BFD MD5 authentication on interface VLAN1:

```
Switch_config#
Switch_config#int vlan1
Switch_config_v1#bfd enable
Switch_config_v1#bfd authentication-mode md5 1
```

Related command

bfd enable

69.1.9 show bfd

To display the BFD-related information, run the following command:

show bfd interfaces *[details]* **| neighbors** *[details]*

Parameter

N/A

Default value

Command mode

Global configuration mode

Explanation

This command is used to set the BFD-related information.

Example

N/A

Related command

bfd enable

bfd neighbor

Chapter 70 SNTP Configuration Commands

70.1 SNTP Configuration Commands

SNTP configuration commands include:

- sntp master
- sntp query-interval
- sntp server
- sntp peer
- sntp source
- show sntp
- debug sntp
- time-zone

70.1.1 sntp master

To set the level of the local clock, run **sntp master *num***; to cancel this settings, run **no sntp master**.

sntp master *num*

no sntp master

Parameter

Parameter	Description
num	Means the level of the clock.

Default

None

Command mode

Routing configuration mode

Remark

The clock level is disabled by default; if it is enabled, the level ranges between 1 and 15, and will be 8 without configuration.

Example

Router_config#sntp master 5

Related Commands

sntp peer

sntp server

70.1.2 sntp query-interval

To set the interval of sending the SNTP requests, run **sntp query-interval *time***. To resume the default settings, run **no sntp query-interval**.

sntp query-interval *time*

no sntp query-interval

Parameter

Parameter	Description
Time	Means the interval of sending the requests.

Default

The default value is 1, that is, the requests will be sent every minute.

Command mode

Routing configuration mode

Remark

The time ranges between 1 and 1440 minutes.

Example

Router_config#sntp query-interval 5

70.1.3 sntp server

To set the address of the SNTP server, run **sntp server *address*** **[key *key-number*** | **version *version-number*]**.

sntp server *address* ［**key** *key-number* | **version** *version-number*］

no sntp server *address*

Parameter

Parameter	Description
address	Means the address of the SNTP server.
version-number	Means the version ID of SNTP (1-4).
key-number	Means the key ID of the SNTP server.

Default

None

Command mode

Routing configuration mode

Remark

You can set multiple addresses for the SNTP server. There is no SNTP server by default.

Example

Router_config#sntp server 1.1.1.1 4

Related Command

sntp peer

70.1.4 sntp peer

To set the SNTP peer, run **sntp peer *address version***. To delete the SNTP peer, run **no sntp peer *address***.

sntp peer *address version*

no sntp peer *address*

Parameter

Parameter	Description
address	Means the address of the SNTP peer.
version	Means the version ID of SNTP (1-4).

Default

None

Command mode

Routing configuration mode

Remark

This command is used to set the address of the SNTP peer.

Example

Router_config#sntp peer 1.1.1.1 4

Related Command

Sntp server

70.1.5 sntp source

To set the designated local source address when SNTP is triggered, run **Sntp source [interface *inter* | *addr*]**.

Sntp source ［**interface** *inter* | *addr*］

No sntp source

Parameter

Parameter	Description
inter	Means an interface.
Address	Means a designated source address.

Default

None

Command mode

Routing configuration mode

Remark

This command is used to designate the source address of sending the SNTP packets.

Example

Router_config#sntp source 1.1.1.1

70.1.6 sntp authenticate

To enable the SNTP authentication, run **sntp authenticate**.

sntp authenticate

no sntp authenticate

Parameter

None

Default

The authentication is disabled.

Command mode

Routing configuration mode

Remark

This command is used to enable SNTP authentication.

Example

Router_config#sntp authenticate

70.1.7 sntp authentication-key

To set the local authentication key of SNTP, run **sntp authentication-key *number* md5 *type password***.

sntp authentication-key *number* **md5** *type password*

no sntp authentication-key *number*

Parameter

Parameter	Description
number	Key number
type	Means the mode to display the password.
password	Means the corresponding MD5 password.

Default

None

Command mode

Routing configuration mode

Remark

This command is used to set the local authentication key.

Example

Router_config#sntp authentication-key 2 md5 0 123456

70.1.8 sntp trusted-key

To set the trusted local key, run **sntp trusted-key *number***.

sntp trusted-key *number*

no sntp trusted-key *number*

Parameter

Parameter	Description
number	Key number

Default

None

Command mode

Routing configuration mode

Remark

This command is used to set the trusted local key.

Example

```
Router_config#sntp trusted-key 1
```

70.1.9 show sntp

To display the SNTP related information, run the following command:

Show sntp

Parameter

None

Default

None

Command mode

EXEC mode

Remark

This command is used to display the current status of SNTP.

Example

```
Router_config#show sntp
Master Mode: Yes              Master Clock Stratum: 5
  Debug Mode: Off             Client Status: idle
Interval to Query SNTP Server: 1 (minutes)
Configured SNTP Server List:
Current SNTP Server :    00010003
Configured SNTP Peer List:
              IP: 1.1.1.1         Version: 4
Current SNTP Peer : 1.1.1.1 00010003
```

The local time (UTC): Date: 2002-3-25 Time: 17:36:59

70.1.10 debug sntp

To enable SNTP debugging, run **debug sntp**. To disable SNTP debugging, run **no debug sntp**.

Debug sntp

no debug sntp

Parameter

None

Default

None

Command mode

EXEC mode

Remark

You can browse the SNTP operation according to the displayed information.

Example

None

70.1.11 time-zone

To open the time zone, run **time-zone *name offset-hour offset-minute***. To close the time zone, run **no time-zone**.

time-zone *name offset-hour offset-minute*

no time-zone

Parameter

Parameter	Description
name	Means the name of a time zone.
offset-hour	Means the offset hour between the local time and the UTC time (-12-12).

offset-minute	Means the offset minute between the local time and the UTC time (0-59).

Default

None

Command mode

Routing configuration mode

Remark

This command can be used to transfer UTC to the local time.

Example

Router_config#time-zone BeiJing 8

70.1.12 time-range

To open the time range, run **time-range *name***. To close the time zone, run **no time-range *name***.

time-range *name*

no time-range *name*

Parameter

Parameter	Description
name	Means the name of a time range.

Default

None

Command mode

Routing configuration mode

Remark

This command is used to set a time range.

Example

Router_config#time-range aaa

70.1.13 absolute

To set the absolute time of a time range, run **absolute start *hh:mm day month year* end *hh:mm day month year***. To resume the default settings, run **no absolute**.

absolute start *hh:mm day month year* **end** *hh:mm day month year*

no absolute

Parameter

Parameter	Description
hh:mm	Stand for the hour and the minute respectively.
day	Stands for a day.
month	Stands for a month.
year	Stands for a year.

Default

None

Command mode

Time range configuration mode

Remark

This command is used to set an absolute time range.

Example

Router_config_time_range#absolute start 11:11 2 2 2000 end 22:22 3 3 2002

70.1.14 periodic

To set the periodic time of a time range, run the first one of the following two commands.

Periodic *[Monday / Tuesday / Wednesda / Thursday / Friday / Saturday / Sunday / daily / weekdays / weekend] hh:mm to [Monday / Tuesday /*

Wednesda / Thursday / Friday / Saturday / Sunday / daily / weekdays / weekend] hh:mm

no Periodic

Parameter

Parameter	Description
hh:mm	Stand for the hour and the minute respectively.

Default

None

Command mode

Time range configuration mode

Remark

This command is used to set an absolute time range.

Example

Router_config_time_range#periodic monday 11:11 to tuesday 11:11

Chapter 71 Cluster Management Configuration Commands

71.1 Cluster Management Configuration Comamdns

- cluster address-pool
- cluster mode
- cluster commander-address
- cluster member
- cluster discovery hop-count
- cluster hello-time
- cluster hold-time
- show cluster
- show cluster candidate
- show cluster member
- show cluster topo
- show cluster address pool

71.1.1 cluster address-pool

description

cluster address-pool *A.B.C.D mask*

no cluster address-pool

parameter

parameter	parameterinstruction
A.B.C.D	Network segment of the ip address pool. Valid value range: N/A.
mask	Network segment mask of the ip address pool. Valid value range: N/A.

default

Default network segment is 192.166.0.0/255.255.0.0

instruction

This command is used to configure the inner ip address used for cluster management. When the ip address is used, it will not open to the outer user operation. When the cluster feature has not been enabled on the device, this command can be configured repeatedly, only the last configuration is valid. When the cluster feature has been enabled on the device, this command can not be configured repeadly. This command can only be configured on the switch.

Address number in the address pool should be greater than the number of cluster member.

example

The following example sets 192.167.0.0/255.255.0.0 as the cluster address pool:

switch_config#cluster address-pool 192.167.0.0 255.255.0.0

71.1.2 cluster mode

description

To configure the role that a switch plays in the cluster, use the cluster mode member command. Use the no form of this command to restore the default value.

cluster mode member | **commander** *cluster-name*

no cluster mode

parameter

parameter	parameterinstruction
cluster-name	Cluster name. Valid value range: N/A.

default

no cluster mode

instruction

cluster mode member configures switch to cluster candidate member；

cluster mode commander cluster-name configures switch to cluster command switch；

The no cluster mode should be operated when switching between candidate member and command switch.

command mode

global configuration mode

example

The following command configures switch to cluster candicate member：

switch_A_config #cluster mode member

The following command configures switch to cluster command switch：

switch_A_config #cluster mode commander campus

71.1.3 cluster commander-address

description

cluster commander-address *H.H.H* [name *name*]

no cluster commander-address

parameter

parameter	parameterinstruction
H.H.H	MAC address of the server.
name	Name of the cluster. Valid value range is from 1 to 31 characters.

default

default

instruction

You do not need to enter this command from a standalone cluster member switch. The cluster command switch automatically provides its MAC address to cluster member switches when these switches join the cluster. The cluster member switch adds this information and other cluster information to its running configuration file. Use the no form of this global configuration command from the cluster member switch console port to remove the switch from a cluster only during debugging or recovery procedures.

example

The following information is a portion of output of the show running-config command on a cluster member switch：

cluster commander-address 00e0.0f2b.626e name test_cluster

The following command separates the member switch from the cluster：

switch_A_config#no cluster commander-address

71.1.4 cluster member

description

Use the cluster member command on the cluster command switch to add candidates to a cluster. Use the no form of the command to remove members from the cluster.

cluster member [*n*] **mac-address** *H.H.H* [**password** *enable-password*]

no cluster member id *n*

parameter

parameter	parameterinstruction
n	The number that identifies a cluster member. The range is 0 to 255.
H.H.H	MAC address of the cluster member switch in hexadecimal format.
enable-password	Enable password of the candidate switch. The password is not required if there is no password on the candidate switch.

default

no default value

instruction

This command can only be executed on the commander switch. This command cannot be executed repeatedly.

example

This example shows how to add a switch as member 3 with MAC address 00e0.0f2b.626d and the password key to a cluster.

switch_A_config#cluster member id 3 mac-address 00e0.0f2b.626d password key

The following example shows how to add a candidate switch with MAC address 00e0.0f2b.626e to a cluster:

switch_A_config#cluster member mac-address 00e0.0f2b.626e

71.1.5 cluster discovery hop-count

description

cluster discovery hop-count number

no cluster discovery hop-count

parameter

parameter	parameterinstruction
number	Number of hops from the cluster edge that the cluster command switch limits the discovery of candidates. The range is 1 to 7.

default

The hop count is set to 3.

instruction

This command is available only on the cluster command switch. This command does not operate on cluster member switches.

If the hop count is set to 1, it disables extended discovery. The cluster command switch discovers only candidates that are one hop from the edge of the cluster. The edge of the cluster is the point between the last discovered cluster member switch and the first discovered candidate switch.

example

This example shows how to set hop count limit to 4.

switch_A_config#cluster discovery hop-count 4

71.1.6 cluster hello-time

description

cluster hello-time *interval*

no cluster hello-time

parameter

parameter	description
interval	Duration in seconds of the hello timer. The range is 1 to 300 seconds.

default

The default holdtime is 8 seconds.

instruction

Enter this command with the cluster timer global configuration command only on the cluster command switch. The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.

example

This example shows how to change the interval timer and the duration on the cluster command switch.

```
switch_A_config#cluster hellotime 3
```

71.1.7 cluster hold-time

description

cluster hold-time *holdtime*

no cluster hold-time

parameter

parameter	description
interval	Duration in seconds before a switch (either a command or cluster member switch) declares the other switch down. The range is 1 to 300 seconds.

default

The default holdtime is 80 seconds.

instruction

Enter this command with the cluster timer global configuration command only on the cluster command switch. The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.

The holdtime is typically set as a multiple of the interval timer (cluster timer). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.

example

This example shows how to change the interval timer and the duration on the cluster command switch.

switch_A_config#cluster holdtime 30

71.1.8 show cluster

description

show cluster

parameter

none

default

none

instruction

This command shows basic configuration information of the cluster feature. If this device is not among the cluster, the system will output error information; if this device is command switch, the system will display cluster name, total number of mumbers, inaccessible number of mumbers, backup group information, timer information and address pool; if the device is member, the system will display cluster member number, communication status and other information.

example

The display of the command switch is as follows：

switch_A#show cluster
Commander of cluster "zmz"
Total number of members: 2

Hello timer 8
Hold timer 80
Topologic discovery hops 3
Address pool net address 192.166.0.0
Address pool address mask 255.255.0.0
Member 1(mac 00e0.0f2b.626d) is up, hold time 76.780 second

The display of the cluster member is as follows：

switch_B#show cluster
Member 1 of cluster "zmz"
Total number of members: 2
Hello timer 8
Hold timer 80
Topologic discovery hops 3
Address pool net address 192.166.0.0
Address pool address mask 255.255.0.0
Commander mac 00e0.0f2b.6000 is up, hold time 79.880 second

When there is inaccessible mumber, the display of the command switch is as follows：

switch_A#show cluster
Commander of cluster "zmz"
Total number of members: 2
Hello timer 8
Hold timer 80
Topologic discovery hops 3
Address pool net address 192.166.0.0
Address pool address mask 255.255.0.0
Member 1(mac 00e0.0f2b.626d) is down

When there is inaccessible switch, the display of the command switch is as follows：

switch_B#show cluster
Member 1 of cluster "zmz"
Total number of members: 2
Hello timer 8
Hold timer 80
Topologic discovery hops 3
Address pool net address 192.166.0.0
Address pool address mask 255.255.0.0
Commander mac 00e0.0f2b.6000 is down

When configured cluster backup group, the display of the command switch is as follows：

cmdr_config#show cluster
Commander of cluster "zmz"
Total number of members: 3
Redundancy: Enabled
Standby type: hsrp
Standby Group: mytest

Standby Group Number: 1
Hello timer 8
Hold timer 80
Topologic discovery hops 3
Address pool net address 192.166.0.0
Address pool address mask 255.255.0.0
Member 1(mac 00e0.0f50.806c) is up, hold time 76.750 second
Member 2(mac 00e0.0f2b.626d) is up, hold time 76.750 second

When configured cluster backup group, the display of the backup command switch is as follows：

bakup_config#**show cluster**
Member 2(Standby command switch) of cluster "zmz"
Total number of members: 3
Hello timer 8
Hold timer 80
Topologic discovery hops 3
Address pool net address 192.166.0.0
Address pool address mask 255.255.0.0
Commander mac 00e0.0f2b.6000 is up, hold time 74.210 second

71.1.9 show cluster candidate

description

show cluster candidates [detail | mac-address *H.H.H*]

parameter

parameter	description
detail	Displays the detailed information of all candidate members.
mac-address *H.H.H*	Displays candidate member information of the specified mac address.

default

none

instruction

This command is used to display candidate member information in the cluster. The displayable information include: member mac address, device name, up-link device, interface and so on. This command can only be executed on the command switch.

example

The example of command execution：

switch_A#show cluster candidates

ID MAC addr Name Device Type

256 00e0.0f2b.626d switch_B switch Local interface: f0/2(2), Uplink interface: f0/2(2), Uplink device id: 0 ,hops to edge: 1

The example of command execution when the MAC address is specified：

switch_A#show cluster candidates mac-address 00e0.0f2b.626d

Device 'switch_B' with mac address number 00e0.0f2b.626d

Device type: switch

Upstream MAC address: 00e0.0f2b.6000 (Cluster Member 0)

Local port: f0/2 FEC number:

Upstream port: f0/2 FEC Number:

Hops from cluster edge: 1

The example of command execution when detail is specified：

switch_A#show cluster candidates detail

Device 'switch_B' with mac address number 00e0.0f2b.626d

Device type: switch

Upstream MAC address: 00e0.0f2b.6000 (Cluster Member 0)

Local port: f0/2 FEC number:

Upstream port: f0/2 FEC Number:

Hops from cluster edge: 1

71.1.10 show cluster member

description

show cluster member [*n* | detail]

parameter

parameter	parameterinstruction
detail	Displays member’s detailed information.
n	Displays member of the specified number.

default

none

instruction

This command is used to display member information in the cluster. The displayable information include: MAC address of the mumber, name of machine, up-link equipment,

member status and so on. This command can only be executed on the command switch.

example

The example of command execution：

```
switch_A#show cluster member
ID MAC addr          Name      Device Type
0 00e0.0f2b.6000 switch_A switch
Device is commander
---------------------------------------------------------
1 00e0.0f2b.626d switch_B SWITCH
Local interface: f0/2(2), Uplink interface: f0/2(2), Uplink device id: 0 ,hops to cmdr: 1
---------------------------------------------------------
```

The example of command execution when member number is specified：

```
switch_A#show cluster member id 1
Device 'switch_B' with member number 1
        Device type:                SWITCH
        MAC address:                00e0.0f2b.626d
        Upstream MAC address:       00e0.0f2b.6000 (Cluster Member 0)
        Local port:                 f0/2      FEC number:
        Upstream port:              f0/2      FEC Number:
        Hops from command device: 1
```

The example of command execution when detail is specified：

```
switch_A#show cluster member detail
Device 'switch_A' with member number 0 (Command Switch)
        Device type:                SWITCH
        MAC address:                00e0.0f2b.6000
        Upstream MAC address:
        Local port:                           FEC number:
        Upstream port:                        FEC Number:
        Hops from command device: 0
Device 'switch_B' with member number 1
        Device type:                SWITCH
        MAC address:                00e0.0f2b.626d
        Upstream MAC address:       00e0.0f2b.6000 (Cluster Member 0)
        Local port:                 f0/2      FEC number:
        Upstream port:              f0/2      FEC Number:
        Hops from command device: 1
```

71.1.11 show cluster topo

description

show cluster topo

parameter

none

default

none

instruction

This command is used to display topology information in the cluster. The displayable information include: MAC address of member, machine name, up-link equipment and interface, member status and so on. This command can only be executed on the switch.

example

The example of command execution：

```
cmdr#show cluster topo
Total device number discoveried in session: 4
Total link number discoveried in session: 3
------------------------------------------------------------
ID MAC addr          Name      Device Type
258 00e0.0f46.606c sw1 SWITCH
Local interface: f0/7(7), Uplink interface: f0/24(24), Uplink device id: 1, hops to edge: 1
------------------------------------------------------------
256 00e0.0f28.006c sw3 SWITCH
Local interface: f0/2(2), Uplink interface: f0/18(18), Uplink device id: 0, hops to edge: 1
------------------------------------------------------------
0 00e0.0f2b.601b cmdr SWITCH
Device is commander
------------------------------------------------------------
1 00e0.0f50.8000 sw2 SWITCH
Local interface: f0/6(6), Uplink interface: f0/6(6), Uplink device id: 0, hops to cmdr: 1
------------------------------------------------------------
```

71.1.12 show cluster address pool

description

show cluster address pool

parameter

none

default

none

instruction

This command is used to display cluster address pool. This comman can only be operated on the switch.

example

The example of command execution：

```
cmdr#show cluster address pool
    Address pool net address          192.166.0.0
    Address pool address mask          255.255.0.0
```