CONTENT

CONTENT 1

CHAPTER 1 COMMANDS FOR BASIC SWITCH 1-1

1.1 Basic Switch 1-1
1.1.1 Basic Configuration 1-1
1.1.2 Telnet 1-17
1.1.3 Configuring Switch IP 1-27
1.1.4 SNMP 1-30
1.1.5 Switch Upgrade 1-44
1.1.6 Boot Configuration 1-50
1.2 File System 1-57
1.2.1 cd 1-57
1.2.2 copy 1-57
1.2.3 delete 1-58
1.2.4 dir 1-58
1.2.5 Format 1-59
1.2.6 mount 1-59
1.2.7 pwd 1-59
1.2.8 rename 1-59
1.2.9 unmount 1-60
1.3 Cluster 1-60
1.3.1 clear cluster nodes 1-60
1.3.2 cluster auto-add 1-60
1.3.3 cluster commander 1-60
1.3.4 cluster ip-pool 1-61
1.3.5 cluster keepalive interval 1-61
1.3.6 cluster keepalive loss-count 1-62
1.3.7 cluster member 1-62
1.3.8 cluster member auto-to-user 1-63
1.3.9 cluster reset member id 1-63
1.3.10 cluster run 1-64
1.3.11 cluster update member 1-64

1.3.12 debug cluster....1-65
1.3.13 debug cluster packets....1-65
1.3.14 show cluster....1-66
1.3.15 show cluster members....1-67
1.3.16 show cluster candidates....1-67
1.3.17 show cluster topology....1-68
1.3.18 rcommand commander....1-70
1.3.19 rcommand member....1-70
1.4 USB....1-71
1.4.1 cd usb:....1-71
1.4.2 dir....1-71
1.4.3 delete....1-71
1.4.4 rename....1-72
1.4.5 copy....1-72
1.5 Device Management....1-73
1.5.1 debug devsm....1-73
1.5.2 force runcfg-sync....1-73
1.5.3 force sync software-version....1-73
1.5.4 force switchover....1-73
1.5.5 reset slot....1-74
1.5.6 runcfg-sync....1-74
1.5.7 show fan....1-74
1.5.8 show power....1-74
1.5.9 show slot....1-75
1.5.10 show manage-plane context....1-75
1.5.11 debug cpmp....1-76
1.5.12 pull out slot....1-76

CHAPTER 2 NETWORK SECURITY....2-1

2.1 Network Security....2-1
2.1.1 default user password macbased....2-1
2.1.2 first-login change password....2-1
2.1.3 userpassword restriction....2-1
2.1.4 password valid-time....2-2
2.1.5 user-login failed msg....2-2
2.1.6 password feedback....2-3
2.1.7 password security-config....2-3

2.1.8 boot-file security check **2-3**
2.1.9 ssh-server dst-port **2-4**
2.1.10 telnet-server dst-port **2-4**
2.1.11 snmp-server dst-port **2-5**
2.1.12 ip http secure- ciphersuite **2-5**
2.1.13 ssh-server encryption-algorithm **2-6**
2.1.14 service password-encryption type user **2-6**
2.1.15 bfd authentication key md5 ..... **2-7**
2.1.16 enable password **2-7**
2.1.17 enable trustview key **2-8**
2.1.18 ip ftp **2-9**
2.1.19 ntp authentication-key **2-9**
2.1.20 password **2-9**
2.1.21 radius-server accounting host **2-10**
2.1.22 radius-server authentication host **2-11**
2.1.23 radius-server key **2-12**
2.1.24 tacacs-server authentication host **2-12**
2.1.25 tacacs-server key **2-13**
2.1.26 username **2-14**

CHAPTER 3 COMMANDS FOR LAYER 2 SERVICES 2-1

3.1 Port Configuration 2-1
3.1.1 Bandwidth **2-1**
3.1.2 clear counters interface **2-1**
3.1.3 description **2-2**
3.1.4 flow control **2-2**
3.1.5 hardware profile module fanout **2-3**
3.1.6 interface ethernet **2-3**
3.1.7 interface mode **2-3**
3.1.8 loopback **2-4**
3.1.9 media-type **2-4**
3.1.10 negotiation **2-4**
3.1.11 port-rate-statistics interval **2-4**
3.1.12 port-scan-mode **2-5**
3.1.13 port-status query interval **2-5**
3.1.14 rate-violation **2-5**
3.1.15 rate-violation all-bits **2-6**

3.1.16 rate-violation control 2-6
3.1.17 remote-statistics interval 2-7
3.1.18 show interface 2-7
3.1.19 shutdown 2-11
3.1.20 speed-duplex 2-11
3.1.21 storm-control 2-12
3.1.22 virtual-cable-test 2-13
3.1.23 switchport discard packet 2-14
3.1.24 switchport flood-control 2-14
3.1.25 switchport flood-forwarding 2-15
3.2 Port Isolation 2-15
3.2.1 isolate-port group 2-15
3.2.2 isolate-port group switchport interface 2-16
3.2.3 isolate-port apply 2-16
3.2.4 show isolate-port group 2-17
3.3 Port Loopback Detection 2-17
3.3.1 debug loopback-detection 2-17
3.3.2 loopback-detection control 2-18
3.3.3 loopback-detection control-recovery timeout 2-18
3.3.4 loopback-detection interval-time 2-19
3.3.5 loopback-detection trap enable 2-19
3.3.6 loopback-detection specified-vlan 2-19
3.3.7 loopback-detection send packet number 2-20
3.3.8 show loopback-detection 2-20
3.4 ULDP 2-21
3.4.1 debug uldp 2-21
3.4.2 debug uldp error 2-21
3.4.3 debug uldp event 2-22
3.4.4 debug uldp fsm interface ethernet 2-22
3.4.5 debug uldp interface ethernet 2-22
3.4.6 debug uldp packet 2-23
3.4.7 uldp aggressive-mode 2-23
3.4.8 uldp enable 2-23
3.4.9 uldp disable 2-24
3.4.10 uldp hello-interval 2-24
3.4.11 uldp manual-shutdown 2-24
3.4.12 uldp recovery-time 2-25
3.4.13 uldp reset 2-25

3.4.14 show uldp....2-25
3.5 LLDP....2-26
3.5.1 clear lldp remote-table....2-26
3.5.2 debug lldp....2-26
3.5.3 debug lldp packets....2-26
3.5.4 lldp enable....2-27
3.5.5 lldp enable (Port)....2-27
3.5.6 lldp management-address tlv....2-27
3.5.7 lldp mode....2-28
3.5.8 lldp msgTxHold....2-28
3.5.9 lldp neighbors max-num....2-28
3.5.10 lldp notification interval....2-29
3.5.11 lldp tooManyNeighbors....2-29
3.5.12 lldp transmit delay....2-29
3.5.13 lldp transmit optional tlv....2-30
3.5.14 lldp trap....2-30
3.5.15 lldp tx-interval....2-30
3.5.16 show debugging lldp....2-31
3.5.17 show lldp....2-31
3.5.18 show lldp interface ethernet....2-32
3.5.19 show lldp neighbors interface ethernet....2-32
3.5.20 show lldp traffic....2-33
3.6 LLDP-MED....2-33
3.6.1 civic location....2-33
3.6.2 {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}....2-34
3.6.3 ecs location....2-34
3.6.4 lldp med fast count....2-35
3.6.5 lldp med trap....2-35
3.6.6 lldp transmit med tlv all....2-35
3.6.7 lldp transmit med tlv capability....2-36
3.6.8 lldp transmit med tlv extendPoe....2-36
3.6.9 lldp transmit med tlv location....2-37
3.6.10 lldp transmit med tlv inventory....2-37
3.6.11 lldp transmit med tlv networkPolicy....2-37
3.6.12 network policy....2-38
3.6.13 show lldp....2-39
3.6.14 show lldp [interface ethernet <IFNAME>]....2-39

3.6.15 show lldp neighbors 2-40
3.6.16 show lldp traffic 2-41
3.7 Port Channel 2-41
3.7.1 debug port-channel 2-41
3.7.2 interface port-channel 2-42
3.7.3 lacp port-priority 2-42
3.7.4 lacp system-priority 2-42
3.7.5 lacp timeout 2-43
3.7.6 load-balance 2-43
2.7.7 load-balance hash-field 2-43
3.7.8 load-balance hash-random 2-44
3.7.9 load-balance ingress-port 2-44
3.7.10 load-balance hash-shift 2-45
3.7.11 load-balance enhanced profile 2-45
3.7.12 l2 field 2-45
3.7.13 l2 mpls field l2payload 2-45
3.7.14 l2 mpls field l3payload 2-45
3.7.15 ipv4 field 2-45
3.7.16 ipv6 field 2-45
3.7.17 l3 mpls field 2-45
3.7.18 mpls tunnel field 2-46
3.7.19 mim field l2payload 2-46
3.7.20 mim field l3payload 2-46
3.7.21 mim tunnel field 2-46
3.7.22 trill field l2payload 2-46
3.7.23 trill field l3payload 2-46
3.7.24 trill tunnel field l2payload 2-46
3.7.25 trill tunnel field l3payload 2-46
3.7.26 trill tunnel field outerl2 2-46
3.7.27 port-group 2-46
3.7.28 port-group mode 2-47
3.7.29 show port-group 2-47
3.7.30 show load-balance enhanced-profile 2-49
3.8 MTU 2-49
3.8.1 mtu 2-49
3.9 bpdu-tunnel 2-50
3.9.1 bpdu-tunnel dmac 2-50
3.9.2 bpdu-tunnel stp 2-50

3.9.3 bpdu-tunnel gvrp....2-50
3.9.4 bpdu-tunnel uldp....2-51
3.9.5 bpdu-tunnel lacp....2-51
3.9.6 bpdu-tunnel dot1x....2-51
3.9.7 bpdu-tunnel-protocol....2-52
3.9.8 bpdu-tunnel-protocol group-mac....2-52
3.9.9 bpdu-tunnel-protocol protocol-mac....2-52
3.9.10 bpdu-tunnel-protocol ethernetii....2-52
3.9.11 bpdu-tunnel-protocol snap....2-52
3.9.12 bpdu-tunnel-protocol llc....2-52
3.10 DDM....2-52
3.10.1 clear transceiver threshold-violation....2-52
3.10.2 debug transceiver....2-53
3.10.3 show transceiver....2-53
3.10.4 show transceiver threshold-violation....2-53
3.10.5 transceiver-monitoring....2-54
3.10.6 transceiver-monitoring interval....2-54
3.10.7 transceiver threshold....2-55
3.10.8 optician monitor enable|disable....2-56
3.11 EFM OAM....2-56
3.11.1 clear ethernet-oam....2-56
3.11.2 debug ethernet-oam error....2-56
3.11.3 debug ethernet-oam event....2-57
3.11.4 debug ethernet-oam fsm....2-57
3.11.5 debug ethernet-oam packet....2-57
3.11.6 debug ethernet-oam timer....2-57
3.11.7 ethernet-oam....2-58
3.11.8 ethernet-oam errored-frame threshold high....2-58
3.11.9 ethernet-oam errored-frame threshold low....2-59
3.11.10 ethernet-oam errored-frame window....2-59
3.11.11 ethernet-oam errored-frame-period threshold high....2-59
3.11.12 ethernet-oam errored-frame-period threshold low....2-60
3.11.13 ethernet-oam errored-frame-period window....2-60
3.11.14 ethernet-oam errored-frame-seconds threshold high....2-61
3.11.15 ethernet-oam errored-frame-seconds threshold low....2-61
3.11.16 ethernet-oam errored-frame-seconds window....2-62
3.11.17 ethernet-oam errored-symbol-period threshold high....2-62
3.11.18 ethernet-oam errored-symbol-period threshold low....2-63

3.11.19 ethernet-oam errored-symbol-period window 2-63
3.11.20 ethernet-oam link-monitor 2-63
3.11.21 ethernet-oam mode 2-64
3.11.22 ethernet-oam period 2-64
3.11.23 ethernet-oam remote-failure 2-64
3.11.24 ethernet-oam remote-loopback 2-65
3.11.25 ethernet-oam remote-loopback supported 2-65
3.11.26 ethernet-oam timeout 2-66
3.11.27 show ethernet-oam 2-66
3.11.28 show ethernet-oam events 2-70
3.11.29 show ethernet-oam link-events-configuration 2-72
3.11.30 show ethernet-oam loopback-status 2-72
3.12 PORT SECURITY 2-73
3.12.1 clear port-security 2-73
3.12.2 show port-security 2-74
3.12.3 switchport port-security 2-74
3.12.4 switchport port-security aging 2-74
3.12.5 switchport port-security mac-address 2-75
3.12.6 switchport port-security mac-address sticky 2-75
3.12.7 switchport port-security maximum 2-76
3.12.8 switchport port-security violation 2-76
3.13 VLAN 2-77
3.13.1 vlan 2-77
3.13.2 vlan internal 2-77
3.13.3 vlan ingress enable 2-78
3.13.4 switchport trunk native vlan 2-78
3.13.5 switchport trunk allowed vlan 2-78
3.13.6 switchport mode trunk allow-null 2-79
3.13.7 switchport mode 2-79
3.13.8 switchport interface 2-80
3.13.9 switchport hybrid native vlan 2-80
3.13.10 switchport hybrid allowed vlan 2-81
3.13.11 switchport forbidden vlan 2-81
3.13.12 switchport access vlan 2-82
3.13.13 show vlan 2-82
3.13.14 private-vlan association 2-84
3.13.15 private-vlan 2-84
3.13.16 name 2-85

3.13.17 Vlan-flow-statistics 2-85
3.14 GVRP 2-87
3.14.1 garp timer join 2-87
3.14.2 garp timer leave 2-87
3.14.3 garp timer leaveAll 2-87
3.14.4 gvrp (Global) 2-87
3.14.5 gvrp (Port) 2-88
3.14.6 no garp timer 2-88
3.14.7 show garp timer 2-88
3.14.8 show gvrp fsm information 2-89
3.14.9 show gvrp leaveAll fsm information 2-89
3.14.10 show gvrp leavetimer running information 2-90
3.14.11 show gvrp port-member 2-90
3.14.12 show gvrp port registerd vlan 2-91
3.14.13 show gvrp timer running information 2-91
3.14.14 show gvrp vlan registerd port 2-92
3.14.15 debug gvrp event 2-92
3.14.16 debug gvrp packet 2-92
3.15 Dot1q-tunnel 2-93
3.15.1 dot1q-tunnel enable 2-93
3.15.2 dot1q-tunnel tpid 2-94
3.15.3 show dot1q-tunnel 2-94
3.16 VLAN translation 2-94
3.16.1 vlan-translation 2-94
3.16.2 vlan-translation enable 2-95
3.16.3 vlan-translation cvid 2-95
3.16.4 vlan-translation miss drop 2-96
3.16.5 show vlan-translation 2-96
3.17 Dynamic VLAN 2-97
3.17.1 dynamic-vlan mac-vlan prefer 2-97
3.17.2 dynamic-vlan subnet-vlan prefer 2-97
3.17.3 mac-vlan 2-98
3.17.4 mac-vlan vlan 2-98
3.17.5 protocol-vlan 2-98
3.17.6 show dynamic-vlan prefer 2-99
3.17.7 show mac-vlan 2-99
3.17.8 show mac-vlan interface 2-100
3.17.9 show protocol-vlan 2-100

3.17.10 show subnet-vlan **2-100**
3.17.11 show subnet-vlan interface **2-101**
3.17.12 subnet-vlan **2-101**
3.17.13 switchport mac-vlan enable **2-102**
3.17.14 switchport subnet-vlan enable **2-102**
3.18 Voice VLAN 2-103
3.18.1 show voice-vlan **2-103**
3.18.2 switchport voice-vlan enable **2-103**
3.18.3 voice-vlan **2-103**
3.18.4 voice-vlan vlan **2-103**
3.19 Multi-to-One VLAN Translation 2-104
3.19.1 vlan-translation n-to-1 ..... **2-104**
3.19.2 show vlan-translation n-to-1 ..... **2-105**
3.20 Super VLAN 2-105
3.20.1 supervlan **2-105**
3.20.2 subvlan **2-105**
3.20.3 arp-proxy subvlan **2-106**
3.20.4 ip-addr-range subvlan **2-106**
3.20.5 ip-addr-range **2-107**
3.20.6 show supervlan **2-107**
3.21 MAC Address Table 2-108
3.21.1 mac-address-table avoid-collision **2-108**
3.21.2 clear collision-mac-address-table **2-108**
3.21.3 clear mac-address-table dynamic **2-108**
3.21.4 mac-address-learning cpu-control **2-108**
3.21.5 mac-address-table aging-time **2-109**
3.21.6 mac-address-table static | static-multicast | blackhole **2-109**
3.21.7 l2-address-table static-multicast address **2-110**
3.21.8 show collision-mac-address-table **2-110**
3.21.9 show mac-address-table **2-111**
3.21.10 Show l2-address-table multicast **2-111**
3.22 MAC Notification 2-111
3.22.1 clear mac-notification statistics **2-111**
3.22.2 mac-address-table notification **2-111**
3.22.3 mac-address-table notification history-size **2-112**
3.22.4 mac-address-table notification interval **2-112**
3.22.5 mac-notification **2-112**
3.22.6 show mac-notification summary **2-113**

3.22.7 snmp-server enable traps mac-notification 2-113
3.23 Commands for CFM OAM 2-114
3.23.1 clear ethernet cfm 2-114
3.23.2 continuity-check 2-114
3.23.3 continuity-check interval 2-114
3.23.4 continuity-check receive 2-115
3.23.5 cos 2-115
3.23.6 debug ethernet cfm 2-116
3.23.7 debug ethernet cfm error 2-117
3.23.8 debug ethernet cfm operation 2-117
3.23.9 ethernet cfm alarm 2-117
3.23.10 ethernet cfm auto-traceroute cache 2-118
3.23.11 ethernet cfm domain 2-118
3.23.12 ethernet cfm global 2-119
3.23.13 ethernet cfm logging 2-119
3.23.14 ethernet cfm mep 2-119
3.23.15 ethernet cfm mip 2-120
3.23.16 ethernet cfm mode 2-121
3.23.17 ethernet cfm pvlan 2-121
3.23.18 ethernet cfm snmp-server enable traps 2-121
3.23.19 ethernet cfm y1731 global 2-122
3.23.20 id 2-122
3.23.21 mep mepid 2-122
3.23.22 mip auto-create 2-123
3.23.23 ping ethernet 2-124
3.23.24 sender-id 2-125
3.23.25 service 2-125
3.23.26 show ethernet cfm domain 2-126
3.23.27 show ethernet cfm errors 2-127
3.23.28 show ethernet cfm maintenance-points local 2-128
3.23.29 show ethernet cfm maintenance-points remote 2-130
3.23.30 show ethernet cfm maintenance-points remote detail 2-131
3.23.31 show ethernet cfm mpdb 2-132
3.23.32 show ethernet cfm service 2-133
3.23.33 show ethernet cfm statistic 2-134
3.23.34 show ethernet cfm status 2-136
3.23.35 show ethernet cfm traceroute-reply auto 2-136
3.23.36 show ethernet cfm vlan table 2-137

3.23.37 switchport ulpp group <group-id> track cfm cc level <level-value>2-138
3.23.38 traceroute ethernet 2-138
3.23.39 traceroute ethernet auto..... 2-139

CHAPTER 4 COMMANDS FOR IP SERVICES 2-1

4.1 Layer 3 Interface..... 2-1
4.1.1 Bandwidth 2-1
4.1.2 description 2-1
4.1.3 description (VRF mode) 2-1
4.1.4 interface loopback 2-2
4.1.5 mac-address 2-2
4.1.6 interface vlan 2-3
4.1.7 ip vrf 2-3
4.1.8 ip vrf forwarding vrfName 2-3
4.1.9 no interface IFNAME 2-4
4.1.10 rd 2-4
4.1.11 route-target 2-4
4.1.12 show ip route 2-5
4.1.13 show ip route vrf 2-6
4.1.14 show ip vrf 2-7
4.1.15 shutdown 2-7
4.2 Network management port..... 2-8
4.2.1 duplex 2-8
4.2.2 interface ethernet 2-8
4.2.3 ip address 2-8
4.2.4 shutdown 2-8
4.2.5 speed 2-9
4.3 IP Configuration..... 2-9
4.3.1 clear ip traffic 2-9
4.3.2 clear ipv6 neighbor 2-9
4.3.3 debug ip icmp 2-10
4.3.4 debug ip packet 2-10
4.3.5 debug ipv6 packet 2-10
4.3.6 debug ipv6 icmp 2-11
4.3.7 debug ipv6 nd 2-11
4.3.8 debug ipv6 tunnel packet 2-12
4.3.9 description 2-13

4.3.10 ip address **2-13**
4.3.11 ip default-gateway **2-13**
4.3.12 ip route **2-13**
4.3.13 ipv6 address **2-14**
4.3.14 ipv6 default-gateway **2-14**
4.3.15 ipv6 route **2-14**
4.3.16 ipv6 redirect **2-15**
4.3.17 ipv6 nd dad attempts **2-15**
4.3.18 ipv6 nd ns-interval **2-16**
4.3.19 ipv6 nd suppress-ra **2-16**
4.3.20 ipv6 nd ra-lifetime **2-16**
4.3.21 ipv6 nd min-ra-interval **2-17**
4.3.22 ipv6 nd max-ra-interval **2-17**
4.3.23 ipv6 nd prefix **2-17**
4.3.24 ipv6 nd ra-hoplimit **2-18**
4.3.25 ipv6 nd ra-mtu **2-18**
4.3.26 ipv6 nd reachable-time **2-18**
4.3.27 ipv6 nd retrans-timer **2-19**
4.3.28 ipv6 nd other-config-flag **2-19**
4.3.29 ipv6 nd managed-config-flag **2-19**
4.3.30 ipv6 neighbor **2-20**
4.3.31 interface tunnel **2-20**
4.3.32 show ip interface **2-20**
4.3.33 show ip traffic **2-21**
4.3.34 show ipv6 interface **2-22**
4.3.35 show ipv6 route **2-24**
4.3.36 show ipv6 neighbors **2-25**
4.3.37 show ipv6 traffic **2-26**
4.3.38 show ipv6 redirect **2-27**
4.3.39 show ipv6 tunnel **2-27**
4.3.40 tunnel source **2-28**
4.3.41 tunnel destination **2-28**
4.3.42 tunnel nexthop **2-28**
4.3.43 tunnel 6to4-relay **2-29**
4.3.44 tunnel mode **2-29**
4.4 IP Forwarding 2-29
4.4.1 ip fib optimize **2-29**
4.5 URPF 2-30

4.5.1 debug urpf....2-30
4.5.2 ip urpf enable....2-30
4.5.3 show urpf rule ipv4 num....2-30
4.5.4 show urpf rule ipv6 num....2-30
4.5.5 show urpf rule ipv4....2-30
4.5.6 show urpf rule ipv6....2-30
4.5.7 show urpf....2-31
4.5.8 urpf enable....2-31
4.6 ARP....2-31
4.6.1 arp....2-31
4.6.2 clear arp-cache....2-32
4.6.3 clear arp traffic....2-32
4.6.4 debug arp....2-32
4.6.5 clear ip arp dynamic....2-33
4.6.6 clear ipv6 nd dynamic....2-33
4.6.7 ip proxy-arp....2-33
4.6.8 l3 hashselect....2-34
4.6.9 show arp....2-34
4.6.10 show arp traffic....2-34
4.7 station movement....2-35
4.7.1 l3-station-move....2-35
4.8 Hardware Tunnel Capacity....2-35
4.8.1 hardware tunnel-capacity....2-35
4.9 ARP Scanning Prevention....2-36
4.9.1 anti-arpscan enable [ip|port]....2-36
4.9.2 anti-arpscan port-based threshold....2-36
4.9.3 anti-arpscan ip-based threshold....2-36
4.9.4 anti-arpscan trust....2-37
4.9.5 anti-arpscan trust ip....2-37
4.9.6 anti-arpscan recovery enable....2-38
4.9.7 anti-arpscan recovery time....2-38
4.9.8 anti-arpscan log enable....2-38
4.9.9 anti-arpscan trap enable....2-39
4.9.10 anti-arpscan FFP max-num <num>....2-39
4.9.11 debug anti-arpscan....2-39
4.9.12 show anti-arpscan....2-40
4.9.13 show anti-arpscan ip-based attack-list [history]....2-41
4.9.14 show anti-arpscan ip-based running-config....2-42

4.10 Preventing ARP Spoofing....2-42
4.10.1 ip arp-security updateprotect....2-42
4.10.2 ip arp-security learnprotect....2-43
4.10.3 ip arp-security convert....2-43
4.11 ARP GUARD....2-44
4.11.1 arp-guard ip....2-44
4.12 ARP Local Proxy....2-44
4.12.1 ip local proxy-arp....2-44
4.13 Gratuitous ARP....2-45
4.13.1 ip gratuitous-arp....2-45
4.13.2 show ip gratuitous-arp....2-45
4.14 Keepalive Gateway....2-46
4.14.1 keepalive gateway....2-46
4.14.2 show ip interface....2-47
4.14.3 show keepalive gateway....2-47
4.15 Dynamic ARP Inspection....2-47
4.15.1 ip arp inspection....2-47
4.15.2 ip arp inspection port....2-48
4.15.3 ip arp inspection trust....2-48
4.15.4 ip arp inspection limit-rate....2-49
4.16 DHCP....2-49
4.16.1 DHCP Server....2-49
4.16.2 DHCP Relay....2-62
4.17 DHCP Option 82....2-64
4.17.1 debug ip dhcp relay packet....2-64
4.17.2 ip dhcp relay information option....2-64
4.17.3 ip dhcp relay information option delimiter....2-64
4.17.4 ip dhcp relay information option remote-id....2-65
4.17.5 ip dhcp relay information option remote-id format....2-65
4.17.6 ip dhcp relay information option self-defined remote-id....2-66
4.17.7 ip dhcp relay information option self-defined remote-id format....2-66
4.17.8 ip dhcp relay information option self-defined subscriber-id....2-67
4.17.9 ip dhcp relay information option self-defined subscriber-id format2-67
4.17.10 ip dhcp relay information option subscriber-id....2-68
4.17.11 ip dhcp relay information option subscriber-id format....2-68
4.17.12 ip dhcp relay information policy....2-69
4.17.13 ip dhcp server relay information enable....2-69
4.17.14 show ip dhcp relay information option....2-70

4.18 DHCP Snooping 2-70
4.18.1 debug ip dhcp snooping binding 2-70
4.18.2 debug ip dhcp snooping event.....2-71
4.18.3 debug ip dhcp snooping packet.....2-71
4.18.4 debug ip dhcp snooping packet interface 2-71
4.18.5 debug ip dhcp snooping ha.....2-71
4.18.6 debug ip dhcp snooping update 2-72
4.18.7 enable trustview key.....2-72
4.18.8 ip dhcp snooping 2-72
4.18.9 ip dhcp snooping action 2-72
4.18.10 ip dhcp snooping action MaxNum 2-73
4.18.11 ip dhcp snooping binding 2-73
4.18.12 ip dhcp snooping binding arp 2-74
4.18.13 ip dhcp snooping binding dot1x 2-74
4.18.14 ip dhcp snooping binding user 2-75
4.18.15 ip dhcp snooping binding user-control.....2-75
4.18.16 ip dhcp snooping binding user-control max-user 2-76
4.18.17 ip dhcp snooping information enable 2-76
4.18.18 ip dhcp snooping information option allow-untrusted (replace|)2-77
4.18.19 ip dhcp snooping information option delimiter.....2-77
4.18.20 ip dhcp snooping information option remote-id 2-78
4.18.21 ip dhcp snooping information option self-defined remote-id.....2-78
4.18.22 ip dhcp snooping information option self-defined remote-id format2-79
4.18.23 ip dhcp snooping information option self-defined subscriber-id2-79
4.18.24 ip dhcp snooping information option self-defined subscriber-id format 2-80
4.18.25 ip dhcp snooping information option subscriber-id format 2-80
4.18.26 ip dhcp snooping timeout detection.....2-81
4.18.27 ip dhcp snooping timeout quiet 2-81
4.18.28 ip dhcp snooping trust.....2-82
4.18.29 ip dhcp snooping vlan.....2-82
4.18.30 ip user helper-address 2-82
4.18.31 ip user private packet version two.....2-83
4.18.32 show ip dhcp snooping.....2-83
4.18.33 show ip dhcp snooping binding all.....2-86
4.18.34 show trustview status 2-87
4.19 DHCP option 60 and option 43 2-88
4.19.1 option 43 ascii LINE.....2-88

4.19.2 option 43 hex WORD 2-88
4.19.3 option 43 ip A.B.C.D.....2-88
4.19.4 option 60 ascii LINE.....2-89
4.19.5 option 60 hex WORD 2-89
4.19.6 option 60 ip A.B.C.D.....2-89

CHAPTER 5 COMMANDS FOR ROUTING PROTOCOL..... 2-1

5.1 Routing Protocol Overview.....2-1
5.1.1 ip prefix-list description 2-1
5.1.2 ip prefix-list seq.....2-1
5.1.3 ip prefix-list sequence-number 2-2
5.1.4 match as-path.....2-2
5.1.5 match community 2-3
5.1.6 match interface.....2-3
5.1.7 match ip.....2-3
5.1.8 match ipv6 address.....2-4
5.1.9 match ipv6 next-hop 2-4
5.1.10 match metric.....2-5
5.1.11 match origin.....2-5
5.1.12 match route-type 2-5
5.1.13 match tag 2-6
5.1.14 route-map.....2-6
5.1.15 set aggregator 2-7
5.1.16 set as-path 2-7
5.1.17 set atomic-aggregate.....2-8
5.1.18 set comm-list 2-8
5.1.19 set community.....2-8
5.1.20 set extcommunity.....2-9
5.1.21 set ip next-hop.....2-9
5.1.22 set local-preference 2-10
5.1.23 set metric 2-10
5.1.24 set metric-type.....2-10
5.1.25 set origin 2-11
5.1.26 set originator-id.....2-11
5.1.27 set tag.....2-11
5.1.28 set vpnv4 next-hop 2-12
5.1.29 set weight.....2-12

5.1.30 show ip prefix-list <list-name> 2-13
5.1.31 show ip prefix-list <detail | summary> 2-13
5.1.32 show route-map 2-14
5.1.33 show router-id 2-14
5.2 Static Route 2-15
5.2.1 ip route 2-15
5.2.2 ip route vrf 2-16
5.2.3 show ip route 2-16
5.2.4 show ip route vrf 2-17
5.2.5 show ip route fib 2-18
5.3 RIP 2-18
5.3.1 accept-lifetime 2-18
5.3.2 address-family ipv4 2-19
5.3.3 clear ip rip route 2-20
5.3.4 debug rip 2-20
5.3.5 debug rip redistribute message send 2-21
5.3.6 debug rip redistribute route receive 2-21
5.3.7 default-information originate 2-22
5.3.8 default-metric 2-22
5.3.9 distance 2-22
5.3.10 distribute-list 2-23
5.3.11 exit-address-family 2-23
5.3.12 ip rip aggregate-address 2-23
5.3.13 ip rip authentication key-chain 2-24
5.3.14 ip rip authentication mode 2-24
5.3.15 ip rip authentication string 2-25
5.3.16 ip rip authentication cisco-compatible 2-25
5.3.17 ip rip receive-packet 2-26
5.3.18 ip rip receive version 2-26
5.3.19 ip rip send-packet 2-26
5.3.20 ip rip send version 2-27
5.3.21 ip rip split-horizon 2-27
5.3.22 key 2-27
5.3.23 key chain 2-28
5.3.24 key-string 2-28
5.3.25 maximum-prefix 2-28
5.3.26 neighbor 2-29
5.3.27 network 2-29

5.3.28 offset-list **2-30**
5.3.29 passive-interface **2-30**
5.3.30 recv-buffer-size **2-30**
5.3.31 redistribute **2-31**
5.3.32 redistribute ospf (vrf command) **2-31**
5.3.33 route **2-31**
5.3.34 router rip **2-32**
5.3.35 send-lifetime **2-32**
5.3.36 show debugging rip **2-33**
5.3.37 show ip protocols rip **2-33**
5.3.38 show ip rip **2-34**
5.3.39 show ip rip database **2-35**
5.3.40 show ip rip database vrf **2-35**
5.3.41 show ip rip interface **2-35**
5.3.42 show ip rip interface vrf **2-36**
5.3.43 show ip rip aggregate **2-36**
5.3.44 show ip rip redistribute **2-37**
5.3.45 show ip vrf **2-37**
5.3.46 timers basic **2-38**
5.3.47 version **2-39**
5.4 OSPF 2-39
5.4.1 area authentication **2-39**
5.4.2 area default-cost **2-39**
5.4.3 area filter-list **2-40**
5.4.4 area nssa **2-40**
5.4.5 area range **2-41**
5.4.6 area stub **2-42**
5.4.7 area virtual-link **2-42**
5.4.8 auto-cost reference-bandwidth **2-43**
5.4.9 compatible rfc1583 ..... **2-43**
5.4.10 clear ip ospf process **2-44**
5.4.11 debug ospf events **2-44**
5.4.12 debug ospf ifsm **2-44**
5.4.13 debug ospf lsa **2-44**
5.4.14 debug ospf nfsm **2-45**
5.4.15 debug ospf nsm **2-45**
5.4.16 debug ospf packet **2-45**
5.4.17 debug ospf route **2-46**

5.4.18 debug ospf redistribute message send....2-46
5.4.19 debug ospf redistribute route receive....2-46
5.4.20 default-information originate....2-46
5.4.21 default-metric....2-47
5.4.22 distance....2-48
5.4.23 distribute-list....2-48
5.4.24 filter-policy....2-49
5.4.25 host area....2-49
5.4.26 ip ospf authentication....2-50
5.4.27 ip ospf authentication-key....2-50
5.4.28 ip ospf cost....2-50
5.4.29 ip ospf database-filter....2-51
5.4.30 ip ospf dead-interval....2-51
5.4.31 ip ospf disable all....2-52
5.4.32 ip ospf hello-interval....2-52
5.4.33 ip ospf message-digest-key....2-52
5.4.34 ip ospf mtu....2-53
5.4.35 ip ospf mtu-ignore....2-53
5.4.36 ip ospf network....2-54
5.4.37 ip ospf priority....2-54
5.4.38 ip ospf retransmit-interval....2-55
5.4.39 ip ospf transmit-delay....2-55
5.4.40 key....2-55
5.4.41 key chain....2-56
5.4.42 log-adjacency-changes detail....2-56
5.4.43 max-concurrent-dd....2-56
5.4.44 neighbor....2-57
5.4.45 network area....2-57
5.4.46 ospf abr-type....2-58
5.4.47 ospf router-id....2-58
5.4.48 overflow database....2-59
5.4.49 overflow database external....2-59
5.4.50 passive-interface....2-59
5.4.51 redistribute....2-60
5.4.52 redistribute ospf....2-60
5.4.53 router ospf....2-61
5.4.54 show ip ospf....2-61
5.4.55 show ip ospf border-routers....2-63

5.4.56 show ip ospf database 2-63
5.4.57 show ip ospf interface 2-64
5.4.58 show ip ospf neighbor 2-65
5.4.59 show ip ospf redistribute 2-65
5.4.60 show ip ospf route 2-66
5.4.61 show ip ospf virtual-links 2-67
5.4.62 show ip route process-detail 2-67
5.4.63 show ip route vrf process-detail 2-68
5.4.64 show ip protocols 2-68
5.4.65 summary-address 2-68
5.4.66 timers spf 2-69
5.5 BGP 2-69
5.5.1 address-family 2-69
5.5.2 aggregate-address 2-70
5.5.3 bgp aggregate-nexthop-check 2-71
5.5.4 bgp always-compare-med 2-71
5.5.5 bgp asnotation asdot 2-71
5.5.6 bgp bestpath as-path ignore 2-72
5.5.7 bgp bestpath compare-confed-aspath 2-72
5.5.8 bgp bestpath compare-routerid 2-73
5.5.9 bgp bestpath med 2-73
5.5.10 bgp client-to-client reflection 2-74
5.5.11 bgp cluster-id 2-74
5.5.12 bgp confederation identifier 2-74
5.5.13 bgp confederation peers 2-75
5.5.14 bgp dampening 2-75
5.5.15 bgp default 2-76
5.5.16 bgp deterministic-med 2-76
5.5.17 bgp enforce-first-as 2-76
5.5.18 bgp fast-external-failover 2-77
5.5.19 bgp inbound-route-filter 2-77
5.5.20 bgp inbound-max-route-num 2-77
5.5.21 bgp log-neighbor-changes 2-78
5.5.22 bgp network import-check 2-78
5.5.23 bgp rfc1771-path-select 2-78
5.5.24 bgp rfc1771-strict 2-79
5.5.25 bgp router-id 2-79
5.5.26 bgp scan-time 2-79

5.5.27 clear ip bgp 2-80
5.5.28 clear ip bgp dampening 2-80
5.5.29 clear ip bgp flap-statistics 2-80
5.5.30 debug bgp 2-81
5.5.31 debug bgp redistribute message send 2-81
5.5.32 debug bgp redistribute route receive 2-81
5.5.33 distance 2-82
5.5.34 distance bgp 2-82
5.5.35 exit-address-family 2-82
5.5.36 import map 2-83
5.5.37 ip as-path access-list 2-84
5.5.38 ip community-list 2-84
5.5.39 ip extcommunity-list 2-84
5.5.40 neighbor activate 2-85
5.5.41 neighbor advertisement-interval 2-85
5.5.42 neighbor allowas-in 2-86
5.5.43 neighbor as-override 2-86
5.5.44 neighbor attribute-unchanged 2-87
5.5.45 neighbor capability 2-87
5.5.46 neighbor capability orf prefix-list 2-88
5.5.47 neighbor collide-established 2-88
5.5.48 neighbor default-originate 2-89
5.5.49 neighbor description 2-89
5.5.50 neighbor distribute-list 2-90
5.5.51 neighbor dont-capability-negotiate 2-90
5.5.52 neighbor ebgp-multihop 2-91
5.5.53 neighbor enforce-multihop 2-91
5.5.54 neighbor filter-list 2-92
5.5.55 neighbor interface 2-92
5.5.56 neighbor maximum-prefix 2-93
5.5.57 neighbor next-hop-self 2-93
5.5.58 neighbor override-capability 2-94
5.5.59 neighbor passive 2-94
5.5.60 neighbor peer-group (Creating) 2-94
5.5.61 neighbor peer-group (Configuring group members) 2-95
5.5.62 neighbor port 2-95
5.5.63 neighbor prefix-list 2-96
5.5.64 neighbor remote-as 2-96

5.5.65 neighbor remove-private-AS 2-97
5.5.66 neighbor route-map 2-97
5.5.67 neighbor route-reflector-client 2-98
5.5.68 neighbor route-server-client 2-98
5.5.69 neighbor send-community 2-99
5.5.70 neighbor shutdown 2-99
5.5.71 neighbor soft-reconfiguration inbound 2-100
5.5.72 neighbor soo 2-100
5.5.73 neighbor strict-capability-match 2-101
5.5.74 neighbor timers 2-101
5.5.75 neighbor timers connect 2-101
5.5.76 neighbor unsuppress-map 2-102
5.5.77 neighbor update-source 2-102
5.5.78 neighbor version 4 2-103
5.5.79 neighbor weight 2-103
5.5.80 network (BGP) 2-104
5.5.81 redistribute (BGP) 2-104
5.5.82 redistribute ospf 2-104
5.5.83 router bgp 2-105
5.5.84 show ip bgp 2-105
5.5.85 show ip bgp attribute-info 2-106
5.5.86 show ip bgp community 2-106
5.5.87 show ip bgp community-info 2-107
5.5.88 show ip bgp community-list 2-107
5.5.89 show ip bgp dampening 2-108
5.5.90 show ip bgp filter-list 2-109
5.5.91 show ip bgp inconsistent-as 2-109
5.5.92 show ip bgp neighbors 2-110
5.5.93 show ip bgp paths 2-111
5.5.94 show ip bgp prefix-list 2-111
5.5.95 show ip bgp quote-regexp 2-111
5.5.96 show ip bgp redistribute 2-112
5.5.97 show ip bgp neighbors 2-112
5.5.98 show ip bgp regexp 2-112
5.5.99 show ip bgp route-map 2-113
5.5.100 show ip bgp scan 2-113
5.5.101 show ip bgp summary 2-114
5.5.102 show ip bgp view 2-115

5.5.103 show ip bgp view neighbors....2-115
5.5.104 show ip bgp vrf....2-115
5.5.105 show ip bgp vpnv4....2-117
5.5.106 timers bgp....2-118
5.6 IPv4 Black Hole Routing....2-118
5.6.1 ip route null0....2-118
5.7 GRE....2-119
5.7.1 debug gre....2-119
5.7.2 ip address....2-119
5.7.3 ip route....2-120
5.7.4 ipv6 address....2-120
5.7.5 ipv6 route....2-120
5.7.6 loopback-group (Global)....2-121
5.7.7 loopback-group (Port)....2-121
5.7.8 loopback-group (Tunnel Interface)....2-121
5.7.9 show gre tunnel....2-121
5.7.10 show interface tunnel....2-122
5.7.11 tunnel destination....2-122
5.7.12 tunnel mode gre ip....2-123
5.7.13 tunnel mode gre ipv6....2-123
5.7.14 tunnel source....2-123
5.8 ECMP....2-123
5.8.1 load-balance....2-123
5.8.2 maximum-paths....2-124
5.8.3 load-balance hash-shift....2-124
5.9 BFD....2-125
5.9.1 bfd authentication key....2-125
5.9.2 bfd authentication key md5|sm3....2-125
5.9.3 bfd authentication key text....2-126
5.9.4 bfd echo....2-126
5.9.5 bfd echo-source-ip....2-126
5.9.6 bfd echo-source-ipv6....2-127
5.9.7 bfd enable....2-127
5.9.8 bfd interval....2-128
5.9.9 bfd min-echo-recv-interval....2-128
5.9.10 bfd mode....2-129
5.9.11 debug bfd....2-129
5.9.12 ip ospf bfd enable....2-129

5.9.13 ip route bfd 2-130
5.9.14 ipv6 ospf bfd enable 2-130
5.9.15 ipv6 ospf bfd enable instance-id 2-130
5.9.16 ipv6 rip bfd enable 2-131
5.9.17 ipv6 route bfd 2-131
5.9.18 neighbor 2-131
5.9.19 rip bfd enable 2-132
5.9.20 show bfd neighbor 2-132
5.10 BGP GR 2-133
5.10.1 bgp graceful-restart 2-133
5.10.2 bgp graceful-restart restart-time 2-133
5.10.3 bgp graceful-restart stale-path-time 2-134
5.10.4 bgp selection-deferral-time 2-134
5.10.5 neighbor capability graceful-restart 2-134
5.11 OSPF GR 2-135
5.11.1 capability restart graceful 2-135
5.11.2 debug ospf events gr 2-135
5.11.3 ospf graceful-restart grace-period 2-136
5.11.4 ospf graceful-restart helper max-grace-period 2-136
5.11.5 ospf graceful-restart helper never 2-136
5.11.6 show ip ospf 2-137
5.11.7 show ip ospf graceful-restart 2-137

CHAPTER 6 COMMANDS FOR MULTICAST PROTOCOL 2-1

6.1 Multicast 2-1
6.1.1 show ip mroute 2-1
6.2 PIM-DM 2-2
6.2.1 debug pim timer sat 2-2
6.2.2 debug pim timer srt 2-2
6.2.3 ip mroute 2-2
6.2.4 ip pim bsr-border 2-3
6.2.5 ip pim dense-mode 2-3
6.2.6 ip pim dr-priority 2-3
6.2.7 ip pim exclude-genid 2-4
6.2.8 ip pim hello-holdtime 2-4
6.2.9 ip pim hello-interval 2-5
6.2.10 ip pim multicast-routing 2-5

6.2.11 ip pim neighbor-filter 2-5
6.2.12 ip pim scope-border 2-6
6.2.13 ip pim state-refresh origination-interval 2-6
6.2.14 show ip pim interface 2-7
6.2.15 show ip pim mroute dense-mode 2-7
6.2.16 show ip pim neighbor 2-9
6.2.17 show ip pim nexthop 2-9
6.3 PIM-SM 2-10
6.3.1 clear ip pim bsr rp-set 2-10
6.3.2 debug pim event 2-10
6.3.3 debug pim mfc 2-10
6.3.4 debug pim mib 2-11
6.3.5 debug pim nexthop 2-11
6.3.6 debug pim nsm 2-11
6.3.7 debug pim packet 2-12
6.3.8 debug pim state 2-12
6.3.9 debug pim timer 2-12
6.3.10 ip mroute 2-13
6.3.11 ip multicast unresolved-cache aging-time 2-14
6.3.12 ip pim accept-register 2-14
6.3.13 ip pim bsr-border 2-15
6.3.14 ip pim bsr-candidate 2-15
6.3.15 ip pim cisco-register-checksum 2-15
6.3.16 ip pim dr-priority 2-16
6.3.17 ip pim exclude-genid 2-16
6.3.18 ip pim hello-holdtime 2-16
6.3.19 ip pim hello-interval 2-17
6.3.20 ip pim ignore-rp-set-priority 2-17
6.3.21 ip pim jp-timer 2-18
6.3.22 ip pim multicast-routing 2-18
6.3.23 ip pim neighbor-filter 2-18
6.3.24 ip pim register-rate-limit 2-19
6.3.25 ip pim register-rp-reachability 2-19
6.3.26 ip pim register-source 2-20
6.3.27 ip pim register-suppression 2-20
6.3.28 ip pim rp-address 2-20
6.3.29 ip pim rp-candidate 2-21
6.3.30 ip pim rp-register-kat 2-21

6.3.31 ip pim scope-border 2-22
6.3.32 ip pim sparse-mode 2-22
6.3.33 show ip pim bsr-router 2-22
6.3.34 show ip pim interface 2-23
6.3.35 show ip pim mroute sparse-mode 2-24
6.3.36 show ip pim neighbor 2-25
6.3.37 show ip pim nexthop 2-25
6.3.38 show ip pim rp-hash 2-26
6.3.39 show ip pim rp mapping 2-26
6.4 MSDP 2-27
6.4.1 cache-sa-holdtime 2-27
6.4.2 cache-sa-maximum 2-27
6.4.3 cache-sa-state 2-28
6.4.4 clear msdp peer 2-28
6.4.5 clear msdp sa-cache 2-28
6.4.6 clear msdp statistics 2-29
6.4.7 connect-source 2-29
6.4.8 debug msdp all 2-29
6.4.9 debug msdp events 2-30
6.4.10 debug msdp filter 2-30
6.4.11 debug msdp fsm 2-30
6.4.12 debug msdp keepalive 2-31
6.4.13 debug msdp nsm 2-31
6.4.14 debug msdp packet 2-31
6.4.15 debug msdp peer 2-32
6.4.16 debug msdp timer 2-32
6.4.17 default-rpf-peer 2-32
6.4.18 description 2-33
6.4.19 exit-peer-mode 2-33
6.4.20 mesh-group 2-33
6.4.21 originating-rp 2-34
6.4.22 peer 2-34
6.4.23 redistribute 2-35
6.4.24 remote-as 2-35
6.4.25 router msdp 2-35
6.4.26 sa-filter 2-36
6.4.27 sa-request 2-36
6.4.28 sa-request-filter 2-37

6.4.29 show msdp global....2-37
6.4.30 show msdp local-sa-cache....2-38
6.4.31 show msdp peer....2-39
6.4.32 show msdp sa-cache....2-40
6.4.33 show msdp sa-cache summary....2-41
6.4.34 show msdp statistics....2-41
6.4.35 show msdp summary....2-42
6.4.36 shutdown....2-43
6.4.37 ttl-threshold....2-43
6.5 ANYCAST RP....2-44
6.5.1 debug pim anycast-rp....2-44
6.5.2 ip pim anycast-rp....2-44
6.5.3 ip pim anycast-rp....2-44
6.5.4 ip pim anycast-rp self-rp-address....2-45
6.5.5 ip pim rp-candidate....2-46
6.5.6 show debugging pim....2-46
6.5.7 show ip pim anycast-rp first-hop....2-46
6.5.8 show ip pim anycast-rp non-first-hop....2-47
6.5.9 show ip pim anycast-rp status....2-48
6.6 PIM-SSM....2-48
6.6.1 ip multicast ssm....2-48
6.7 DVMRP....2-49
6.7.1 debug dvmrp....2-49
6.7.2 ip dvmrp enable....2-50
6.7.3 ip dvmrp metric....2-50
6.7.4 ip dvmrp multicast-routing....2-51
6.7.5 ip dvmrp output-report-delay....2-51
6.7.6 ip dvmrp reject-non-pruners....2-51
6.7.7 ip dvmrp tunnel....2-52
6.7.8 show ip dvmrp....2-52
6.7.9 show ip dvmrp interface....2-53
6.7.10 show ip dvmrp neighbor....2-53
6.7.11 show ip dvmrp prune....2-54
6.7.12 show ip dvmrp route....2-54
6.8 DCSCM....2-55
6.8.1 access-list (Multicast Destination Control)....2-55
6.8.2 access-list (Multicast Source Control)....2-56
6.8.3 ip multicast destination-control....2-57

6.8.4 ip multicast destination-control access-group (sip) 2-57
6.8.5 ip multicast destination-control access-group (vmac) 2-57
6.8.6 ip multicast policy 2-58
6.8.7 ip multicast source-control 2-58
6.8.8 ip multicast source-control access-group 2-59
6.8.9 multicast destination-control 2-59
6.8.10 profile-id (Multicast Destination Control Rule List) 2-60
6.8.11 show ip multicast destination-control 2-60
6.8.12 show ip multicast destination-control access-list 2-61
6.8.13 show ip multicast destination-control filter-profile-list 2-61
6.8.14 show ip multicast policy 2-62
6.8.15 show ip multicast source-control 2-62
6.8.16 show ip multicast source-control access-list 2-62
6.9 IGMP 2-63
6.9.1 clear ip igmp group 2-63
6.9.2 debug igmp event 2-63
6.9.3 debug igmp snooping all/packet/event/timer/mfc/authentication/ha 2-63
6.9.4 ip igmp access-group 2-64
6.9.5 ip igmp immediate-leave 2-64
6.9.6 ip igmp join-group 2-65
6.9.7 ip igmp last-member-query-interval 2-65
6.9.8 ip igmp limit 2-65
6.9.9 ip igmp query-interval 2-66
6.9.10 ip igmp query-max-response-time 2-66
6.9.11 ip igmp query-timeout 2-67
6.9.12 ip igmp robust-variable 2-67
6.9.13 ip igmp static-group 2-67
6.9.14 ip igmp version 2-68
6.9.15 show ip igmp groups 2-68
6.9.16 show ip igmp interface 2-69
6.10 IGMP Snooping 2-70
6.10.1 clear ip igmp snooping vlan 2-70
6.10.2 clear ip igmp snooping vlan <1-4094> mrouter-port 2-70
6.10.3 debug igmp snooping all/packet/event/timer/mfc 2-71
6.10.4 ip igmp snooping 2-71
6.10.5 ip igmp snooping proxy 2-71
6.10.6 ip igmp snooping vlan 2-72
6.10.7 ip igmp snooping vlan immediate-leave 2-72

6.10.8 ip igmp snooping vlan <id> immediately-leave mac-based.....2-72
6.10.9 ip igmp snooping vlan l2-general-querier.....2-73
6.10.10 ip igmp snooping vlan l2-general-querier-source.....2-73
6.10.11 ip igmp snooping vlan l2-general-querier-version.....2-74
6.10.12 ip igmp snooping vlan limit.....2-74
6.10.13 ip igmp snooping vlan interface (ethernet | port-channel|) IFNAME limit.....2-75
6.10.14 ip igmp snooping vlan mrouter-port interface.....2-75
6.10.15 ip igmp snooping vlan mrouter-port learnpim.....2-76
6.10.16 ip igmp snooping vlan mrpt.....2-76
6.10.17 ip igmp snooping vlan query-interval.....2-76
6.10.18 ip igmp snooping vlan query-mrsp.....2-77
6.10.19 ip igmp snooping vlan query-robustness.....2-77
6.10.20 ip igmp snooping vlan report source-address.....2-78
6.10.21 ip igmp snooping vlan specific-query-mrsp.....2-78
6.10.22 ip igmp snooping vlan static-group.....2-78
6.10.23 ip igmp snooping vlan passthrough-group.....2-79
6.10.24 ip igmp snooping vlan not-forward.....2-79
6.10.25 ip igmp snooping vlan suppression-query-time.....2-80
6.10.26 show ip igmp snooping.....2-80
6.11 IGMP Proxy.....2-81
6.11.1 clear ip igmp proxy agggroup.....2-81
6.11.2 debug igmp proxy all.....2-82
6.11.3 debug igmp proxy event.....2-82
6.11.4 debug igmp proxy mfc.....2-82
6.11.5 debug igmp proxy packet.....2-83
6.11.6 debug igmp proxy timer.....2-83
6.11.7 ip igmp proxy.....2-83
6.11.8 ip igmp proxy aggregate.....2-84
6.11.9 ip igmp proxy downstream.....2-84
6.11.10 ip igmp proxy limit.....2-84
6.11.11 ip igmp proxy multicast-source.....2-85
6.11.12 ip igmp proxy unsolicited-report interval.....2-85
6.11.13 ip igmp proxy unsolicited-report robustness.....2-85
6.11.14 ip igmp proxy upstream.....2-86
6.11.15 ip multicast ssm.....2-86
6.11.16 ip pim bsr-border.....2-87
6.11.17 show debugging igmp proxy.....2-87

6.11.18 show ip igmp proxy 2-87
6.11.19 show ip igmp proxy mroute 2-88
6.11.20 show ip igmp proxy upstream groups 2-89
6.12 Multicast VLAN 2-89
6.12.1 multicast-vlan 2-89
6.12.2 multicast-vlan association 2-90
6.12.3 multicast-vlan association interface 2-90
6.12.4 multicast-vlan mode 2-91
6.12.5 switchport association multicast-vlan 2-91

CHAPTER 7 COMMANDS FOR SECURITY FUNCTION 2-1

7.1 ACL 2-1
7.1.1 absolute-periodic/periodic 2-1
7.1.2 absolute start 2-2
7.1.3 access-list deny-preemption 2-2
7.1.4 access-list (ip extended) 2-2
7.1.5 access-list (ip standard) 2-4
7.1.6 access-list(mac extended) 2-4
7.1.7 access-list(mac-ip extended) 2-5
7.1.8 access-list(mac standard) 2-7
7.1.9 clear access-group 2-8
7.1.10 firewall 2-8
7.1.11 ip access extended 2-8
7.1.12 ip access standard 2-8
7.1.13 ipv6 access-list 2-9
7.1.14 ipv6 access standard 2-10
7.1.15 ipv6 access extended 2-10
7.1.16 {ip|ipv6|mac|mac-ip} access-group 2-11
7.1.17 {ip|ipv6|mac|mac-ip} access-group (Interface Mode) 2-12
7.1.18 mac access extended 2-12
7.1.19 mac-ip access extended 2-12
7.1.20 permit | deny (ip extended) 2-12
7.1.21 permit | deny(ip standard) 2-13
7.1.22 permit | deny(ipv6 extended) 2-14
7.1.23 permit | deny(ipv6 standard) 2-15
7.1.24 permit | deny(mac extended) 2-15
7.1.25 permit | deny(mac-ip extended) 2-16

7.1.26 show access-lists....2-18
7.1.27 show access-group....2-19
7.1.28 show firewall....2-20
7.1.29 show ipv6 access-lists....2-20
7.1.30 show time-range....2-21
7.1.31 time-range....2-21
7.2 Self-defined ACL....2-22
7.2.1 permit | deny....2-22
7.2.2 udf-access-list standard....2-22
7.2.3 userdefined-access-list standard offset....2-22
7.2.4 userdefined-access-list extended offset....2-23
7.2.5 userdefined-access-list standard....2-23
7.2.6 userdefined-access-list extended....2-23
7.2.7 userdefined access-group....2-23
7.2.8 vacl userdefined access-group....2-23
7.3 802.1x....2-24
7.3.1 authentication dot1x radius none....2-24
7.3.2 debug dot1x detail....2-24
7.3.3 debug dot1x error....2-25
7.3.4 debug dot1x fsm....2-25
7.3.5 debug dot1x packet....2-26
7.3.6 dot1x accept-mac....2-26
7.3.7 dot1x eapor enable....2-27
7.3.8 dot1x enable....2-27
7.3.9 dot1x ipv6 passthrough....2-27
7.3.10 dot1x guest-vlan....2-27
7.3.11 dot1x macfilter enable....2-28
7.3.12 dot1x macbased guest-vlan....2-29
7.3.13 dot1x macbased port-down-flush....2-29
7.3.14 dot1x max-req....2-30
7.3.15 dot1x user allow-movement....2-30
7.3.16 dot1x user free-resource....2-30
7.3.17 free-resource destination....2-31
7.3.18 dot1x max-user macbased....2-31
7.3.19 dot1x max-user userbased....2-31
7.3.20 dot1x portbased mode single-mode....2-32
7.3.21 dot1x port-control....2-32
7.3.22 dot1x port-method....2-33

7.3.23 dot1x privateclient enable....2-33
7.3.24 dot1x privateclient protect enable....2-34
7.3.25 dot1x re-authenticate....2-34
7.3.26 dot1x re-authentication....2-34
7.3.27 dot1x timeout quiet-period....2-35
7.3.28 dot1x timeout re-authperiod....2-35
7.3.29 dot1x timeout tx-period....2-35
7.3.30 dot1x unicast enable....2-36
7.3.31 dot1x web authentication enable....2-36
7.3.32 dot1x web authentication ipv6 passthrough....2-36
7.3.33 dot1x web redirect....2-36
7.3.34 dot1x web redirect enable....2-36
7.3.35 free-mac....2-37
7.3.36 show dot1x....2-37
7.3.37 show dot1x user....2-39
7.3.38 clear dot1x all....2-39
7.3.39 user-control limit ipv4....2-39
7.3.40 user-control limit ipv6....2-39
7.3.41 vlan-pool....2-39
7.4 The Number Limitation Function of MAC and IP in Port, VLAN....2-40
7.4.1 debug ip arp count....2-40
7.4.2 debug ipv6 nd count....2-40
7.4.3 debug switchport arp count....2-40
7.4.4 debug switchport mac count....2-41
7.4.5 debug switchport nd count....2-41
7.4.6 debug vlan mac count....2-42
7.4.7 ip arp dynamic maximum....2-42
7.4.8 ipv6 nd dynamic maximum....2-43
7.4.9 mac-address query timeout....2-43
7.4.10 show arp-dynamic count....2-44
7.4.11 show mac-address dynamic count....2-44
7.4.12 show nd-dynamic count....2-45
7.4.13 switchport arp dynamic maximum....2-45
7.4.14 switchport mac-address dynamic maximum....2-46
7.4.15 switchport mac-address violation....2-46
7.4.16 switchport nd dynamic maximum....2-47
7.4.17 vlan mac-address dynamic maximum....2-47
7.5 AM....2-48

7.5.1 am enable **2-48**
7.5.2 am port **2-48**
7.5.3 am ip-pool **2-49**
7.5.4 am mac-ip-pool **2-49**
7.5.5 no am all **2-49**
7.5.6 show am **2-50**
7.6 Security Feature 2-51
7.6.1 dosattack-check srcip-equal-dstip enable **2-51**
7.6.2 dosattack-check ipv4-first-fragment enable **2-51**
7.6.3 dosattack-check tcp-flags enable **2-51**
7.6.4 dosattack-check srcport-equal-dstport enable **2-52**
7.6.5 dosattack-check tcp-fragment enable **2-52**
7.6.6 dosattack-check tcp-segment **2-52**
7.6.7 dosattack-check icmp-attacking enable **2-52**
7.6.8 dosattack-check icmpV4-size **2-53**
7.6.9 dosattack-check icmpv6-size **2-53**
7.6.10 invalid-dip-drop **2-53**
7.7 TACACS+ 2-53
7.7.1 tacacs-server authentication host **2-53**
7.7.2 tacacs-server key **2-54**
7.7.3 tacacs-server nas-ipv4 ..... **2-54**
7.7.4 tacacs-server timeout **2-55**
7.7.5 debug tacacs-server **2-55**
7.8 RADIUS 2-56
7.8.1 aaa enable **2-56**
7.8.2 aaa-accounting enable **2-56**
7.8.3 aaa-accounting update **2-56**
7.8.4 aaa group server radius **2-57**
7.8.5 debug aaa packet **2-57**
7.8.6 debug aaa detail attribute **2-57**
7.8.7 debug aaa detail connection **2-58**
7.8.8 debug aaa detail escape **2-58**
7.8.9 debug aaa detail event **2-58**
7.8.10 debug aaa error **2-59**
7.8.11 radius nas-ipv4 ..... **2-59**
7.8.12 radius nas-ipv6 ..... **2-59**
7.8.13 radius-server accounting host **2-60**
7.8.14 radius-server authentication host **2-61**

7.8.15 radius-server dead-time 2-62
7.8.16 radius-server key 2-62
7.8.17 radius-server retransmit 2-62
7.8.18 radius-server timeout 2-63
7.8.19 radius-server accounting-interim-update timeout 2-63
7.8.20 server 2-64
7.8.21 show aaa authenticated-user 2-64
7.8.22 show aaa authenticating-user 2-64
7.8.23 show aaa config 2-65
7.8.24 show radius authenticated-user count 2-66
7.8.25 show radius authenticating-user count 2-66
7.8.26 show radius count 2-66
7.8.27 Radius Escaping 2-67
7.9 SSL 2-68
7.9.1 ip http secure-server 2-68
7.9.2 ip http secure-port 2-68
7.9.3 ip http secure- ciphersuite 2-68
7.9.4 show ip http secure-server status 2-69
7.9.5 debug ssl 2-69
7.10 VLAN-ACL 2-70
7.10.1 clear vacl statistic vlan 2-70
7.10.2 show vacl vlan 2-70
7.10.3 vacl ip access-group 2-71
7.10.4 vacl ipv6 access-group 2-72
7.10.5 vacl mac access-group 2-72
7.10.6 vacl mac-ip access-group 2-72
7.11 Captive Portal Authentication 2-73
7.11.1 Authentication 2-73
7.11.2 Free-resource 2-87
7.11.3 Automatic Page Pushing after Successful Authentication 2-87
7.11.4 Portal Escaping 2-89
7.12 MAB 2-90
7.12.1 authentication mab 2-90
7.12.2 clear mac-authentication-bypass binding 2-90
7.12.3 debug mac-authentication-bypass 2-90
7.12.4 mac-authentication-bypass binding-limit 2-91
7.12.5 mac-authentication-bypass enable 2-91
7.12.6 mac-authentication-bypass guest-vlan 2-91

7.12.7 mac-authentication-bypass spoofing-garp-check 2-92
7.12.8 mac-authentication-bypass timeout linkup-period 2-92
7.12.9 mac-authentication-bypass timeout offline-detect 2-92
7.12.10 mac-authentication-bypass timeout quiet-period 2-93
7.12.11 mac-authentication-bypass timeout reauth-period 2-93
7.12.12 mac-authentication-bypass timeout stale-period 2-94
7.12.13 mac-authentication-bypass username-format 2-94
7.12.14 show mac-authentication-bypass 2-94
7.13 PPPoE Intermediate Agent 2-96
7.13.1 debug pppoe packet {receive | send} interface ethernet <interface-name> 2-96
7.13.2 pppoe intermediate-agent 2-96
7.13.3 pppoe intermediate-agent (Port) 2-97
7.13.4 pppoe intermediate-agent circuit-id.....2-97
7.13.5 pppoe intermediate-agent delimiter.....2-98
7.13.6 pppoe intermediate-agent format.....2-98
7.13.7 pppoe intermediate-agent remote-id 2-98
7.13.8 pppoe intermediate-agent trust.....2-99
7.13.9 pppoe intermediate-agent type self-defined circuit-id.....2-99
7.13.10 pppoe intermediate-agent type self-defined remoteid.....2-99
7.13.11 pppoe intermediate-agent type tr-101 circuit-id access-node-id2-100
7.13.12 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter 2-100
7.13.13 pppoe intermediate-agent vendor-tag strip 2-101
7.13.14 show pppoe intermediate-agent access-node-id 2-102
7.13.15 show pppoe intermediate-agent identifier-string option delimiter2-102
7.13.16 show pppoe intermediate-agent info 2-102
7.14 QoS.....2-103
7.14.1 accounting 2-103
7.14.2 class 2-103
7.14.3 class-map.....2-104
7.14.4 clear mls qos statistics 2-104
7.14.5 drop 2-104
7.14.6 match.....2-105
7.14.7 mls qos aggregate-policy.....2-106
7.14.8 mls qos cos 2-107
7.14.9 mls qos internal-priority.....2-108
7.14.10 mls qos map 2-108

7.14.11 mls qos queue weight.....2-110
7.14.12 mls qos queue wred 2-110
7.14.13 mls qos queue wdrr weight.....2-110
7.14.14 mls qos trust.....2-111
7.14.15 pass-through-cos.....2-111
7.14.16 pass-through-dscp-exp 2-111
7.14.17 policy 2-112
7.14.18 policy aggregate.....2-113
7.14.19 policy-map 2-114
7.14.20 service-policy input 2-114
7.14.21 service-policy input vlan 2-115
7.14.22 set 2-115
7.14.23 show class-map 2-116
7.14.24 show policy-map.....2-116
7.14.25 show mls qos interface 2-117
7.14.26 show mls qos in {interface <interface-name> policy | vlan <vlan-id>2-120
7.14.27 show mls qos maps.....2-120
7.14.28 show mls qos vlan 2-122
7.14.29 show mls qos aggregate-policy 2-122
7.14.30 transmit 2-123
7.15 Flow-based Redirection.....2-123
7.15.1 access-group redirect to interface ethernet 2-123
7.15.2 match vlan <1-4096> redirect interface (ethernet|) IFNAME 2-124
7.15.3 port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME.....2-124
7.15.4 show flow-based-redirect.....2-125
7.15.5 vlan-port-redirect vlan maximum <1-1000> 2-125
7.16 Egress QoS 2-126
7.16.1 mls qos egress green remark.....2-126
7.16.2 mls qos map 2-126
7.16.3 service-policy output.....2-129
7.16.4 service-policy output vlan.....2-129
7.16.5 set 2-129
7.16.6 show mls qos egress green remark.....2-130
7.16.7 show mls qos maps.....2-130
7.17 Flexible QinQ.....2-131
7.17.1 Add.....2-131
7.17.2 delete 2-131

7.17.3 Match **2-131**
7.17.4 service-policy **2-132**
7.17.5 set **2-133**

CHAPTER 8 COMMANDS FOR RELIABILITY **2-1**

8.1 MSTP 2-1
8.1.1 MSTP **2-1**
8.1.2 Monitor and Debug **2-15**
8.1.3 MSTP Spanning-tree Process **2-19**
8.2 VRRP 2-19
8.2.1 advertisement-interval **2-19**
8.2.2 circuit-failover **2-20**
8.2.3 debug vrrp **2-20**
8.2.4 disable **2-21**
8.2.5 enable **2-21**
8.2.6 interface **2-22**
8.2.7 preempt-mode **2-22**
8.2.8 priority **2-22**
8.2.9 router vrrp **2-22**
8.2.10 show vrrp **2-23**
8.2.11 virtual-ip **2-24**
8.2.12 vrrp track **2-24**
8.3 MRPP 2-25
8.3.1 control-vlan **2-25**
8.3.2 clear mrpp statistics **2-25**
8.3.3 debug mrpp **2-25**
8.3.4 enable **2-26**
8.3.5 errp domain **2-26**
8.3.6 fail-timer **2-27**
8.3.7 hello-timer **2-27**
8.3.8 mrpp eaps compatible **2-27**
8.3.9 mrpp enable **2-28**
8.3.10 mrpp errp compatible **2-28**
8.3.11 mrpp poll-time **2-29**
8.3.12 mrpp ring **2-29**
8.3.13 mrpp ring primary-port **2-29**
8.3.14 mrpp ring secondary-port **2-30**

8.3.15 node-mode **2-30**
8.3.16 show mrpp **2-30**
8.3.17 show mrpp statistics **2-31**
8.4 ULPP 2-31
8.4.1 clear ulpp flush counter interface **2-31**
8.4.2 control vlan **2-31**
8.4.3 debug ulpp error **2-32**
8.4.4 debug ulpp event **2-32**
8.4.5 debug ulpp flush {send | receive} interface **2-32**
8.4.6 description **2-33**
8.4.7 flush disable arp **2-33**
8.4.8 flush disable mac **2-33**
8.4.9 flush disable mac-vlan **2-34**
8.4.10 flush enable arp **2-34**
8.4.11 flush enable mac **2-34**
8.4.12 flush enable mac-vlan **2-35**
8.4.13 preemption delay **2-35**
8.4.14 preemption mode **2-35**
8.4.15 protect vlan-reference-instance **2-36**
8.4.16 show ulpp flush counter interface **2-36**
8.4.17 show ulpp flush-receive-port **2-36**
8.4.18 show ulpp group **2-37**
8.4.19 ulpp control vlan **2-37**
8.4.20 ulpp flush disable arp **2-38**
8.4.21 ulpp flush disable mac **2-38**
8.4.22 ulpp flush disable mac-vlan **2-38**
8.4.23 ulpp flush enable arp **2-39**
8.4.24 ulpp flush enable mac **2-39**
8.4.25 ulpp flush enable mac-vlan **2-39**
8.4.26 ulpp group **2-40**
8.4.27 ulpp group master **2-40**
8.4.28 ulpp group slave **2-40**
8.5 ULSM 2-41
8.5.1 debug ulsm event **2-41**
8.5.2 show ulsm group **2-41**
8.5.3 ulsm group **2-41**
8.5.4 ulsm group {uplink | downlink} **2-42**
8.6 ERPS 2-42

8.6.1 ethernet tcn-propagation erps to {erps | stp} 2-42
8.6.2 erps-ring <ring-name> 2-43
8.6.3 version {v1 | v2} 2-43
8.6.4 open-ring 2-44
8.6.5 raps-virtual-channel {with | without} 2-45
8.6.6 erps-ring <ring-name> port0 [port1-none] 2-45
8.6.7 erps-ring <ring-name> port1 2-46
8.6.8 failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id> 2-47
8.6.9 erps-instance <instance-id> 2-48
8.6.10 description 2-49
8.6.11 ring-id <ring-id> 2-50
8.6.12 rpl {port0 | port1} {owner | neighbour} 2-50
8.6.13 non-revertive 2-51
8.6.14 guard-timer <guard-times> 2-52
8.6.15 holdoff-timer < holdoff-times> 2-52
8.6.16 wtr-timer <wtr-times> 2-53
8.6.17 protected-instance 2-53
8.6.18 raps-mel <level-value> 2-54
8.6.19 control-vlan <vlan-id> 2-55
8.6.20 forced-switch {port0 | port1} 2-56
8.6.21 manual-switch {port0 | port1} 2-56
8.6.22 clear command 2-57
8.6.23 show erps ring {<ring-name> | brief} 2-58
8.6.24 show erps instance [ring <ring-name> [instance <instance-id>]] .2-60
8.6.25 show erps status [ring <ring-name> [instance <instance-id>]] 2-61
8.6.26 show erps statistics [ring <ring-name> [instance <instance-id>]] 2-62
8.6.27 clear erps statistics [ring <ring-name> [instance <instance-id>]] .2-62
8.6.28 debug erps 2-63
8.6.29 debug erps error 2-63
8.6.30 debug erps event 2-63
8.6.31 no debug all 2-64
8.6.32 show debugging 2-64

CHAPTER 9 COMMANDS FOR DEBUGGING AND DIAGNOSIS2-1

9.1 Monitor and Debug 2-1

9.1.1 clear history all-users **2-1**
9.1.2 history all-users max-length **2-1**
9.1.3 ping **2-1**
9.1.4 ping6 ..... **2-3**
9.1.5 show boot-files **2-4**
9.1.6 show debugging **2-5**
9.1.7 show fan **2-5**
9.1.8 show flash **2-6**
9.1.9 show history **2-6**
9.1.10 show history all-users **2-6**
9.1.11 show memory usage **2-7**
9.1.12 show running-config **2-7**
9.1.13 show running-config current-mode **2-8**
9.1.14 show startup-config **2-8**
9.1.15 show switchport interface **2-8**
9.1.16 show tcp **2-9**
9.1.17 show tcp ipv6 ..... **2-9**
9.1.18 show telnet login **2-10**
9.1.19 show temperature **2-10**
9.1.20 show tech-support **2-10**
9.1.21 show udp **2-11**
9.1.22 show udp ipv6 ..... **2-11**
9.1.23 show version **2-11**
9.1.24 traceroute **2-12**
9.1.25 traceroute6 ..... **2-12**
9.2 Logging 2-13
9.2.1 logging executed-commands **2-13**
9.2.2 show logging executed-commands state **2-13**
9.2.3 clear logging **2-13**
9.2.4 logging **2-13**
9.2.5 logging loghost sequence-number **2-14**
9.2.6 logging source-ip **2-14**
9.2.7 show logging buffered **2-14**
9.2.8 show logging executed-commands state **2-14**
9.2.9 show logging source **2-14**
9.3 Reload Switch after Specified Time 2-14
9.3.1 reload after **2-14**
9.3.2 reload cancel **2-15**

9.3.3 show reload 2-15
9.4 Debugging and Diagnosis for Packets Received and Sent by CPU 2-15
9.4.1 clear cpu-rx-stat protocol.....2-15
9.4.2 cpu-rx-limitnotify enable interval 2-16
9.4.3 cpu-rx-limitnotify protocol (all|WORD)(enable|disable).....2-16
9.4.4 cpu-rx-ratelimit channel 2-17
9.4.5 cpu-rx-ratelimit enhanced 2-17
9.4.6 cpu-rx-ratelimit protocol 2-17
9.4.7 cpu-rx-ratelimit queue-length 2-17
9.4.8 cpu-rx-ratelimit total 2-17
9.4.9 debug driver 2-18
9.4.10 protocol filter 2-18
9.4.11 show cpu-rx protocol.....2-19
9.5 CPU-Protect 2-19
9.5.1 cpu-protect enable 2-19
9.5.2 cpu-protect log enable 2-19
9.5.3 cpu-protect trap enable 2-20
9.5.4 cpu-protect interval.....2-20
9.5.5 cpu-protect recovery-time.....2-20
9.5.6 cpu-protect threshold.....2-21
9.5.7 cpu-protect limit-speed 2-21
9.5.8 show cpu-protect attack-list 2-22
9.5.9 show cpu-protect running-config 2-22
9.6 Info-Center.....2-23
9.6.1 info-center enable 2-23
9.6.2 info-center prefix.....2-24
9.6.3 info-center match 2-24
9.6.4 info-center output-enable.....2-25
9.6.5 info-center record-cmd.....2-26
9.6.6 info-center loghost.....2-26
9.6.7 info-center logfile 2-27
9.6.8 info-center clear 2-28
9.6.9 show info-center config 2-28
9.6.10 show info-center logbuffer.....2-29
9.6.11 show info-center trapbuffer 2-30
9.6.12 show info-center logfile.....2-31
9.6.13 info-center list all disk 2-33
9.6.14 info-center save all 2-33

9.7 Mirror 2-34
9.7.1 monitor session source interface 2-34
9.7.2 monitor session source interface access-list 2-34
9.7.3 monitor session destination interface 2-35
9.7.4 show monitor 2-35
9.7.5 mirror sample rate 2-36
9.8 RSPAN 2-36
9.8.1 remote-span 2-36
9.8.2 monitor session remote vlan 2-36
9.8.3 monitor session reflector-port 2-37
9.9 ERSPAN 2-37
9.9.1 monitor session destination tunnel 2-37
9.10 sFlow 2-38
9.10.1 sflow agent-address 2-38
9.10.2 sflow analyzer 2-38
9.10.3 sflow counter-interval 2-39
9.10.4 sflow data-len 2-39
9.10.5 sflow destination 2-39
9.10.6 sflow header-len 2-40
9.10.7 sflow priority 2-40
9.10.8 sflow rate 2-40
9.10.9 sflow version 2-41
9.10.10 show sflow 2-41
9.11 NQA 2-43
9.11.1 nqa agent 2-43
9.11.2 nqa entry type icmp-echo 2-43
9.11.3 nqa entry type icmp-jitter 2-43
9.11.4 nqa entry type udp-echo 2-44
9.11.5 nqa entry type udp-jitter 2-44
9.11.6 nqa entry type tcp 2-45
9.11.7 nqa entry type dhcp 2-45
9.11.8 nqa entry description 2-46
9.11.9 nqa entry frequency 2-46
9.11.10 nqa entry probe-count 2-46
9.11.11 nqa entry probe-timeout 2-47
9.11.12 nqa entry datasize 2-47
9.11.13 nqa entry ttl 2-48
9.11.14 nqa entry tos 2-48

9.11.15 nqa entry fail-percent....2-48
9.11.16 nqa entry records-result....2-49
9.11.17 nqa entry probe-threshold....2-49
9.11.18 nqa entry start....2-49
9.11.19 nqa alarm enable....2-50
9.11.20 nqa traps enable....2-50
9.11.21 nqa entry alarm enable....2-50
9.11.22 nqa entry traps enable....2-51
9.11.23 nqa server....2-51
9.11.24 nqa server tcp-port....2-51
9.11.25 nqa server udp-port....2-52
9.11.26 track nqa....2-52
9.11.27 track list boolean....2-53
9.11.28 ip route track....2-53
9.11.29 rip track....2-53
9.11.30 ospf track....2-54
9.11.31 bgp track....2-54
9.11.32 show nqa results....2-54
9.11.33 show track status....2-55

CHAPTER 10 COMMANDS FOR NETWORK TIME MANAGEMENT....2-1

10.1 NTP....2-1
10.1.1 clock timezone....2-1
10.1.2 debug ntp adjust....2-1
10.1.3 debug ntp authentication....2-1
10.1.4 debug ntp events....2-2
10.1.5 debug ntp packet....2-2
10.1.6 debug ntp sync....2-2
10.1.7 ntp access-group....2-3
10.1.8 ntp authenticate....2-3
10.1.9 ntp authentication-key....2-3
10.1.10 ntp broadcast client....2-4
10.1.11 ntp broadcast server count....2-4
10.1.12 ntp disable....2-4
10.1.13 ntp enable....2-4

10.1.14 ntp ipv6 multicast client 2-5
10.1.15 ntp multicast client 2-5
10.1.16 ntp server 2-5
10.1.17 ntp syn-interval 2-6
10.1.18 ntp trusted-key 2-6
10.1.19 show ntp status 2-7
10.1.20 show ntp session 2-7
10.2 SNTP 2-7
10.2.1 clock timezone 2-7
10.2.2 debug sntp 2-8
10.2.3 sntp polltime 2-8
10.2.4 sntp server 2-8
10.2.5 show sntp 2-9
10.3 DNSv4/v6 2-10
10.3.1 clear dynamic-host 2-10
10.3.2 debug dns 2-10
10.3.3 dns-server 2-10
10.3.4 dns lookup 2-11
10.3.5 show dns name-server 2-11
10.3.6 show dns domain-list 2-12
10.3.7 show dns hosts 2-12
10.3.8 show dns config 2-12
10.3.9 show dns client 2-13
10.3.10 ip domain-lookup 2-13
10.3.11 ip domain-list 2-13
10.3.12 ip dns server 2-14
10.3.13 ip dns server queue maximum 2-14
10.3.14 ip dns server queue timeout 2-14
10.4 Summer Time 2-15
10.4.1 clock summer-time absolute 2-15
10.4.2 clock summer-time recurring 2-15
10.4.3 clock summer-time recurring 2-16

CHAPTER 11 COMMANDS FOR VIRTUALIZATION 2-1

11.1 VSF 2-1
11.1.1 Basic VSF 2-1
11.1.2 Configuration and Debugging of VSF Conflict Detection 2-7

11.1.3 VSF Debugging.....2-10

CHAPTER 12 COMMANDS FOR DATACENTER 2-1

12.1 Commands for MC-LAG.....2-1
12.1.1 evpn nve mac-address 2-1
12.1.2 mac-address 2-1
12.1.3 mclag 2-1
12.1.4 mclag domain-id.....2-2
12.1.5 mclag priority 2-2
12.1.6 mclag enable 2-2
12.1.7 mclag group.....2-3
12.1.8 mclag local-ip 2-3
12.1.9 mclag peer-ip.....2-3
12.1.10 ip address 2-4
12.1.11 ipv6 address 2-4
12.1.12 mclag dad link 2-5
12.1.13 error-down exclude.....2-5
12.1.14 mclag up-delay.....2-6
12.1.15 mclag probe-interval.....2-6
12.1.16 show mclag.....2-6
12.1.17 show mclag group 2-7
12.1.18 switchport mclag data link.....2-7
12.1.19 virtual-equipment-group ID.....2-8
12.1.20 virtual-equipment-group ID.....2-8
12.1.21 virtual-equipment-group ID.....2-8
12.2 Commands for NETCONF 2-9
12.2.1 netconf server enable.....2-9
12.2.2 show netconf session 2-9
12.2.3 show netconf tcp.....2-9
12.3 Commands for Telemetry 2-10
12.3.1 Telemetry.....2-10
12.3.2 grpc-sever.....2-10
12.3.3 destination-group.....2-10
12.3.4 destination-group ipv4-address 2-11
12.3.5 sensor-group 2-11
12.3.6 sensor-group path memoryInfo 2-12
12.3.7 sensor-group path cpuInfo 2-12

12.3.8 sensor-group path ifStatistics 2-13
12.3.9 subscription 2-13
12.3.10 subscription destination-group 2-13
12.3.11 subscription sensor-group 2-14
12.3.12 tun interface vlan 2-14
12.3.13 show telemetry subscription 2-15
12.3.14 show telemetry dynamic-subscription 2-16
12.4 VXLAN Commands 2-17
12.4.1 arp proxy-answer enable 2-17
12.4.2 arp suppression enable 2-17
12.4.3 arp suppress-drop 2-17
12.4.4 arp suppression table kat 2-18
12.4.5 clear nvi statistics 2-18
12.4.6 description 2-18
12.4.7 description 2-19
12.4.8 destination 2-19
12.4.9 flooding disable 2-19
12.4.10 interface nve 2-20
12.4.11 interface nvi-interface 2-20
12.4.12 ip address 2-20
12.4.13 ipv6 address 2-21
12.4.14 join nvi 2-21
12.4.15 mac-address 2-21
12.4.16 mac-address-table static address nvi 2-22
12.4.17 nd proxy-answer enable 2-22
12.4.18 nd suppression enable 2-23
12.4.19 nd suppress-drop 2-23
12.4.20 nd suppression table kat 2-23
12.4.21 nve mode 2-23
12.4.22 nvi 2-24
12.4.23 remote ip 2-24
12.4.24 show interface nve 2-24
12.4.25 show interface nvi-interface 2-25
12.4.26 show ipv6 interface nvi-interface 2-26
12.4.27 show nvi arp suppression 2-27
12.4.28 show nvi detail 2-27
12.4.29 show nvi nd suppression 2-28
12.4.30 show nvi nve tunnel 2-29

12.4.31 show nvi statistics **2-29**
12.4.32 show virtual-equipment-group ID **2-30**
12.4.33 show virtual-equipment-group ID service **2-30**
12.4.34 show vxlan mac-address-table **2-31**
12.4.35 show vxlan mac-address-table count **2-32**
12.4.36 source **2-32**
12.4.37 source ip **2-32**
12.4.38 virtual-equipment-group ID **2-33**
12.4.39 vxlan remote arp-learning disable **2-33**
12.4.40 vxlan remote mac-address-learning disable **2-33**
12.4.41 vxlan remote nd-learning disable **2-34**
12.4.42 vxlan udp destination-port-number **2-34**
12.4.43 vxlan-id **2-34**
12.4.44 xconnect nvi **2-35**
12.5 EVPN Commands 2-35
12.5.1 address-family l2vpn evpn **2-35**
12.5.2 distributed-gateway enable **2-35**
12.5.3 dup-addr-detection **2-36**
12.5.4 enable/disable **2-36**
12.5.5 esi **2-36**
12.5.6 evpn **2-37**
12.5.7 evpn nve source-address **2-37**
12.5.8 evpn nvi-vlan-mapping-monitor disable **2-38**
12.5.9 evpn timer df-delay **2-38**
12.5.10 evpn-exit **2-38**
12.5.11 exit-address-family **2-39**
12.5.12 ip vrf forwarding **2-39**
12.5.13 l3-vni **2-39**
12.5.14 rd **2-40**
12.5.15 route-target **2-40**
12.5.16 neighbor activate **2-41**
12.5.17 neighbor route-reflector-client **2-41**
12.5.18 show evpn es **2-41**
12.5.19 show evpn mac-ip **2-42**
12.5.20 show evpn mac-mobility **2-43**
12.5.21 show evpn nvi **2-44**
12.5.22 show ip bgp evpn **2-44**

CHAPTER 13 COMMANDS FOR IPV6 2-1

13.1 DHCPv6 2-1
13.1.1 clear ipv6 dhcp binding 2-1
13.1.2 clear ipv6 dhcp conflict 2-1
13.1.3 clear ipv6 dhcp statistics 2-2
13.1.4 debug ipv6 dhcp client packet 2-2
13.1.5 debug ipv6 dhcp detail 2-2
13.1.6 debug ipv6 dhcp relay packet 2-2
13.1.7 debug ipv6 dhcp server 2-3
13.1.8 dns-server 2-3
13.1.9 domain-name 2-3
13.1.10 excluded-address 2-4
13.1.11 ipv6 address 2-4
13.1.12 ipv6 dhcp client pd 2-4
13.1.13 ipv6 dhcp client pd hint 2-5
13.1.14 ipv6 dhcp pool 2-5
13.1.15 ipv6 dhcp relay destination 2-6
13.1.16 ipv6 dhcp server 2-6
13.1.17 ipv6 general-prefix 2-7
13.1.18 ipv6 local pool 2-7
13.1.19 lifetime 2-8
13.1.20 network-address 2-8
13.1.21 prefix-delegation 2-9
13.1.22 prefix-delegation add static route 2-9
13.1.23 prefix-delegation pool 2-10
13.1.24 service dhcpv6 2-10
13.1.25 show ipv6 dhcp 2-11
13.1.26 show ipv6 dhcp binding 2-11
13.1.27 show ipv6 dhcp conflict 2-11
13.1.28 show ipv6 dhcp interface 2-11
13.1.29 show ipv6 dhcp pool 2-12
13.1.30 show ipv6 dhcp statistics 2-12
13.1.31 show ipv6 general-prefix 2-14
13.1.32 show ipv6 local pool 2-14
13.2 DHCPv6 option37, 38 2-15
13.2.1 Commands for DHCPv6 option37, 38 2-15

13.2.2 Commands for Monitoring and Debugging 2-24
13.3 Prevent ND Spoofing.....2-27
13.3.1 ipv6 nd-security updateprotect 2-27
13.3.2 ipv6 nd-security learnprotect.....2-27
13.3.3 ipv6 nd-security convert 2-28
13.4 RIPng.....2-28
13.4.1 clear ipv6 route.....2-28
13.4.2 default-information originate.....2-29
13.4.3 default-metric 2-29
13.4.4 distance.....2-30
13.4.5 distribute-list 2-30
13.4.6 debug ipv6 rip.....2-30
13.4.7 debug ipv6 rip redistribute message send 2-31
13.4.8 debug ipv6 rip redistribute route receive.....2-31
13.4.9 ipv6 rip aggregate-address.....2-32
13.4.10 ipv6 rip split-horizon.....2-32
13.4.11 ipv6 router rip 2-32
13.4.12 neighbor.....2-33
13.4.13 offset-list.....2-33
13.4.14 passive-interface.....2-34
13.4.15 redistribute 2-34
13.4.16 redistribute ospf.....2-34
13.4.17 route 2-35
13.4.18 router ipv6 rip.....2-35
13.4.19 show debugging ipv6 rip.....2-35
13.4.20 show ipv6 rip interface.....2-36
13.4.21 show ipv6 rip redistribute 2-36
13.4.22 show ipv6 protocols rip.....2-37
13.4.23 show ipv6 rip 2-37
13.4.24 show ipv6 rip database 2-38
13.4.25 show ipv6 rip aggregate.....2-38
13.4.26 show ipv6 rip redistribute 2-39
13.4.27 timers basic 2-39
13.5 OSPFv3 2-40
13.5.1 area authentication-mode 2-40
13.5.2 area default cost.....2-40
13.5.3 area range 2-41
13.5.4 area stub 2-41

13.5.5 area virtual-link....2-42
13.5.6 abr-type....2-42
13.5.7 default-metric....2-43
13.5.8 debug ipv6 ospf events....2-43
13.5.9 debug ipv6 ospf ifsm....2-43
13.5.10 debug ipv6 ospf lsa....2-44
13.5.11 debug ipv6 ospf nfsm....2-44
13.5.12 debug ipv6 ospf nsm....2-44
13.5.13 debug ipv6 ospf packet....2-44
13.5.14 debug ipv6 ospf redistribute message send....2-45
13.5.15 debug ipv6 ospf redistribute route receive....2-45
13.5.16 debug ipv6 ospf route....2-45
13.5.17 ipv6 ospf authentication-mode....2-45
13.5.18 ipv6 ospf cost....2-46
13.5.19 ipv6 ospf dead-interval....2-46
13.5.20 ipv6 ospf display route single-line....2-47
13.5.21 ipv6 ospf hello-interval....2-47
13.5.22 ipv6 ospf priority....2-48
13.5.23 ipv6 ospf retransmit-interval....2-48
13.5.24 ipv6 ospf transmit-delay....2-49
13.5.25 ipv6 router ospf....2-49
13.5.26 max-concurrent-dd....2-50
13.5.27 passive-interface....2-50
13.5.28 redistribute....2-51
13.5.29 redistribute ospf....2-51
13.5.30 router-id....2-52
13.5.31 router ipv6 ospf....2-52
13.5.32 show ipv6 ospf....2-52
13.5.33 show ipv6 ospf database....2-53
13.5.34 show ipv6 ospf interface....2-54
13.5.35 show ipv6 ospf neighbor....2-56
13.5.36 show ipv6 ospf route....2-56
13.5.37 show ipv6 ospf redistribute....2-57
13.5.38 show ipv6 ospf topology....2-57
13.5.39 show ipv6 ospf virtual-links....2-58
13.5.40 show ipv6 route process-detail....2-58
13.5.41 timers spf....2-59
13.6 MBGP4+....2-59

13.6.1 debug ipv6 bgp redistribute message send 2-59
13.6.2 debug ipv6 bgp redistribute route receive....2-59
13.6.3 redistribute ospf (MBGP4+) 2-60
13.6.4 show ipv6 bgp redistribute 2-60
13.7 Black Hole Routing....2-61
13.7.1 ipv6 route null0....2-61
13.8 IPv6 Multicast Protocol....2-61
13.8.1 Multicast....2-61
13.8.2 PIM-DM6 2-62
13.8.3 PIM-SM6 2-70
13.8.4 ANYCAST RP v6....2-88
13.8.5 PIM-SSM6....2-92
13.8.6 IPv6 DCSCM....2-93
13.8.7 MLD....2-100
13.8.8 MLD Snooping....2-107
13.9 IPv6 Security RA 2-114
13.9.1 ipv6 security-ra enable....2-114
13.9.2 ipv6 security-ra enable....2-115
13.9.3 show ipv6 security-ra 2-115
13.9.4 debug ipv6 security-ra....2-115
13.10 SAVI....2-116
13.10.1 Commands for SAVI....2-116
13.10.2 Commands for Monitor and Debug....2-122
13.11 IPv6 VRRPv3....2-125
13.11.1 advertisement-interval....2-125
13.11.2 circuit-failover....2-125
13.11.3 debug ipv6 vrrp 2-126
13.11.4 disable 2-126
13.11.5 enable 2-126
13.11.6 preempt-mode 2-127
13.11.7 priority 2-127
13.11.8 router ipv6 vrrp....2-127
13.11.9 show ipv6 vrrp....2-128
13.11.10 virtual-ipv6 interface....2-129

CHAPTER 14 COMMANDS FOR VPN....2-1

14.1 MPLS....2-1

14.1.1 mpls egress-ttl....2-1
14.1.2 mpls enable....2-1
14.1.3 mpls ingress-ttl....2-1
14.1.4 mpls local-packet-handling....2-2
14.1.5 mpls mtu....2-2
14.1.6 show mpls....2-2
14.1.7 show mpls enable....2-3
14.1.8 show mpls forwarding-table....2-3
14.1.9 show mpls ftn-table brief....2-4
14.1.10 show mpls ftn-table detail....2-4
14.1.11 show mpls ilm-table....2-5
14.1.12 show mpls vrf-table....2-6
14.2 LDP....2-7
14.2.1 advertisement-mode....2-7
14.2.2 clear ldp adjacency....2-8
14.2.3 clear ldp session....2-8
14.2.4 clear ldp statistics....2-9
14.2.5 control-mode....2-9
14.2.6 debug ldp all....2-9
14.2.7 debug ldp dsm....2-10
14.2.8 debug ldp error....2-10
14.2.9 debug ldp events....2-10
14.2.10 debug ldp fsm....2-11
14.2.11 debug ldp hexdump....2-11
14.2.12 debug ldp nsm....2-11
14.2.13 debug ldp packet....2-12
14.2.14 debug ldp timer....2-12
14.2.15 debug ldp tsm....2-12
14.2.16 debug ldp usm....2-13
14.2.17 ldp {enable|disable}....2-13
14.2.18 global-merge-capability....2-13
14.2.19 hello-interval....2-14
14.2.20 hold-time....2-14
14.2.21 import-bgp-routes....2-15
14.2.22 keepalive-interval....2-15
14.2.23 keepalive-timeout....2-16
14.2.24 label-retention-mode....2-16
14.2.25 label-switching....2-17

14.2.26 ldp advertisement-mode **2-17**
14.2.27 ldp hello-interval **2-18**
14.2.28 ldp hold-time **2-18**
14.2.29 ldp keepalive-interval **2-18**
14.2.30 ldp keepalive-timeout **2-19**
14.2.31 ldp label-retention-mode **2-19**
14.2.32 ldp multicast-hellos **2-20**
14.2.33 ldp targeted-peer-hello-interval **2-20**
14.2.34 ldp targeted-peer-hold-time **2-21**
14.2.35 loop-detection **2-21**
14.2.36 loop-detection-count **2-21**
14.2.37 multicast-hellos **2-22**
14.2.38 propagate-release **2-22**
14.2.39 request-retry **2-23**
14.2.40 request-retry-timeout **2-23**
14.2.41 router ldp **2-23**
14.2.42 router-id **2-24**
14.2.43 show ldp **2-24**
14.2.44 show ldp adjacency **2-26**
14.2.45 show ldp downstream **2-26**
14.2.46 show ldp fec **2-27**
14.2.47 show ldp interface **2-27**
14.2.48 show ldp lsp **2-28**
14.2.49 show ldp session **2-28**
14.2.50 show ldp statistics **2-28**
14.2.51 show ldp targeted-peers **2-29**
14.2.52 show ldp upstream **2-29**
14.2.53 show mpls ldp discovery **2-30**
14.2.54 show mpls ldp fec **2-30**
14.2.55 show mpls ldp neighbor **2-31**
14.2.56 show mpls ldp parameter **2-31**
14.2.57 show mpls ldp session **2-32**
14.2.58 targeted-hello-accept **2-33**
14.2.59 targeted-peer **2-33**
14.2.60 targeted-peer-hello-interval **2-33**
14.2.61 targeted-peer-hold-time **2-34**
14.2.62 transport-address **2-34**
14.3 MPLS VPN 2-35

14.3.1 address-family ipv4....2-35
14.3.2 address-family vpnv4....2-35
14.3.3 aggregate-address....2-36
14.3.4 clear ip bgp....2-36
14.3.5 debug bgp mpls....2-37
14.3.6 debug bgp update....2-37
14.3.7 description....2-37
14.3.8 import map....2-38
14.3.9 ip route vrf....2-38
14.3.10 ip vrf....2-38
14.3.11 ip vrf forwarding vrfName....2-39
14.3.12 neighbor remote-as....2-39
14.3.13 neighbor as-override....2-40
14.3.14 neighbor soo....2-40
14.3.15 rd....2-41
14.3.16 route-target....2-41
14.3.17 show ip bgp vpnv4....2-42
14.3.18 show ip route vrf....2-42
14.3.19 show ip vrf....2-43
14.4 VPLS&VPWS....2-44
14.4.1 clear mac-address-table....2-44
14.4.2 debug vpls packet....2-44
14.4.3 description....2-44
14.4.4 encapsulation....2-45
14.4.5 l2-vc....2-45
14.4.6 mac-address-table limit....2-45
14.4.7 mac-address-table static address....2-46
14.4.8 mtu....2-46
14.4.9 peer....2-47
14.4.10 pw-class....2-47
14.4.11 show mpls l2-vc....2-48
14.4.12 show pw-class....2-48
14.4.13 show vpls....2-48
14.4.14 show vpls fib....2-49
14.4.15 show vfi mac-address-table....2-49
14.4.16 show vfi mac-address-table count....2-50
14.4.17 show vpls peer....2-50
14.4.18 transport-mode....2-51

14.4.19 ptag.....2-51
14.4.20 Vfi.....2-52
14.4.21 vfi vfi-name 2-52
14.4.22 xconnect l2-vc 2-52
14.4.23 xconnect vfi 2-53

Chapter 1 Commands for Basic Switch

1.1 Basic Switch

1.1.1 Basic Configuration

1.1.1.1 authentication line login

Command: authentication line {console | vty | web} login {local | radius | tacacs}
no authentication line {console | vty | web} login

Function: Configure VTY (login with Telnet and SSH), Web and Console, so as to select the priority of the authentication mode for the login user. The no form command restores the default authentication mode.

Default: No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.

Command Mode: Global Mode.

Usage Guide: The authentication method for Console, VTY and Web login can be configured respectively. And authentication method can be any one or combination of Local, RADIUS and TACACS. When login method is configured in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives corresponding protocol's answer whether refuse or accept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. AAA function and RADIUS server should be configured before the RADIUS authentication can be used. And TACACS server should be configured before the TACACS configuration method can be used.The **authentication line console login** command is exclusive with the **login** command. The **authentication line console login** command configures the switch to use the Console login method. And the **login** command makes the Console login to use the passwords configured by the **password** command for authentication.

If local authentication is configured while no local users are configured, users will be able to login the switch via the Console method.

Example: Configure the Telnet and ssh login method to RADIUS authentication method.

Switch(config)# authentication line vty login radius

Relative Command: aaa enable, radius-server authentication host, tacacs-server authentication host, tacacs-server key

1.1.1.2 banner

Command: banner motd <LINE>

no banner motd

Function: This command is used to configure the information displayed when the login authentication of a telnet or console user is successful, the no command configures that the information is not displayed when the authentication is successful.

Parameters: <*LINE*>: The information displayed when the authentication is successful, length limit from 1 to 256 characters.

Default: Do not show the information when the authentication is successful.

Command mode: Global mode.

Example:

Switch(config)#banner motd Welcome

1.1.1.3 boot img

Command: boot img <img-file-url> {primary | backup}

Function**:** Configure the first and second img files used in the next boot of master board.

Parameters**:** primary means to configure the first IMG file, backup means to configure the second IMG file, <img-file-url> is the full path of the booting IMG file, the format of which is as follows:

1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between two parts.

2. The suffix of all file names should be .img.

3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.

Command Mode: Admin Mode.

Default: The factory original configuration only specifies the first booting IMG file, it is nos.img file in the FLASH, without the second booting IMG file.

Example:

1. Set flash:/nos.img as the second booting IMG file used in the next booting of the system.

Switch#boot img flash:/nos.img backup

2. Set flash:/5.4.128.0_nos.img as the first booting IMG file used in the next booting of the system.

Switch#boot img flash:/5.4.128.0_nos.img primary

1.1.1.4 boot startup-config

Command: boot startup-config {NULL | <file-url> }

Function: Configure the CFG file used in the next booting of the master board.

Parameters: The NULL keyword means to use the factory original configuration as the next booting configuration. Setting the CFG file used in the next booting as NULL equals to implementing set default and write commands. ***<file-url>*** is the full path of CFG file used in the next booting.

1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between two parts.

2. The suffix of all file names should be .cfg.

3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 **characters**.

***Command* Mode**: Admin Mode.

Default Settings: None.

Example:

1. Set flash:/ startup.cfg as the booting CFG file used in the next booting of the system.

Switch# boot startup-config flash:/ startup.cfg

2. Set flash:/ test-trunk.cfg as the booting CFG file used in the next booting of the system.

Switch#boot startup-config flash:/ test-trunk.cfg

1.1.1.5 clock set

Command: clock set *<HH:MM:SS> <YYYY.MM.DD>*

Function: Set system date and time.

Parameter: ***<HH:MM:SS>***is the current time, and the valid scope for ***HH*** is 0 to 23, ***MM*** and ***SS*** 0 to 59; ***<YYYY.MM.DD>*** is the current year, month and date, and the valid scope for ***YYYY*** is 2001~2037, ***MON*** meaning month, and ***DD*** between 1 to 31.

Command mode: Admin Mode.

Default: upon first time start-up, it is defaulted to 2006.1.1 0: 0: 0.

Usage guide: The switch can not continue timing with power off, hence the current date and time must be first set at environments where exact time is required.

Example: To set the switch current date and time to 2002.8.1 23: 0: 0:

Switch#clock set 23:0:0 2002.8.1

Relative Command: show clock

1.1.1.6 config

Command: config [terminal]

Function: Enter Global Mode from Admin Mode.

Parameter: [terminal] indicates terminal configuration.

Command mode: Admin Mode

Example:

Switch#config

1.1.1.7 debug ssh-server

Command: debug ssh-server

no debug ssh-server

Function: Display SSH server debugging information; the "**no debug ssh-server**" command stops displaying SSH server debugging information.

Default: This function is disabled by default.

Command mode: Admin Mode.

1.1.1.8 disable

Command: disable
Function: Disable admin mode.
Parameter: None.
Default: None.
Command mode: Admin Mode.
Usage Guide: None.
Example:
Switch#disable
Switch>

1.1.1.9 enable

Command: enable [<*1-15*>]
Function: Use **enable** command to enter Admin Mode from User Mode, or change the privilege level of the users.
Command mode: User Mode/ Admin Mode.
Default: None.
Usage Guide: To prevent unauthorized access of non-admin user, user authentication is required (i.e. Admin user password is required) when entering Admin Mode from User Mode. If the correct Admin user password is entered, Admin Mode access is granted; if 3 consecutive entry of Admin user password are all wrong, it remains in the User Mode. When the user's privilege is changed from the low level to the high level, it needs to authenticate the password of the corresponding level, or else it will not authenticate the password. Set the Admin user password under Global Mode with "**enable password**" command.
Example:
Switch>enable
Switch#

1.1.1.10 enable password

Command: enable password [level <*1-15*>] [0 | 7] <*password*>
no enable password [level <*1-15*>]
Function: Configure the password used for enter Admin Mode from the User Mode,
The "**no enable password**" command deletes this password.
Parameter: level <*1-15*> is used to specify the privilege level, the default level is 15. **<*password*>** is the password for the user. If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted.
Command mode: Global Mode
Default: This password is empty by system default
Usage Guide: Configure this password to prevent unauthorized entering Admin Mode. It is recommended to set the password at the initial switch configuration. Also, it is recommended to

exit Admin Mode with "**exit**" command when the administrator needs to leave the terminal for a long time.

1.1.1.11 end

Command: end
Function: Quit current mode and return to Admin mode when not at User Mode/ Admin Mode.
Command mode: Except User Mode/ Admin Mode
Example: Quit VLAN mode and return to Admin mode.
Switch(config-vlan1)#end
Switch#

1.1.1.12 exec-timeout

Command: exec-timeout *<minutes>* [*<seconds>*]
no exec-timeout
Function: Configure the timeout of exiting admin mode. The "**no exec-timeout**" command restores the default value.
Parameters: ***<minute>*** is the time value shown in minute and ranges between 0~35791. ***<seconds>*** is the time value shown in seconds and ranges between 0~59.
Command mode: Global mode
Default: Default timeout is 10 minutes.
Usage guide: To secure the switch, as well to prevent malicious actions from unauthorized user, the time will be count from the last configuration the admin had made, and the system will exit the admin mode at due time. It is required to enter admin code and password to enter the admin mode again. The timeout timer will be disabled when the timeout is set to 0.
Example: Set the admin mode timeout value to 6 minutes.
Switch(config)#exec-timeout 6
Set the admin mode timeout value to 5 minutes, 30 seconds.
Switch(config)#exec-timeout 5 30

1.1.1.13 exit

Command: exit
Function: Quit current mode and return to it's previous mode.
Command mode: All Modes
Usage Guide: This command is to quit current mode and return to it's previous mode.
Example: Quit global mode to it's previous mode
Switch#exit
Switch#

1.1.1.14 help

Command: help

Function: Output brief description of the command interpreter help system.

Command mode: All configuration modes.

Usage Guide: An instant online help provided by the switch. Help command displays information about the whole help system, including complete help and partial help. The user can type in '?' any time to get online help.

Example:

```
switch(config)#help
CLI provides advanced help feature.    When you need help,
anytime at the command line please press '?'.

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. 'show ve?'.)
```

1.1.1.15 hostname

Command: hostname *<hostname>*

no hostname

Function: Set the prompt in the switch command line interface. The no operation cancels the configuration.

Parameter: *<hostname>* is the string for the prompt, up to 64 characters are allowed.

Command mode: Global Mode

Default: The default prompt is relative with the switch.

Usage Guide: With this command, the user can set the CLI prompt of the switch according to their own requirements.

Example: Set the prompt to "Test".

```
Switch(config)#hostname Test
Test(config)#
```

1.1.1.16 ip host

Command: ip host *<hostname> <ip_addr>*

no ip host {*<hostname>*|all}

Function: Set the mapping relationship between the host and IP address; the "no ip host" parameter of this command will delete the mapping.

Parameter: *<hostname>* is the host name, up to 64 characters are allowed; ***<ip_addr>*** is the

corresponding IP address for the host name, takes a dot decimal format; **all** is all of the host name.

Command mode: Global Mode

Usage Guide: Set the association between host and IP address, which can be used in commands like "**ping *<host>***".

Example: Set IP address of a host with the hostname of "test" to 200.121.1.1.

Switch(config)#ip host test 200.121.1.1

Command related: telnet, ping, traceroute

1.1.1.17 ipv6 host

Command: ipv6 host *<hostname> <ipv6_addr>*

no ipv6 host { *<hostname>* | all}

Function: Configure the mapping relationship between the IPv6 address and the host; the no command deletes this mapping relationship.

Parameter: *<hostname>* is the name of the host, containing max 64 characters; ***<ipv6_addr>*** is the IPv6 address corresponding to the host name. **all** is all the host address.

Command Mode: Global Mode

Usage Guide: Configure a fixed corresponding relationship between the host and the IPv6 address, applicable in commands such as **traceroute6 <host>**, etc.

Example: Set the IPv6 address of the host named test to 2001:1:2:3::1.

Switch(config)#ipv6 host test 2001:1:2:3::1

Command related: ping6, traceroute6

1.1.1.18 ip http server

Command: ip http server

no ip http server

Function: Enable Web configuration; the "**no ip http server**" command disables Web configuration

Default: Enable.

Command mode: Global mode

Usage guide: Web configuration is for supplying an interface configured with HTTP for the user, which is straight and visual, easy to understand.

Example: Enable Web Server function and enable Web configurations.

Switch(config)#ip http server

1.1.1.19 language

Command: language {chinese | english}

Function: Set the language for displaying the help information.

Parameter: chinese for Chinese display; **english** for English display.

Command mode: Admin and Config Mode.

Default: The default setting is English display.

Usage Guide: Switch provides help information in two languages, the user can select the language according to their preference. After the system restart, the help information display will revert to English.

1.1.1.20 login

Command: login

no login

Function: login enable password authentication, no login command cancels the login configuration.

Command mode: Global mode

Default: No login by default

Usage guide: By using this command, users have to enter the password set by password command to enter normal user mode with console; no login cancels this restriction.

Example: Enable password

Switch(config)#login

1.1.1.21 password

Command: password [0 | 7] *<password>*

no password

Function: Configure the password used for enter normal user mode on the console. The "**no password**" command deletes this password.

Parameter: password is the password for the user. If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted.

Command mode: Global mode

Default: This password is empty by system default

Usage guide: When both this password and login command are configured, users have to enter the password set by password command to enter normal user mode on console.

Example:

Switch(config)#password 0 test

Switch(config)#login

1.1.1.22 password feedback

Command: password feedback {none | star}

no password feedback

Function: Set the password feedback format for user login. The 'no' command restores the default feedback format.

Parameter:

none: When the user enters their password during login, no feedback message is displayed.

star: When the user enters their password during login, asterisks (*) will be displayed in

place of the characters.

Command mode: Global mode

Default: When the user enters their password during login, the user password is displayed as "*" by default.

Usage guide: Include SSH/Telnet/console login.

Example:

Switch(config)# password feedback none

1.1.1.23 privilege

Command: privilege mode level <*1-15*> LINE

no privilege mode level <*1-15*> LINE

Function: Configure the level for the specified command, the no command restores the original level of the command.

Parameters: mode: register mode of the command, 'Tab' or '?' is able to show all register modes

<*1-15*> is the level, its range between 1 and 15

LINE: the command needs to be configured, it supports the command abbreviation

Command Mode: Global mode

Usage Guide: This function cannot change the command itself. LINE must be the whole command format, the command with the abbreviation format must be analyzed successfully. For half-baked command, false command about writing and command that abbreviation cannot be analyzed successfully, the configuration is failure. For changing the command line with the parameter, it should fill in the parameter which is able to be selected discretionarily according to the required format. However, level of the no command is able to be set optionally and it does not affect the result. When using no command, LINE must be the configured command line. If the command line with the parameter, the parameter must be matched with the configured command. (After configure the privilege of enable command, please add command **authencation line console login local** and configure corresponding privilege username password to ensure users can enter privilege mode again. If console link in usual user mode after complete configuration through other login way, please input exit or quit again, it will prompt user to input user name password to enter privilege mode.)

Example: Change the level of **show ip route** command to level 5.

Switch(config)#privilege exec level 5 show ip route

Change the level of **peer A.B.C.D** command to level 6.

Switch(config)#privilege router-msdp level 6 peer 1.2.3.4

Restore the original level for **show ip route** command.

Switch(config)#no privilege exec level 5 show ip route

Restore the original level for **peer A.B.C.D** command.

Switch(config)#no privilege router-msdp level 6 peer 1.2.3.4

1.1.1.24 privilege mode level <1-15> all

This command is not supported by the switch.

1.1.1.25 reload

Command: reload
Function: Warm reset the switch.
Command mode: Admin Mode.
Usage Guide: The user can use this command to restart the switch without power off.

1.1.1.26 service password-encryption

Command: service password-encryption
no service password-encryption
Function: Encrypt system password. The "**no service password-encryption**" command cancels the encryption.
Command mode: Global Mode
Default: No service password-encryption by system default
Usage guide: The current unencrypted passwords as well as the coming passwords configured by password, enable password, ip ftp and username command will be encrypted by executed this command. no service password-encryption cancels this function however encrypted passwords remain unchanged.
Example: Encrypt system passwords
Switch(config)#service password-encryption

1.1.1.27 service terminal-length

Command: service terminal-length <0-512>
no service terminal-length
Function: Configure the columns of characters displayed in each screen on terminal (vty). The "**no service terminal-length**" command cancels the screen shifting operation.
Parameter: Columns of characters displayed on each screen of vty, ranging between 0-512.
Command mode: Global Mode
Usage guide: Configure the columns of characters displayed on each screen of the terminal. The columns of characters displayed on each screen on the telent.ssh client and the Console will be following this configuration.
Example: Set the number of vty threads to 20.
Switch(config)#service terminal-length 20

1.1.1.28 sysContact

Command: sysContact <LINE>
no sysContact
Function: Set the factory contact mode, the "**no sysContact**" command reset the switch to

factory settings.
Parameter: <LINE> is the prompt character string, range from 0 to 255 characters.
Command mode: Global Mode
Default: The factory settings.
Usage guide: The user can set the factory contact mode bases the fact instance.
Example: Set the factory contact mode to test.
Switch(config)#sysContact test

1.1.1.29 sysLocation

Command: sysLocation <LINE>
no sysLocation
Function: Set the factory address, the "**no sysLocation**" command reset the switch to factory settings.
Parameter: <LINE> is the prompt character string, range from 0 to 255 characters.
Command mode: Global Mode
Default: The factory settings.
Usage guide: The user can set the factory address bases the fact instance.
Example: Set the factory address to test.
Switch(config)#sysLocation test

1.1.1.30 set default

Command: set default
Function: Reset the switch to factory settings.
Command mode: Admin Mode.
Usage Guide: Reset the switch to factory settings. That is to say, all configurations made by the user to the switch will disappear. When the switch is restarted, the prompt will be the same as when the switch was powered on for the first time.
Note: After the command, "**write**" command must be executed to save the operation. The switch will reset to factory settings after restart.
Example:
Switch#set default
Are you sure? [Y/N] = y
Switch#write
Switch#reload

1.1.1.31 set boot password

This command is not supported by the switch.

1.1.1.32 setup

Command: setup
Function: Enter the Setup Mode of the switch.
Command mode: Admin Mode.
Usage Guide: Switch provides a Setup Mode, in which the user can configure IP addresses, etc.

1.1.1.33 show clock

Command: show clock
Function: Display the current system clock.
Command mode: Admin and Configuration Mode.
Usage Guide: If the system clock is inaccurate, user can adjust the time by examining the system date and clock.
Example:
Switch#show clock
Current time is TUE AUG 22 11：00：01 2002
Command related: clock set

1.1.1.34 show cpu usage

Command: show cpu usage [<slotno>]
Function: Show CPU usage rate.
Command mode: Admin and configuration mode.
Usage Guide: Check the current usage of CPU resource by **show cpu usage** command. Only **the *chassis switch*** uses **slotno** parameter which is used to show the CPU usage rate of the card on specified slot, if there is no parameter, the default is current card.
Example: Show the current usage rate of CPU.
Switch#show cpu usage
Last 5 second CPU IDLE: 87%
Last 30 second CPU IDLE: 89%
Last 5 minute CPU IDLE: 89%
From running CPU IDLE: 89%

1.1.1.35 show cpu utilization

Command: show cpu utilization
Function: Show the current CPU utilization rate.
Parameter: None.
Default: None.
Command mode: Admin mode.
Usage Guide: This command is used to show CPU utilization rate in the past 5 seconds, 30 seconds and 5 minutes.
Example: Show CPU utilization rate.
Switch#show cpu utilization

Last 5 second CPU USAGE: 9%
Last 30 second CPU USAGE: 11%
Last 5 minute CPU USAGE: 11%
From running CPU USAGE: 11%

1.1.1.36 show memory usage

Command: show memory usage [<slotno>]
Function: Show memory usage rate.
Command mode: Admin and configuration mode.
Usage Guide: Check the current usage of memory resource by **show memory usage** command. Only **the *chassis switch*** uses **slotno** parameter which is used to show the memory usage rate of card on the specified slot, if there is no parameter, the default is current card.
Example: Show the current usage rate of the memory.
Switch#show memory usage
The memory total 128 MB, free 58914872 bytes, usage is 56.10%

1.1.1.37 show privilege

Command: show privilege
Function: Show privilege of the current users.
Parameter: None.
Command Mode: All configuration modes
Example: Show privilege of the current user.
Switch(Config)#show privilege
Current privilege level is 15

1.1.1.38 show privilege mode LINE

Command: show privilege mode LINE
Function: Show the level of the specified command.
Parameters: mode: register mode of the command, 'Tab' or '?' is able to show all register modes
LINE: the command needs to be configured, it supports the command abbreviation
Command Mode: Admin and configuration mode
Usage Guide: LINE must be the whole command format, the abbreviation format is used to the command which can be analyzed successfully. For half-baked command, false command about writing and command that abbreviation cannot be analyzed successfully, the level of them cannot be shown.
Example: Show the level of **privilege** command.
Switch(config)#show privilege exec show ip route
The command : show ip route
Privilege is : 15

1.1.1.39 show tcam usage

Command: show tcam usage
Function: Display the current acl resource information of the switch.
Command mode: All mode.
Usage Guide: This command is used to display the current acl resource information of the switch.
Example:
Switch(Config)#show tcam usage
TCAM Total: 1024 extended (2048 standard) entries on unit: 0
USED: 25 extended entries for l4 function
FREE: 999 extended entries

1.1.1.40 show temperature

Command: show temperature
Function**:** Display the current temputerature of the switch CPU.
Command mode: All mode.
Usage Guide: This command is used to monitor the temperature of the switch CPU.
Example: Display the current temperature of the switch CPU.
Switch(Config)#show temperature

Temperature: 47.0625 ℃

1.1.1.41 show tech-support

Command: show tech-support [no-more]
Function: Display the operational information and the task status of the switch. The technique specialist use this command to diagnose whether the switch operate normally.
Parameter: no-more: Display the operational information and the task status of the switch directly, do not connect the user by “more”.
Command mode: Admin and Configuration Mode.
Usage Guide: This command is used to collect the relative information when the switch operation is malfunctioned.
Example:
Switch#show tech-support

1.1.1.42 show version

Command: show version
Function: Display the version information of the switch.
Command mode: Admin and Configuration Mode.
Usage Guide: This command is used to show the version of the switch, it includes the hardware version and the software version information.

Example:
Switch#show version.

1.1.1.43 username

Command: username <*username*> [privilege <*privilege*>] [password [0 | 7] <*password*>]
no username <*username*>

Function: Configure local login username and password along with its privilege level.

Parameter: <*username*> is the username, its range should not exceed 32 characters. **<*privilege*>** is the maximum privilege level of the commands that the user is able to execute, its value is limited between 1 and 15, and 1 by default. **<*password*>** is the password for the user. If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted (Use 32 bits password encrypted by MD5).

Command Mode: Global Mode.

Usage Guide: There are two available choices for the preferences of the registered commands in the switch. They are 1 and 15. Preference of 1 is for the commands of the normal user configuration mode. Preference of 15 is for the commands registered in modes other than the normal user configuration modes. 16 local users at most can be configured through this command, and the maximum length of the password should be no less than 32.

Notice: The user can log in user and priority after the command configures, before issuing the command authentication line console login local, it should be made sure that at one user has be configured as preference level of 15, in order to login the switch and make configuration changes in privileged mode and global mode. If there are no configured local users with preference level of 15, while only Local authentication is configured for the Console login method, the switch can be login without any authentication. When using the HTTP method to login the switch, only users with preference level of 15 can login the switch, users with preference level other than 15 will be denied.

Example: Configure an administrator account named admin, with the preference level as 15. And configure two normal accounts with its preference level as 1. Then enable local authentication method.

Above all the configurations, only the admin user is able to login the switch in privileged mode through Telnet or Console login method, user1 and user2 can only login the switch in normal user mode through the telnet and console login method. For HTTP login method, only the admin user can pass the authentication configuration, user1 and user2 will be denied.

Switch(config)#username admin privilege 15 password 0 admin
Switch(config)# username user1 privilege 1 password 7
4a7d1ed414474e4033ac29ccb8653d9b (The password is 32 bits password encrypted by MD5)
Switch(config)# username user2 password 0 user2
Switch(config)# authentication line console login local

1.1.1.44 web-auth privilege <1-15>

Command: web-auth privilege <1-15>

no web-auth privilege

Function: Configure the level of logging in the switch by web.

Parameter: <1-15>: Appoint the level of logging in the switch by web and the range is from 1 to 15.

Command Mode: Global Mode.

Default: 15.

Usage Guide: After configured the level of logging in the switch by web, only the user with the level that is equal to or higher than it can login in the switch by web.

Example: Configure the level of logging in the switch by web as 10.

Switch(config)# web-auth privilege 10

1.1.1.45 write

Command: write

Function: Save the currently configured parameters to the Flash memory.

Command mode: Admin Mode.

Usage Guide: After a set of configuration with desired functions, the setting should be saved to the specified configuration file, so that the system can revert to the saved configuration automatically in the case of accidentally powered off or power failure. This is the equivalent to the **copy running-config startup-config** command.

1.1.1.46 write running-config

Command: write running-config [<*startup-config-file-name*>]

Function: Save the current running config as .cfg file to Flash Memory.

Parameters: <*startup-config-file-name*> is the full path of the cfg file. The format of which is as follows:

1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between two parts.

2. The suffix of all file names should be .cfg.

3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 121 characters.

Command Mode: Admin Mode.

Usage Guide: Config file saved by Flash Memory can be used for startup file.

Example: Save the current running config as .cfg file with name of 123.

Switch#write running-config 123.cfg

1.1.2 Telnet

1.1.2.1 aaa authorization config-commands

Command: aaa authorization config-commands

no aaa authorization config-commands

Function: Enable command authorization function for the login user with VTY (login with Telnet and SSH). The no command disables this function. Only enabling this command and configuring command authorization manner, it will request to authorize when executing some command.

Default: Disable.

Command Mode: Global Mode.

Usage Guide: Only after configuring this command and configuring command authorization manner and authorization selection priority of login user with VTY, it can be authorized when configuring command with corresponding command level for login user with VTY.

Example: Enable VTY command authorization function.

Switch(config)# aaa authorization config-commands

1.1.2.2 accounting exec

Command: accounting line {console | vty} exec {start-stop | stop-only | none} method1 [method2…]

no accounting line {console | vty} exec

Function: Configure the list of the accounting method for the login user with VTY (login with Telnet and SSH) and Console. The no command restores the default accounting method.

Parameters: line selects the accounting line, including **console**, **vty** (telnet and ssh); **start-stop** sends the accounting start or the accounting stop when the user is logging or exit the login; **stop-only** sends the accounting stop when the user exits the login only; **none** does not send the accounting start or the accounting stop; **method** is the list of the accounting method, it only supports **tacacs** keyword; **tacacs** uses the remote TACACS+ server to count.

Default: There is no accounting.

Command Mode: Global Mode.

Usage Guide: console and **vty** login method are able to set the corresponding accounting method respectively, the accounting method only supports TACACS+ method currently.

Example: Configure the login accounting with the telnet method.

Switch(config)#accounting line vty exec start-stop tacacs

1.1.2.3 authentication enable

Command: authentication enable method1 [method2…]

no authentication enable

Function: Configure the list of the enable authentication method. The no command restores the default authentication method.

Parameters: method is the list of the authentication method, it must be among **local**, **tacacs** and **radius** keywords; **local** uses the local database to authenticate; **tacacs** uses the remote TACACS+ authentication server to authenticate; **radius** uses the remote RADIUS authentication server to authenticate.

Default: The local authentication is enable command by default.

Command Mode: Global Mode.

Usage Guide: The enable authentication method can be any one or combination of Local, RADIUS and TACACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

Example: Configure the enable authentication method to be tacacs and local.

Switch(config)#authentication enable tacacs local

1.1.2.4 authentication ip access-class

Command: authentication ip access-class {<num-std>|<name>}

no authentication ip access-class

Function: Binding standard IP ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.

Parameters: <num-std> is the access-class number for standard numeric ACL, ranging between 1-299; <name> is the access-class name for standard ACL, the character string length is ranging between 1 and 64.

Default: The binding ACL to Telnet/SSH/Web function is closed by default.

Command Mode: Global Mode.

Example: Binding standard IP ACL protocol to access-class 1.

Switch(config)#authentication ip access-class 1 in

1.1.2.5 authentication ipv6 access-class

Command: authentication ipv6 access-class {<num-std>|<name>} in

no authentication ipv6 access-class

Function: Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.

Parameters: <num-std> is the access-class number for standard numeric ACL, ranging between 500-599; <name> is the access-class name for standard ACL, the character string length is ranging between 1 and 64.

Default: The binding ACL to Telnet/SSH/Web function is closed by default.

Command Mode: Global Mode.

Example: Binding standard IP ACL protocol to access-class 500.

Switch(config)#authentication ipv6 access-class 500 in

1.1.2.6 authentication line login

Command: authentication line {console | vty | web} login method1 [method2…]

no authentication line {console | vty | web} login

Function: Configure VTY (login with Telnet and SSH), Web and Console, so as to select the list of the authentication method for the login user. The no form command restores the default authentication method.

Parameters: line selects the login line, including **console**, **vty** (telnet and ssh) and **web**; **method** is the list of the authentication method, it must be among **local**, **tacacs** and **radius** keywords; **local** uses the local database to authenticate; **tacacs** uses the remote TACACS+ authentication server to authenticate; **radius** uses the remote RADIUS authentication server to authenticate.

Default: No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.

Command Mode: Global Mode.

Usage Guide: The authentication method for Console, VTY and Web login can be configured respectively. And authentication method can be any one or combination of Local, RADIUS and TACACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

The **authentication line console login** command is exclusive with the "**login**" command. The **authentication line console login** command configures the switch to use the Console login method. And the **login** command makes the Console login to use the passwords configured by the **password** command for authentication.

If local authentication is configured while no local users are configured, users will be able to login the switch via the Console method.

Example: Configure the telnet and ssh login with the remote RADIUS authentication.

Switch(config)#authentication line vty login radius

Relative Command: aaa enable，radius-server authentication host，tacacs-server authentication host， tacacs-server key

1.1.2.7 authentication securityip

Command: authentication securityip <*ip-addr*>

no authentication securityip <*ip-addr*>

Function: To configure the trusted IP address for Telnet and HTTP login method. The no form of this command will remove the trusted IP address configuration.

Parameters: <*ip-addr*> is the trusted IP address of the client in dotted decimal format which can login the switch.

Default: No trusted IP address is configured by default.

Command Mode: Global Mode.

Usage Guide: IP address of the client which can login the switch is not restricted before the trusted IP address is not configured. After the trusted IP address is configured, only clients with trusted IP addresses are able to login the switch. Up to 32 trusted IP addresses can be configured in the switch.

Example: To configure 192.168.1.21 as the trusted IP address.

Switch(config)# authentication securityip 192.168.1.21

1.1.2.8 authentication securityipv6

Command: authentication securityipv6 *<ipv6-addr>*

no authentication securityipv6 *<ipv6-addr>*

Function: To configure the security IPv6 address for Telnet and HTTP login method. The no form of this command will remove the specified configuration.

Parameters: *<ipv6-addr>* is the security IPv6 address which can login the switch.

Default: No security IPv6 addresses are configured by default.

Command Mode: Global Mode.

Usage Guide: IPv6 address of the client which can login the switch is not restricted before the security IPv6 address is not configured. After the security IPv6 address is configured, only clients with security IPv6 addresses are able to login the switch. Up to 32 security IPv6 addresses can be configured in the switch.

Example: Configure the security IPv6 address is 2001:da8:123:1::1.

Switch(config)# authentication securityipv6 2001:da8:123:1::1

1.1.2.9 authorization

Command: authorization line {console | vty | web} exec method [method…]

no authorization line {console | vty | web} exec

Function: Configure the list of the authorization method for the login user with VTY (login with Telnet and SSH), Web and Console. The no command restores the default authorization method.

Parameters: line selects the authorization line, including **console**, **vty** (telnet and ssh) and **web**; **method** is the list of the authorization method, it must be among **local**, **tacacs** and **radius** keywords; **local** uses the local database to authorize; **tacacs** uses the remote TACACS+ server to authorize; **radius** uses the remote RADIUS server to authorize.

Default: There is no authorization mode.

Command Mode: Global Mode.

Usage Guide: The authorization method for Console, VTY and Web login can be configured respectively. And authorization method can be any one or combination of Local, RADIUS or TACACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authorization method, authorization method of lower preferences will be ignored. To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authorization method; it will attempt the next authorization method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server

should be configured before the TACACS configuration method can be used.

The local users adopt username command permission while authorization command is not configured, the users login the switch via RADIUS/TACACS method and works under common mode.

Example: Configure the telnet authorization method to RADIUS.

Switch(config)#authorization line vty exec radius

1.1.2.10 authorization line vty command

Command: authorization line vty command <1-15> {local | radius | tacacs} (none|)

no authorization line vty command <1-15>

Function: Configure command authorization manner and authorization selection priority of login user with VTY (login with Telnet and SSH). The no command recovers to be default manner.

Default: The authorization manner is not configured as default.

Command Mode: Global Mode.

Usage Guide: Configure the authorization manner when VTY login user configures command, the manners include any combination of Local, RADIUS and TACACS, the manner of none is just as the last manner. When using combination authorization manners, the priority of the front authorization manner is the highest and the others are in descending order; if the authorization with high priority passed, it is successful to configure command and the back authorization manner will be ignored. Notice: as long as one authorization manner receives a clear response of the corresponding agreement. Whether it is received or refused, the next authorization manner will not be attempted. If the clear response is not received, try the next manner. When using RADIUS authorization, AAA function must be enabled and configure RADIUS server. when using TACACS authorization, TACACS server must be configured. None is the manner of escaping and it only can be the last manner. This manner returns to passed authorization directly and it is successful to configure the command.

Example: Configure level 1 command authorization manner of telnet login user as TACACS.

Switch(config)#authorization line vty command 1 tacacs

1.1.2.11 clear line vty <0-31>

Command: clear line vty <0-31>

Function: Delete the logged user information on the appointed line, force user to get down the line who logs in through telnet or ssh.

Command mode: Admin Mode.

Usage guide: After inputting this command, there is need to judge for this command, “Confirm[Y/N]: “, when inputting “Y“ or “y“, run to delete; when inputting “N“, do not run to delete, print the notice information only. When inputting other characters, do not run to delete.

1.1.2.12 crypto key clear rsa

Command: crypto key clear rsa

Function: Clear the secret key of ssh.
Command mode: Admin Mode.

1.1.2.13 terminal length

Command: terminal length <0-512>
terminal no length
Function: Set length of characters displayed in each screen on terminal; the "**terminal no length**" cancels the screen switching operation and display content once in all.
Parameter: Length of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display).
Command mode: Admin Mode.
Default: Default Length is 25.
Usage guide: Set length of characters displayed in each screen on terminal, so that the-More-message will be shown when displayed information exceeds the screen. Press any key to show information in next screen. Default length is 25.
Example: Configure length of characters in each display to 20.
Switch#terminal length 20

1.1.2.14 terminal monitor

Command: terminal monitor
terminal no monitor
Function: Copy debugging messages to current display terminal; the "**terminal no monitor**" command restores to the default value.
Command mode: Admin Mode.
Usage guide: Configures whether the current debugging messages is displayed on this terminal. If this command is configured on telnet or SSH clients, debug messages will be sent to that client. The debug message is displayed on console by default.
Example:
Switch#terminal monitor

1.1.2.15 telnet

Command: telnet [vrf <*vrf-name*>] {<*ip-addr*> | <*ipv6-addr*> | host <*hostname*>} [<*port*>]
Function: Login on the remote host by Telnet
Parameter: <*vrf-name*> is the specific VRF name; **<*ip-addr*>** is the IP address of the remote host, shown in dotted decimal notation; **<*ipv6-addr*>** is the IPv6 address of the remote host; **<*hostname*>** is the name of the remote host, containing max 64 characters; **<*port*>** is the port number, ranging between 0 and 65535.
Command Mode: Admin Mode.
Usage Guide: This command is used when the switch is applied as Telnet client, for logging on remote host to configure. When a switch is applied as a Telnet client, it can only establish one

TCP connection with the remote host. To connect to another remote host, the current TCP connection must be disconnected with a hotkey “CTRL+ \”. To telnet a host name, mapping relationship between the host name and the IP/IPv6 address should be previously configured. For required commands please refer to ip host and ipv6 host. In case a host corresponds to both an IPv4 and an IPv6 addresses, the IPv6 should be preferred when telneting this host name.

Example: The switch telnets to a remote host whose IP address is 20.1.1.1.

Switch#telnet 20.1.1.1 23
Connecting Host 20.1.1.1 Port 23...
Service port is 23
Connected to 20.1.1.1
login:123
password:***
router>

1.1.2.16 telnet server enable

Command: telnet server enable
no telnet server enable

Function: Enable the Telnet server function in the switch: the “no telnet server enable” command disables the Telnet function in the switch.

Default: Telnet server function is enabled by default.

Command mode: Global Mode

Usage Guide: This command is available in Console only. The administrator can use this command to enable or disable the Telnet client to login to the switch.

Example: Disable the Telnet server function in the switch.

Switch(config)#no telnet server enable

1.1.2.17 telnet-server max-connection

Command: telnet-server max-connection {<max-connection-number> | default}

Function: Configure the max connection number supported by the Telnet service of the switch.

Parameters: <max-connection-number>: the max connection number supported by the Telnet service, ranging from 1 to 16. The default option will restore the default configuration.

Default: The system default value of the max connection number is 5.

Command Mode: Global Mode

Usage Guide: None.

Example: Set the max connection number supported by the Telnet service as 10.

Switch(config)#telnet-server max-connection 10

1.1.2.18 ssh-server authentication-retries

Command: ssh-server authentication-retries <authentication-retries>
no ssh-server authentication-retries

Function: Configure the number of times for retrying SSH authentication; the "**no ssh-server authentication-retries**" command restores the default number of times for retrying SSH authentication.
Parameter: < authentication-retries > is the number of times for retrying authentication; valid range is 1 to 10.
Command mode: Global Mode
Usage Guide: None.
Default: The number of times for retrying SSH authentication is 3 by default.
Example: Set the time for retrying SSH authentication to 5.
Switch(config)#ssh-server authentication-retries 5

1.1.2.19 ssh-server enable

Command: ssh-server enable
no ssh-server enable
Function: Enable SSH function on the switch; the "**no ssh-server enable**" command disables SSH function.
Command mode: Global Mode
Default: SSH function is disabled by default.
Usage Guide: In order that the SSH client can log on the switch, the users need to configure the SSH user and enable SSH function on the switch.
Example: Enable SSH function on the switch.
Switch(config)#ssh-server enable

1.1.2.20 ssh-server host-key create rsa

Command: ssh-server host-key create rsa [modulus < modulus >]
Function: Generate new RSA host key.
Parameter: modulus is the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024.
Command mode: Global Mode
Default: The system uses the key generated when the ssh-server is started at the first time.
Usage Guide: This command is used to generate the new host key. When SSH client logs on the server, the new host key is used for authentication. After the new host key is generated and "write" command is used to save the configuration, the system uses this key for authentication all the time. Because it takes quite a long time to compute the new key and some clients are not compatible with the key generated by the modulus 2048, it is recommended to use the key which is generated by the default modulus 1024.
Example: Generate new host key.
Switch(config)#ssh-server host-key create rsa

1.1.2.21 ssh-server max-connection

Command: ssh-server max-connection {<max-connection-number>|default}
Function: Configure the max connection number supported by the SSH service of the switch.
Parameters: <max-connection-number>: the max connection number supported by the SSH service, ranging from 1 to 16. The default option will restore the default configuration.
Default: The system default value of the max connection number is 5.
Command Mode: Global Mode
Usage Guide: None.
Example: Set the max connection number supported by the SSH service as 10.
Switch(config)#ssh-server max-connection 10

1.1.2.22 ssh-server timeout

Command: ssh-server timeout <timeout>
no ssh-server timeout
Function: Configure timeout value for SSH authentication; the "**no ssh-server timeout**" command restores the default timeout value for SSH authentication.
Parameter: ***<timeout>*** is timeout value; valid range is 10 to 600 seconds.
Command mode: Global Mode
Default: SSH authentication timeout is 180 seconds by default.
Usage Guide: This command is used to set SSH authentication timeout, the default timeout is 180 seconds.
Example: Set SSH authentication timeout to 240 seconds.
Switch(config)#ssh-server timeout 240

1.1.2.23 show crypto key

Command: show crypto key
Function: Show the secret key of ssh.
Command mode: Admin Mode.

1.1.2.24 show ssh-server

Command: show ssh-server
Function: Display SSH state and users which log on currently.
Command mode: Admin Mode.
Example:
Switch#show ssh-server
ssh server is enabled
ssh-server timeout 180s
ssh-server authentication-retries 3
ssh-server max-connection number 6
ssh-server login user number 2

1.1.2.25 show telnet login

Command: show telnet login

Function: Display the information of the Telnet client which currently establishes a Telnet connection with the switch.

Command Mode: Admin and Configuration Mode.

Usage Guide: Check the Telnet client messages connected through Telnet with the switch.

Example:

Switch#show telnet login
Authenticate login by local
Login user:
aa

1.1.2.26 show users

Command: show users

Function: Show the user information who logs in through telnet or ssh. It includes line number, user name and user IP.

Command mode: Admin Mode.

Usage Guide: When inputting this command, show the user information who logs in through telnet or ssh. It includes line number, user name and user IP. Because 16 telnet users and 16 ssh users are supported at most currently, vty0-15 are used for telnet, and 16-31 are used for ssh.

Example:

Switch#show users

Line	User	Location
vty 16	a	192.168.1.1
vty 0	admin	192.168.1.2
vty 17	mab	192.168.1.13
vty 1	test	192.168.1.40

1.1.2.27 who

Command: who

Function: Show the current login users with vty.

Parameter: None.

Command Mode: All configuration modes

Example: Show the current login users with vty.

Switch#who
Telnet user a login from 192.168.1.20

1.1.3 Configuring Switch IP

1.1.3.1 interface vlan

Command: interface vlan <*vlan-id*>

no interface vlan <*vlan-id*>

Function: Enter the VLAN interface configuration mode; the no operation of this command will delete the existing VLAN interface.

Parameters: <*vlan-id*> is the VLAN ID of an existing VLAN, ranging from 1 to 4094.

Command Mode: Global Configuration Mode.

Usage Guide: Users should first make sure the existence of a VLAN before configuring it. User "**exit**" command to quit the VLAN interface configuration mode back to the global configuration mode.

Example: Enter the VLAN interface configuration mode of VLAN1.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#

1.1.3.2 interface ethernet 0

This command is not supported by the switch.

1.1.3.3 ip address

Command: ip address <*ip-address*> <*mask*> [secondary]

no ip address [<*ip-address*> <*mask*>] [secondary]

Function: Set the IP address and mask for the specified VLAN interface; the "**no ip address <*ip address*> <*mask*> [secondary]**" command deletes the specified IP address setting.

Parameter: <*ip-address*> is the IP address in dot decimal format; **<*mask*>** is the subnet mask in dot decimal format; **[secondary]** indicates the IP configured is a secondary IP address.

Default: No IP address is configured upon switch shipment.

Command mode: VLAN Interface Mode

Usage Guide: A VLAN interface must be created first before the user can assign an IP address to the switch.

Example: Set 10.1.128.1/24 as the IP address of VLAN1 interface.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0

Switch(Config-if-Vlan1)#exit

Switch(config)#

Relative Command: ip bootp-client enable, ip dhcp-client enable

1.1.3.4 ipv6 address

Command: ipv6 address <*ipv6address | prefix-length*> [eui-64]

no ipv6 address <*ipv6address | prefix-length*> [eui-64]

Function: Configure aggregatable global unicast address, site-local address and link-local address for the interface.

Parameters: ***<ipv6address>*** is the prefix of an IPV6 address; ***<prefix-length>***is the length of the prefix of an IPV6 address, ranging from 3 to 128; **eui-64** means that the eui64 interface id of the interface will automatically create an IPV6 address.

Command Mode: Interface Configuration Mode.

Default: None.

Usage Guide: The prefix of an IPV6 address should not be a multicast address, or other kinds of IPV6 addresses with specific usage. Different layer-three VLAN interfaces are forbidden to share a same address prefix. As for any global unicast address, the prefix should be limited in the range from 2001:: to 3fff ::, with a length no shorter than 3. And the prefix length of a site-local address or a link-local address should not be shorter than 10.

Examples: Configure an IPV6 address at the layer-three interface of VLAN1: set the prefix as 2001:3f:ed8::99, the length of which is 64.

Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64

1.1.3.5 ip bootp-client enable

Command: ip bootp-client enable

no ip bootp-client enable

Function: Enable the switch to be a BootP Client and obtain IP address and gateway address through BootP negotiation; the "**no ip bootp-client enable**" command disables the BootP Client function and releases the IP address obtained in BootP.

Default: BootP client function is disabled by default.

Command mode: VLAN Interface Mode

Usage Guide: Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any two methods for obtaining IP address is not allowed. Note: To obtain IP address via BootP, a DHCP server or a BootP server is required in the network.

Example: Get IP address through BootP.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip bootp-client enable

Switch (Config-if-Vlan1)#exit

Switch(config)#

Relative command: ip address, ip dhcp-client enable

1.1.3.6 ip dhcp-client enable

Command: ip dhcp-client enable

no ip dhcp-client enable

Function: Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip dhcp-client enable**" command disables the DHCP client function and releases the IP address obtained in DHCP. Note: To obtain IP address via DHCP, a DHCP server is required in the network.

Default: the DHCP client function is disabled by default.
Command mode: VLAN Interface Mode、Interface Mode.
Usage Guide: Obtaining IP address by DHCP, Manual configuration and BootP are mutually exclusive, enabling any 2 methods for obtaining an IP address is not allowed.
Example: Getting an IP address through DHCP.
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dhcp-client enable
Switch(Config-if-Vlan1)#exit
Switch(config)#

1.1.3.7 ip dhcp-client upgrade enable

Command: ip dhcp-client upgrade enable
no ip dhcp-client upgrade enable
Function: Enables the switch to realize the automatic upgrade function of img / cfg file through DHCP option66 and option 67; the no operation of this command is to close the function of automatic upgrade of img / cfg file through DHCP option66 and option 67.
Default: The automatic upgrade function of DHCP client is disabled by default.
Command mode: VLAN Interface Mode、Interface Mode.
Usage Guide: Enables the switch to realize the automatic upgrade function of img / cfg file through DHCP option66 and option 67.
Example: Enables DHCP automatic upgrade function.
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dhcp-client enable
Switch(Config-if-Vlan1)#ip dhcp-client upgrade enable
Switch(Config-if-Vlan1)#exit
Switch(config)#
Relative command: ip dhcp-client enable

1.1.3.8 ip dhcp-client upgrade begin

Command: ip dhcp-client upgrade begin
Function: Starts up the switch to realize the automatic upgrade function of img / cfg file through DHCP option66 and option 67.
Default: The automatic upgrade function of DHCP client is closed by default.
Command mode: VLAN Interface Mode、Interface Mode.
Usage Guide: Starts up the switch to realize the automatic upgrade function of img / cfg file through DHCP option66 and option 67.
Example: Starts up DHCP automatic upgrade function.
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dhcp-client enable

```
Switch(Config-if-Vlan1)#ip dhcp-client upgrade enable
Switch(Config-if-Vlan1)#ip dhcp-client upgrade begin
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

Relative command: ip dhcp-client enable, ip dhcp-client upgrade enable

1.1.4 SNMP

1.1.4.1 debug snmp mib

Command: debug snmp mib

no debug snmp mib

Function: Enable the SNMP mib debugging; the "**no debug snmp mib**" command disables the debugging.

Command Mode: Admin Mode.

Usage Guide: When user encounters problems in applying SNMP, the SNMP debugging is available to locate the problem causes.

Example:

Switch#debug snmp mib

1.1.4.2 debug snmp kernel

Command: debug snmp kernel

no debug snmp kernel

Function: Enable the SNMP kernel debugging; the "**no debug snmp kernel**" command disables the debugging function.

Command Mode: Admin Mode.

Usage Guide: When user encounters problems in applying SNMP, the SNMP debugging is available to locate the problem causes.

Example:

Switch#debug snmp kernel

1.1.4.3 rmon enable

Command: rmon enable

no rmon enable

Function: Enable RMON; the "**no rmon enable**" command disables RMON.

Command mode: Global Mode

Default: RMON is enabled by default.

Example:

Enable RMON.

```
Switch(config)#rmon enable
```

Disable RMON.
Switch(config)#no rmon enable

1.1.4.4 show private-mib oid

Command: show private-mib oid
Function: Show the original oid of the private mib.
Command mode: Admin and configuration mode.
Usage Guide: Check the beginning oid of the private mib by **show private-mib oid** command.
Example: Show the original oid of the private mib.
Switch#show private-mib oid
Private MIB OID:1.3.6.1.4.1.6339

1.1.4.5 show snmp

Command: show snmp
Function: Display all SNMP counter information.
Command mode: Admin and Configuration Mode.
Example:
Switch#show snmp
0 SNMP packets input
0 Bad SNMP version errors
0 Unknownnnnn community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs
0 SNMP packets output
0 Too big errors (Max packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Get-response PDUs
0 SNMP trap PDUs

Displayed information	Explanation
snmp packets input	Total number of SNMP packet inputs.
bad snmp version errors	Number of version information error packets.
unknownnnnn community name	Number of community name error packets.

illegal operation for community name supplied	Number of permission for community name error packets.
encoding errors	Number of encoding error packets.
number of requested variable	Number of variables requested by NMS.
number of altered variables	Number of variables set by NMS.
get-request PDUs	Number of packets received by “get” requests.
get-next PDUs	Number of packets received by “getnext” requests.
set-request PDUs	Number of packets received by “set” requests.
snmp packets output	Total number of SNMP packet outputs.
too big errors	Number of “Too_ big” error SNMP packets.
maximum packet size	Maximum length of SNMP packets.
no such name errors	Number of packets requesting for non-existent MIB objects.
bad values errors	Number of “Bad_values” error SNMP packets.
general errors	Number of “General_errors” error SNMP packets.
response PDUs	Number of response packets sent.
trap PDUs	Number of Trap packets sent.

1.1.4.6 show snmp engineid

Command: show snmp engineid

Function: Display the engine ID commands.

Command Mode: Admin and Configuration Mode.

Example:

Switch#show snmp engineid

SNMP engineID:3138633303f1276c Engine Boots is:1

Displayed Information	Explanation
SNMP engineID	Engine number
Engine Boots	Engine boot counts

1.1.4.7 show snmp group

Command: show snmp group

Function: Display the group information commands.

Command Mode: Admin and Configuration Mode.

Example:

Switch#show snmp group

Group Name:initial Security Level:noAuthnoPriv

Read View:one
Write View:<no writeview specified>
Notify View:one

Displayed Information	Explanation
Group Name	Group name
Security level	Security level
Read View	Read view name
Write View	Write view name
Notify View	Notify view name
<no writeview specified>	No view name specified by the user

1.1.4.8 show snmp mib

Command: show snmp mib
Function: Display all MIB supported by the switch.
Command Mode: Admin and Configuration Mode.

1.1.4.9 show snmp status

Command: show snmp status
Function: Display SNMP configuration information.
Command mode: Admin and Configuration Mode.
Example:
Switch#show snmp status
Trap enable
RMON enable
Community Information:
V1/V2c Trap Host Information:
V3 Trap Host Information:
Security IP Information:

Displayed information	Description
Community string	Community string
Community access	Community access permission
Trap-rec-address	IP address which is used to receive Trap.
Trap enable	Enable or disable to send Trap.
SecurityIP	IP address of the NMS which is allowed to access Agent

1.1.4.10 show snmp user

Command: show snmp user
Function: Display the user information commands.

Command Mode: Admin and Configuration Mode.

Example:

Switch#show snmp user

User name: initialsha

Engine ID: 1234567890

Auth Protocol:MD5 Priv Protocol:DES-CBC

Row status:active

Displayed Information	Explanation
User name	User name
Engine ID	Engine ID
Priv Protocol	Employed encryption algorithm
Auth Protocol	Employed identification algorithm
Row status	User state

1.1.4.11 show snmp view

Command: show snmp view

Function: Display the view information commands.

Command Mode: Admin and Configuration Mode.

Example:

Switch#show snmp view

View Name:readview 1. -Included active

1.3. Excluded active

Displayed Information	Explanation
View Name	View name
1.and1.3.	OID number
Included	The view includes sub trees rooted by this OID
Excluded	The view does not include sub trees rooted by this OID
active	State

1.1.4.12 snmp-server community

Command: snmp-server community {ro | rw} {0 | 7} *<string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}] [read *<read-view-name>*] [write *<write-view-name>*]

no snmp-server community *<string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]

Function: Configure the community string for the switch; the no command deletes the configured community string.

Parameter: *<string>* is the configured community string. If key option is set as 0, the specified

community string is not encrypted, if key option is set as 7, the specified community string is encrypted;

ro | rw is the specified access mode to MIB, **ro** for read-only and **rw** for read-write;

<num-std> is the access-class number for standard numeric ACL, ranging between 1-99;

<name> is the access-class name for standard ACL, the character string length is ranging between 1-64;

<ipv6-num-std> is the access-class number for standard numeric IPv6 ACL, ranging between 500-599;

<name> is the access-class name for standard IPv6 ACL, the character string length is ranging between 1-64;

<read-view-name> is the name of readable view which includes 1-32 characters;

<write-view-name> is the name of writable view which includes 1-32 characters.

Command mode: Global Mode

Usage Guide: The switch supports up to 4 community strings. It can realize the access-control for specifically community view by binding the community name to specifically readable view or writable view.

Example:

Add a community string named “private” with read-write permission.

Switch(config)#snmp-server community rw 0 private

Add a community string named “public” with read-only permission.

Switch(config)#snmp-server community ro 0 public

Modify the read-write community string named “private” to read-only.

Switch(config)# snmp-server community ro 0 private

Delete community string “private”.

Switch(config)#no snmp-server community 0 private

Bind the read-only community string “public” to readable view “pviewr”.

Switch(config)#snmp-server community ro 0 public read pviewr

Bind the read-write community string “private” to readable view “pviewr” and writable view “pvieww”.

Switch(config)#snmp-server community rw 0 private read pviewr write pvieww

1.1.4.13 snmp-server ddm-electronic-hidden

Command: snmp-server ddm-electronic-hidden { enable | disable }

Function: Configure whether to automatically skip electrical ports when reading DDM information through SNMP.

Parameter: Enable to automatically skip the electrical port; disable means not automatically skipping the electrical port.

Command mode: Global mode.

Default: Not automatically skipping the electrical port.

Usage guide: When obtaining DDM information through SNMP, skipping the electrical port can speed up SNMP reading and avoid SNMP timeout.

Example: Automatically skip electrical ports when reading DDM information through SNMP
Switch(config)# snmp ddm-electronic-hidden enable

1.1.4.14 snmp-server ddm-mib

Command: snmp-server ddm-mib { enable | disable }
Function: Enable or disable the function of reading DDM information through SNMP. Default not enabled.
Parameter: Enable to turn on this feature; Disable to turn off this feature.
Command mode: Global mode.
Default: Default not enabled.
Usage guide: Reading DDM information consumes a large amount of CPU, so this feature is not enabled by default.
Example: Enable the function of obtaining DDM information through SNMP
Switch(config)# snmp ddm-mib enable

1.1.4.15 snmp-server dst-port

Command: snmp-server dst-port <port-number>
no snmp-server dst-port
Function: Configure the UDP destination port number for SNMP. The 'no' command is used to restore the default destination port.
Parameter: <port-number> range 1025～65535.
Command mode: Global mode.
Default: Default destination port 161.
Usage guide: After configuring the SNMP destination port number, the source port number of the SNMP packets sent by the device will be the configured value. When receiving packets, only SNMP requests with the destination port number set to the configured value will be processed.
Example: Configure the UDP destination port number for SNMP to 1400。
Switch(config)# snmp-server dst-port 1400

1.1.4.16 snmp-server enable

Command: snmp-server enable
no snmp-server enable
Function: Enable the SNMP proxy server function on the switch. The "**no snmp-server enable**" command disables the SNMP proxy server function
Command mode: Global mode
Default: SNMP proxy server function is disabled by system default.
Usage guide: To perform configuration management on the switch with network manage software, the SNMP proxy server function has to be enabled with this command.
Example: Enable the SNMP proxy server function on the switch.
Switch(config)#snmp-server enable

1.1.4.17 snmp-server enable traps

Command: snmp-server enable traps

no snmp-server enable traps

Function: Enable the switch to send Trap message; the "**no snmp-server enable traps**" command disables the switch to send Trap message.

Command mode: Global Mode

Default: Forbid to send Trap message.

Usage Guide: When Trap message is enabled, if Down/Up in device ports or of system occurs, the device will send Trap messages to NMS that receives Trap messages.

Example:

Enable to send Trap messages.

Switch(config)#snmp-server enable traps

Disable to send Trap messages.

Switch(config)#no snmp-server enable traps

1.1.4.18 snmp-server engineid

Command: snmp-server engineid *<engine-string>*

no snmp-server engineid

Function: Configure the engine ID; the "no" form of this command restores to the default engine ID.

Command Mode: Global mode

Parameter: *<engine-string>* is the engine ID shown in 1-32 digit hex characters.

Default: Default value is the company ID plus local MAC address.

Usage Guide: None

Example: Set current engine ID to A66688999F

Switch(config)#snmp-server engineid A66688999F

Restore the default engine ID

Switch(config)#no snmp-server engineid

1.1.4.19 snmp-server fdbMacInfoTable-mib

Command: snmp-server fdbMacInfoTable-mib {enable | disable}

Function: Open the switch as a SNMP proxy server to obtain FDB statistics through mib. Parameter: enable turns this feature on; disable turns this feature off.

Command mode: Global configuration mode.

Default situation: The system default turns off this function.

Use Guide: To configure the switch through the network management software, you must first use this command to open the SNMP proxy server function of the switch.

Example: Open the switch as a SNMP proxy server to obtain FDB statistics through the mib.

Switch(config)# snmp-server fdbMacInfoTable-mib enable

1.1.4.20 snmp-server group

Command: snmp-server group <group-string> {NoauthNopriv | AuthNopriv | AuthPriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]] [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]

no snmp-server group *<group-string>* {NoauthNopriv | AuthNopriv | AuthPriv} [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]

Function: This command is used to configure a new group; the "no" form of this command deletes this group.

Command Mode: Global Mode

Parameter: <group-string> group name which includes 1-32 characters

NoauthNopriv Applies the non recognizing and non encrypting safety level

AuthNopriv Applies the recognizing but non encrypting safety level

AuthPriv Applies the recognizing and encrypting safety level

read-string Name of readable view which includes 1-32 characters

write-string Name of writable view which includes 1-32 characters

notify-string Name of trappable view which includes 1-32 characters

<num-std> is the access-class number for standard numeric ACL, ranging between 1-99;

<name> is the access-class name for standard ACL, the character string length is ranging between 1-64;

<ipv6-num-std> is the access-class number for standard numeric IPv6 ACL, ranging between 500-599;

<name> is the access-class name for standard IPv6 ACL, the character string length is ranging between 1-64.

Usage Guide: There is a default view "v1defaultviewname" in the system. It is recommended to use this view as the view name of the notification. If the read or write view name is empty, corresponding operation will be disabled.

Example: Create a group CompanyGroup, with the safety level of recognizing andencrypting, the read viewname isreadview, and the writing is disabled.

Switch (config)#snmp-server group CompanyGroup AuthPriv read readview

Delete group

Switch (config)#no snmp-server group CompanyGroup AuthPriv

1.1.4.21 snmp-server host

Command: snmp-server host { *<host-ipv4-address>* / *<host-ipv6-address>* } {{v1 | v2c {0 | 7 | }} | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <*user-string*>

no snmp-server host { *<host-ipv4-address>* / *<host-ipv6-address>* } {{v1 | v2c { 0 | 7}} | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <*user-string*>

Function: As for the v1/v2c versions this command configures the IPv4 or IPv6 address and Trap community character string of the network manage station receiving the SNMP Trap message. And for v3 version, this command is used for receiving the network manage station IPv4 or IPv6

address and the Trap user name and safety level; the “no” form of this command cancels this IPv4 or IPv6 address.

Command Mode: Global Mode.

Parameter: ***<host-ipv4-addr>*** is IP address of NMS management station which receives Trap message.

<host-ipv6-addr> is IPv6 address of NMS management station which receives Trap message.

v1 | v2c | v3 is the version number when sending the trap.

NoauthNopriv | AuthNopriv | AuthPriv is the safety level v3 trap is applied, which may be non encrypted and non authentication, non encrypted and authentication, encrypted and authentication.

<user-*string*> is the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3. If key option is set as 0, the specified community string is not encrypted, if key option is set as 7, the specified community string is encrypted;

Usage Guide: The Community character string configured in this command is the default community string of the RMON event group. If the RMON event group has no community character string configured, the community character string configured in this command will be applied when sending the Trap of RMON, and if the community character string is configured, its configuration will be applied when sending the RMON trap. This command allows to configure IPv4 or IPv6 addresses of SNMP management station that receive Trap message at the same time, but IPv4 and IPv6 addresses of v1 and v2c version are less than 8 in all.

Example:

Configure an IP address to receive Trap

Switch(config)#snmp-server host 1.1.1.5 v1 usertrap

Delete an IPv6 address to receive Trap.

Switch(config)#no snmp-server host 2001::1 v1 usertrap

1.1.4.22 snmp-server packet delay

This command is not supported by the switch.

1.1.4.23 snmp-server securityip

Command: snmp-server securityip *{<ipv4-address> | <ipv6-address>}*

no snmp-server securityip *{<ipv4-address> | <ipv6-address>}*

Function: Configure security IPv4 or IPv6 address allowed to access NMS management station; the no command deletes security IPv4 or IPv6 address configured.

Command Mode: Global Mode.

Parameter: <ipv4-address> is NMS security IPv4 address, dotted decimal notation.

<ipv6-address> is NMS security IPv6 address, colon hexadecimal.

Usage Guide: It is only the consistency between NMS administration station IPv4 or IPv6 address and security IPv4 or IPv6 address configured by the command, so it send SNMP packet could be

processed by switch, the command only applies to SNMP. Allows configuration the IPv4 or IPv6 address of the network manage station receiving the SNMP Trap message, but the IP addresses are less than 20 in all.

Example:

Configure security IP address of NMS management station.

Switch(config)#snmp-server securityip 1.1.1.5

Delete security IPv6 address.

Switch(config)#no snmp-server securityip 2001::1

1.1.4.24 snmp-server securityip

Command: snmp-server securityip {enable | disable}

Function: Enable/disable the security IP address authentication on NMS management station.

Command Mode: Global Mode

Default: Enable the security IP address authentication function.

Example:

Disable the security IP address authentication function.

Switch(config)#snmp-server securityip disable

1.1.4.25 snmp-server trap-resend-interval

Command: snmp-server trap-resend-interval <6-65535>

no snmp-server trap-resend-interval

Function: Set the trap alert sending interval; the 'no' operation of this command restores the default sending interval.

Parameter: ***<6-65535>*** in seconds.

Command Mode: Global Mode.

Default: Default 300s.

Usage Guide: Set TRAP transmission interval and adjust the transmission frequency of TRAP information

Example: Set the trap alarm message sending interval to 500s.

Switch(config)# snmp-server trap-resend-interval 500

1.1.4.26 snmp-server trap-source

Command: snmp-server trap-source {<ipv4-address> | <ipv6-address>}

no snmp-server trap-source {<ipv4-address> | <ipv6-address>}

Function: Set the source IPv4 or IPv6 address which is used to send trap packet, the no command deletes the configuration.

Parameter: <ipv4-address>: IPv4 address is used to send trap packet in dotted decimal notation

<ipv6-address>: IPv6 address is used to send trap packet in colon hexadecimal.

Command Mode: Global Mode.

Usage Guide: If there is no configuration, select the source address according to the interface

address sent by actual trap packet, when configure the IP address, adopt the configured source address as the source address of trap packet.

Example:

Set the IP address which is used to send trap packet.

Switch(config)#snmp-server trap-source 1.1.1.5

Delete the configured source address which is used to send IPv6 trap packet.

Switch(config)#no snmp-server trap-source 2001::1

1.1.4.27 snmp-server trap-threshold

Command：snmp-server trap-threshold {cpu-usage|memory-usage}{<0-100>}

no snmp-server trap-threshold {cpu-usage|memory-usage}

Function: Set the threshold for the switch to send CPU or high memory utilization alarm; the no operation of this command is to restore the default threshold.

Parameter: cpu-usage represents the switch CPU utilization; memory-usage represents the switch memory utilization; <0-100> represents the alarm threshold set as a percentage.

Command mode: Global configuration mode. Use Guide: This feature is not turned on by default.

Example: Set the threshold for this switch to send a high CPU utilization alarm to 70%.

Switch(config)# snmp-server trap-threshold cpu-usage 70

1.1.4.28 snmp-server user

Command: snmp-server user *<use-string>* *<group-string>* [{authPriv {aes|des|3des {0|7} *<word>*}| authNoPriv} auth {md5 | sha} {0|7} *<word>*] [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]

no snmp-server user *<user-string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]

Function: Add a new user to an SNMP group; the "no" form of this command deletes this user.

Command Mode: Global Mode.

Parameter: *<user-string>* is the user name containing 1-32 characters.

<group-string> is the name of the group the user belongs to, containing 1-32 characters.

authPriv use DES or AES or 3DES for the packet encryption.

authNoPriv not use DES for the packet encryption.

auth perform packet authentication.

md5 packet authentication using HMAC MD5 algorithm.

sha packet authentication using HMAC SHA algorithm.

<word > user password, containing 8-32 character. If key option is set as 0, the specified password string is not encrypted, if key option is set as 7, the specified password string is encrypted;

<num-std> is the access-class number for standard numeric ACL, ranging between 1-99;

<name> is the access-class name for standard ACL, the character string length is ranging between 1-64;

<ipv6-num-std> is the access-class number for standard numeric IPv6 ACL, ranging between 500-599;

<name> is the access-class name for standard IPv6 ACL, the character string length is ranging between 1-64.

Usage Guide: If the encryption and authentication is not selected, the default settings will be no encryption and no authentication. If the encryption is selected, the authentication must be done. When deleting a user, if correct username and incorrect group name is inputted, the user can still be deleted.

Example:

Add a new user tester in the UserGroup with an encryption safety level and HMAC md5 for authentication, the password is hellohello

Switch (config)#snmp-server user tester UserGroup authPriv auth md5 hellohello

Delete an User

Switch (config)#no snmp-server user tester

1.1.4.29 snmp-server view

Command: snmp-server view *<view-string>* *<oid-string>* {include | exclude}

no snmp-server view *<view-string>* [*<oid-string>*]

Function: This command is used to create or renew the view information; the “no" form of this command deletes the view information.

Command Mode: Global Mode.

Parameter: ***<view-string>*** view name, containing 1-32 characters.

<oid-string> is OID number or corresponding node name, containing 1-255 characters.

include | exclude, include/exclude this OID.

Usage Guide: The command supports not only the input using the character string of the variable OID as parameter. But also supports the input using the node name of the parameter.

Example:

Create a view, the name is readview, including iso node but not including the iso.3 node

Switch(config)#snmp-server view readview iso include

Switch(config)#snmp-server view readview iso.3 exclude

Delete the view

Switch(config)#no snmp-server view readview

1.1.4.30 switchport updown notification enable

Command: [no] switchport updown notification enable

Function: Enable/disable the function of sending the trap message to the port of UP/DOWN event.

Default: Send the trap message to the port of IP/DOWN event as default.

Command Mode: Port Mode.
Usage Guide: This command can control to send the trap message when the port happens the UP/DOWN event or not. As default, send the trap message to all the ports of UP/DOWN event after enabled snmp trap.
Example: Disable the function of sending the trap message to the port 1/0/1 of the UP/DOWN event.
Switch(config)#in e 1/0/1
Switch(config-if-ethernet1/0/1)#no switchport updown notification enable
Switch(config-if-ethernet1/0/1)#show running-config current-mode
!
Interface Ethernet1/0/1
no switchport updown notification enable

1.1.5 Switch Upgrade

1.1.5.1 copy（FTP）

Command: copy *<source-url>* *<destination-url>* [ascii | binary]
Function: Download files to the FTP client.
Parameter: ***<source-url>*** is the location of the source files or directories to be copied; ***<destination-url>*** is the destination address to which the files or directories to be copied; forms of ***<source-url>*** and ***<destination-url>*** vary depending on different locations of the files or directories. **ascii** indicates the ASCII standard will be adopted; **binary** indicates that the binary system will be adopted in the file transmission(default transmission method). When URL represents an FTP address, its form should be: ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname> }/<filename>,amongst <username> is the FTP user name, <password> is the FTP user password, <*ipaddress*>|<*ipv6address*> is the IPv4 or IPv6 address of the FTP server/client, <*hostname*> is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses, <*filename*> is the name of the FTP upload/download file.
Special keywords of the filename

Keywords	Source or destination addresses
running-config	Running configuration files
startup-config	It means the reboot configuration files when using copy running-config startup-config command
nos.img	System files
boot.rom	System startup files
stacking/nos.img	As destination address, execute system files upgrade for Slave in stacking mode

stacking/nos.rom	As destination address, execute system startup files upgrade for Slave in stacking mode

Command Mode: Admin Mode.

Usage Guide: This command supports command line hints, namely if the user can enter commands in following forms: copy <filename> ftp:// or copy ftp:// <filename> and press Enter, following hints will be provided by the system:

ftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] >

ftp username>

ftp password>

ftp filename>

Requesting for FTP server address, user name, password and file name

Examples:

(1) Save images in the FLASH to the FTP server of 10.1.1.1, FTP server username is Switch, password is superuser:

Switch#copy nos.img ftp://Switch:superuser@10.1.1.1/nos.img

(2) Obtain system file nos.img from the FTP server 10.1.1.1, the username is Switch, password is superuser

Switch#copy ftp://Switch:superuser@10.1.1.1/nos.img nos.img

(3) Save images in the FLASH to the FTP server of 2004:1:2:3::6

Switch#copy nos.img ftp://username:password@2004:1:2:3::6/ nos.img

(4) Obtain system file nos.img from the FTP server 2004:1:2:3::6

Switch#copy ftp:// username:password@2004:1:2:3::6/nos.img nos.img

(5) Save the running configuration files

Switch#copy running-config startup-config

Relevant Command: write

1.1.5.2 copy（TFTP）

Command: copy *<source-url> <destination-url>* [ascii | binary]

Function: Download files to the TFTP client.

Parameter: ***<source-url>*** is the location of the source files or directories to be copied; ***<destination-url>*** is the destination address to which the files or directories to be copied; forms of ***<source-url>*** and ***<destination-url>*** vary depending on different locations of the files or directories. **ascii** indicates the ASCII standard will be adopted; **binary** indicates that the binary system will be adopted in the file transmission（default transmission method）.When URL represents a TFTP address, its form should be: tftp://{<ipaddress>|<ipv6address>|<hostname>}/<filename>, amongst <ipaddress>| <ipv6address> is the IPv4 or IPv6 address of the TFTP server/client, <hostname> is the name of

the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses,*<filename>* is the name of the TFTP upload/download file.
Special keyword of the filename

Keywords	**Source or destination addresses**
running-config	Running configuration files
startup-config	It means the reboot configuration files when using copy running-config startup-config command
nos.img	System files
boot.rom	System startup files

Command Mode: Admin Mode.
Usage Guide: This command supports command line hints, namely if the user can enter commands in following forms: **copy *<filename>* tftp:**// or **copy tftp:**// ***<filename>*** and press Enter, following hints will be provided by the system:
tftp server ip/ipv6 address[x.x.x.x]/[x:x::x:x]>
tftp filename>
Requesting for TFTP server address, file name
Example:
(1) Save images in the FLASH to the TFTP server of 10.1.1.1
Switch#copy nos.img tftp://10.1.1.1/nos.img

(2) Obtain system file nos.img from the TFTP server 10.1.1.1
Switch#copy tftp://10.1.1.1/nos.img nos.img

(3) Save images in the FLASH to the TFTP server of 2004:1:2:3::6
Switch#copy nos.img tftp:// 2004:1:2:3::6/ nos.img

(4) Obtain system file nos.img from the TFTP server 2004:1:2:3::6
Switch#copy tftp:// 2004:1:2:3::6/nos.img nos.img

(5) Save the running configuration files
Switch#copy running-config startup-config
Relevant Command: write

1.1.5.3 copy（SFTP）

Command: copy *<source-url>* *<destination-url>* [ascii | binary]
Function: Download files to the SFTP client.
Parameter: ***<source-url>*** is the location of the source files or directories to be copied; ***<destination-url>*** is the destination address to which the files or directories to be copied; forms of ***<source-url>*** and ***<destination-url>*** vary depending on different locations of the files or directories. **ascii** indicates the ASCII standard will be adopted; **binary** indicates that the binary

system will be adopted in the file transmission(default transmission method). When URL represents an SFTP address, its form should be: ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname> }/<filename>,amongst <username> is the SFTP user name, <password> is the *S*FTP user password, <*ipaddress*>|<*ipv6address*> is the IPv4 or IPv6 address of the SFTP server/client, <*hostname*> is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses, <*filename*> is the name of the SFTP upload/download file.

Special keywords of the filename

关键字	源地址或目的地址
running-config	运行配置文件
startup-config	在使用 copy running-config startup-config 命令时，代表下次启动的配置文件。
nos.img	系统文件
boot.rom	系统启动文件
stacking/nos.img	作为目的地址在堆叠模式下对 Slave 进行系统文件升级
stacking/nos.rom	作为目的地址在堆叠下对 Slave 进行系统启动文件升级

Command Mode: Admin Mode

Usage Guide: This command supports command line hints, namely if the user can enter commands in following forms: copy <filename> sftp:// or copy sftp:// <filename> and press Enter, following hints will be provided by the system:

sftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] >

sftp username>

sftp password>

sftp filename>

Requesting for SFTP server address, user name, password and file name

Example:

(1) Save images in the FLASH to the SFTP server of 10.1.1.1, SFTP server username is Switch, password is superuser:

Switch#copy nos.img sftp://Switch:superuser@10.1.1.1/nos.img

(2) Obtain system file nos.img from the SFTP server 10.1.1.1, the username is Switch, password is superuser

Switch#copy sftp://Switch:superuser@10.1.1.1/nos.img nos.img

(3) Save images in the FLASH to the SFTP server of 2004:1:2:3::6

Switch#copy nos.img sftp://username:password@2004:1:2:3::6/ nos.img

(4) Obtain system file nos.img from the SFTP server 2004:1:2:3::6

Switch#copy sftp:// username:password@2004:1:2:3::6/nos.img nos.img

(5) Save the running configuration files

Switch#copy running-config startup-config
Relevant Command: write

1.1.5.4 ftp-dir

Command: ftp-dir *<ftp-server-url>*
Function: Browse the file list on the FTP server.
Parameter: The form of **<ftp-server-url>** is： ftp://<username>:<password>@{ <ipv4address> | <ipv6address> }, amongst <username> is *the FTP* user name, <password> is the FTP user password, { <ipv4address> | <*ipv6address*> } is the IPv4 or IPv6 address of the FTP server.
Command Mode: Admin Mode
Example: Browse the list of the files on the server with the FTP client, the username is “Switch”, the password is “superuser”.
Switch#ftp-dir ftp://Switch:superuser @10.1.1.1.

1.1.5.5 ftp-server enable

Command: ftp-server enable
no ftp-server enable
Function: Start FTP server, the “**no ftp-server enable**” command shuts down FTP server and prevents FTP user from logging in.
Default: FTP server is not started by default.
Command mode: Global Mode
Usage Guide: When FTP server function is enabled, the switch can still perform ftp client functions. FTP server is not started by default.
Example: Enable FTP server service.
Switch#config
Switch(config)# ftp-server enable
Relative command: ip ftp

1.1.5.6 ftp-server timeout

Command: ftp-server timeout <*seconds*>
Function: Set data connection idle time.
Parameter: *<seconds>* is the idle time threshold (in seconds) for FTP connection, the valid range is 5 to 3600.
Default: The system default is 600 seconds.
Command mode: Global Mode
Usage Guide: When FTP data connection idle time exceeds this limit, the FTP management connection will be disconnected.
Example: Modify the idle threshold to 100 seconds.
Switch#config
Switch(config)#ftp-server timeout 100

1.1.5.7 ip ftp

Command: ip ftp username <*username*> password [0 | 7] <*password*>

no ip ftp username <*username*>

Function: Configure the username and password for logging in to the FTP; the no operation of this command will delete the configured username and password simultaneously.

Parameters: <*username*> is the username of the FTP link, its range should not exceed 32 characters; **<*password*>** is the password of the FTP link, if input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted.

Default Settings: The system uses anonymous FTP links by default.

Command Mode: Global Configuration Mode.

Examples: Configure the username as Switch and the password as superuser.

Switch#

Switch#config

Switch(config)#ip ftp username Switch password 0 superuser

Switch(config)#

1.1.5.8 show ftp

Command: show ftp

Function: Display the parameter settings for the FTP server.

Command mode: Admin and Configuration Mode.

Default: Do not display.

Example:

Switch#show ftp

Timeout : 600

Displayed information	Description
Timeout	Timeout time.

1.1.5.9 show tftp

Command: show tftp

Function: Display the parameter settings for the TFTP server.

Default: Do not display.

Command mode: Admin and Configuration Mode.

Example:

Switch#show tftp

timeout : 60

Retry Times : 10

Displayed information	Explanation
Timeout	Timeout time.
Retry Times	Retransmission times.

1.1.5.10 tftp-server enable

Command: tftp-server enable

no tftp-server enable

Function: Start TFTP server, the "**no ftp-server enable**" command shuts down TFTP server and prevents TFTP user from logging in.

Default: Disable TFTP Server.

Command mode: Global Mode

Usage Guide: When TFTP server function is enabled, the switch can still perform TFTP client functions. TFTP server is not started by default.

Example: Enable TFTP server service.

Switch#config

Switch(config)#tftp-server enable

Relative Command: tftp-server timeout

1.1.5.11 tftp-server retransmission-number

Command: tftp-server retransmission-number <*number*>

Function: Set the retransmission time for TFTP server.

Parameter: ***<number>*** is the time to re-transfer, the valid range is 1 to 20.

Default: Retransmit 5 times.

Command mode: Global Mode

Example: Modify the retransmission to 10 times.

Switch#config

Switch(config)#tftp-server retransmission-number 10

1.1.5.12 tftp-server transmission-timeout

Command: tftp-server transmission-timeout <*seconds*>

Function: Set the transmission timeout value for TFTP server.

Parameter: ***<seconds>*** is the timeout value, the valid range is 5 to 3600s.

Default: The system default timeout setting is 600 seconds.

Command mode: Global Mode

Example: Modify the timeout value to 60 seconds.

Switch#config

Switch(config)#tftp-server transmission-timeout 60

1.1.6 Boot Configuration

1.1.6.1 baudrate

Command: baudrate *<value>*

Function: This command is used to configure the baud rate of the switch.

Parameters: ***<value>*** is the baud rate, the baud rate the switch supported currently are 9600,14400,19200,38400,57600,115200.

Default: 115200.

Command Mode: Boot Mode.

Usage Guide: This command is used to configure the appropriate baud rate when transmitting the files under the xmodem mode. The baud rate of the switch must be the same as the baud rate of the serial port software in PC.

Example: Configure the baud rate of the switch as 115200 when transmitting the files under the xmodem mode.

[Boot]: baudrate 115200

1.1.6.2 boot img

Command: boot img *<img-file-url>* {primary | backup}

Function: Configure the first and second starting of img files of the switch.

Parameters: primary means to configure the first starting of IMG file, **backup** means to configure the second starting of IMG file, ***<img-file-url>*** is the full path of the booting IMG file.

Command mode: Boot mode.

Default: There is only the first booting IMG file which is nos.img file in the FLASH, the second booting IMG file is free.

Usage Guide: Configure the first and second starting of img files of the switch through this command. If the first booting img file failed, the system will start the second automatically. The format of the img full path is as follows:

1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between those two parts.
2. The suffix of all file names must be .img.
3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.

Example: Configure the first starting of img files of the switch as flash:/nos.img.

[Boot]: boot img flash:/nos.img primary

1.1.6.3 boot startup-config

Command: boot startup-config *<file-url>*

Function: Configure the CFG file used in the next booting of the switch.

Parameters: *<file-url>* is the full path of CFG file used in the next booting.

Command Mode: Boot Mode.

Default: Null as default.

Usage Guide: Configure the CFG file used in the next booting of the switch through this command. The file name must include the suffix of .cfg. The format of the full path is as follows:

1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the

file name. No space is allowed in each part or between those two parts.
2. The suffix of all file names must be .cfg.
3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.
Example: Set flash:/ startup.cfg as the CFG file used in the next booting of the switch.
[Boot]: boot startup-config flash:/ startup-config

1.1.6.4 clearconfig

Command: clearconfig
Function: Recover bootrom parameters to be the default.
Parameters: None.
Command Mode: Boot Mode.
Default Settings: None.
Usage Guide: Recover bootrom parameters to be the default through this command.
Example: Recover bootrom parameters to be the default.
[Boot]: clearconfig
Network interface configure OK.

Boot config set Ok.

1.1.6.5 Copy

Command: copy <srcFileName> <desFileName>
Function: Copy the file in flash.
Parameters: ***<source-file-url>*** is the url of the source file, URLs of the source file can be relative or absolute; ***<dest-file-url>*** is the url of the destination file, URLs of the destination file can only be relative. The suffix name of destination file must be the same as the one of the source file.
Command mode: Boot Mode.
Default: None.
Usage guide: This command can be used to back up IMG files or cfg files.
Example: Copy the img file of .

1.1.6.6 Delete

Command: copy <srcFileName> <desFileName>
Function: Copy the file in flash.
Parameters: ***<source-file-url>*** is the url of the source file, URLs of the source file can be relative or absolute; ***<dest-file-url>*** is the url of the destination file, URLs of the destination file can only be relative. The suffix name of destination file must be the same as the one of the source file.
Command mode: Boot Mode.

Default: None.
Usage guide: This command can be used to back up IMG files or cfg files.
Example: Copy the img file of .

1.1.6.7 dir

Command: dir
Function: Display the files list and property in the current switch.
Default: None.
Command mode: Boot Mode.
Usage guide: Input this command will display the name and size of the file.
Example: View the files list and property in the current switch. Notice: the rom file will not be shown.

```
[[Boot]: dir
   1461094      nos.img.ecc
     91393      mantest.img.ecc
  41559526      nos.img
   2599038      mantest.img
      1547      startup.cfg

5 file(s), 0 dir(s)

Total size:64483328 bytes , used size:45851648 bytes, free size:18631680 bytes
```

1.1.6.8 help

Command: h
help
Function: Show the commands and the function explanation which are supported by the current bootRom.
Default: None
Parameters: None.
Command Mode: Boot Mode.
Usage Guide: View the explanation of the commonly used commands.
Example: Print the explanation of the commonly used commands.

```
[Boot]: help
baudrate                - set the baudrate
boot                    - select the active bootimg image file or startup-config file
clearconfig             - set default bootrom configurations
copy <src> <dst>        - copy a file
delete <filename>       - delete a file
dir                     - display the contents of the current directory
h                       - print help list
```

```
help                    - print help list
load <filename>         - load system image(binary format)
nobootpassword          - no bootpassword for setup
ping <x.x.x.x>          - ping test
reboot                  - reboot system
saveconfig              - save bootrom configurations
setbootpassword         - set boot password
setconfig               - set bootrom configurations
show                    - show machine info
showconfig              - show bootrom configurations
write <filename>        - write file to flash; file gotten by 'load'
xmodem                  - load file by xmodem
```

1.1.6.9 load

Command: load*<filename>*
Function: Download files through the TFTP.
Parameters: ***<filename>*** is the name of file to be downloaded.
Command Mode: Boot Mode.
Usage Guide: Download files through the TFTP by inputting the load + filename command.
Example: Download boot.rom file.
[Boot]:load boot.rom

1.1.6.10 nobootpassword

Command: nobootpassword
Function: Clear the password which is used to enter into the boot.
Parameter: None.
Default: None.
Command mode: Boot Mode.
Usage Guide: Clear password which is used to enter into the boot through this command.
Example: Clear password which is used to enter into the boot.
[Boot]: nobootpassword
clear password ok

1.1.6.11 ping

Command: ping *<x.x.x.x>*
Function: Test the network connection.
Parameters: ***< x.x.x.x >*** is the ip address to ping and it is the ip address of the pc generally.
Command Mode: Boot Mode.
Default: None.
Usage Guide: This command is used to test the network connection. It is like the ping command

of PC, but there is no optional parameters and it can only ping the PC from the switch.
Examples: Test the network connection of 192.168.0.1.
[Boot]:ping 192.168.0.1

1.1.6.12 reboot

Command: reboot
Function: Reboot the switch.
Parameters: None
Default: none
Command mode: Boot Mode
Usage Guide: Reboot the switch in warm mode
Example: Reboot the switch.
[Boot]:reboot

1.1.6.13 saveconfig

Command: saveconfig
Function: Save the configuration of bootrom.
Parameters: None.
Default: None.
Command mode: Boot Mode.
Usage Guide: Save the configuration of bootrom through this command.
Example: Save the configuration of bootrom.
[Boot]: saveconfig
change boot params is OK

1.1.6.14 setbootpassword

Command: setbootpassword
Function: Set the password which is used to enter into the boot.
Parameters: None.
Default: There is no password which is used to enter into the boot as default.
Command mode: Boot Mode.
Usage Guide: Set password which is used to enter into the boot. The length of the password cannot be less than 3 and larger than 32.
Example: Set the password which is used to enter into the boot.
[Boot]: setbootpassword
Password:******
Confirm Password:******

Password has been set successfully!

1.1.6.15 setconfig

Command: setconfig
Function: Set the configuration parameters of bootrom.
Parameters: None.
Default: The Host IP is 10.1.1.1 and the Server IP is 10.1.1.2 as default.
Command mode: Boot Mode.
Usage Guide: Set the configuration parameters of bootrom through this command. The two parameters which are used to configure the Host IP and Server IP only support TFTP protocol currently.
Example: Set the configuration parameters of bootrom.

```
[Boot]: setconfig
Host IP Address: [10.1.1.1] 192.168.1.1
Server IP Address: [10.1.1.2] 192.168.1.2
```

1.1.6.16 show

Command: show [board|config|boot-files|partition]
Function: Show the configuration of the corresponding switch.
Parameters: board is the parameter information of switch, such as type, mac, sn and etc. **config** is the configuration parameter of the current bootrom; **boot-files** is the configuration parameter of first /second img files and cfg files; **partition** is the partition of flash.
Default: None.
Command mode: Boot Mode.
Usage Guide: show board is used to show the parameters information of switch, such as type, mac, sn and etc. **Show config** is used to show the configuration parameter of bootrom; **show boot-files** is used to show the configuration parameter of first /second img files and cfg files; **show partition** is used to show the partition of flash.
Example: Show the configuration of first img files.

```
[Boot]: show boot-files
The primary img file : flash:/1.img
The backup img file : flash:/nos.img
```

1.1.6.17 showconfig

Command: showconfig
Function: Show the configuration parameter of bootrom, this command is the same as **show config** command.
Parameters: None.
Default: None.
Command mode: Boot Mode.
Usage Guide: Show the user configuration of bootrom.
Example: Show the configuration parameter of bootrom.

[Boot]: showconfig
Host IP Address: 192.168.1.1
Server IP Address: 192.168.1.2

1.1.6.18 write

Command: write *<filename>*
Function: Write the file which was downloaded before into the memory such as flash.
Parameters: *<filename>* is the name of the file which will be written into the memory.
Default: None.
Command mode: Boot Mode.
Usage Guide: Write the file which was downloaded before into the flash or bootrom.
Example: Write the boot file in the flash and name it as boot.rom.
[Boot]:write boot.rom

1.1.6.19 xmodem

Command: xmodem
Function: The command is used to transmit the files through the Xmodem protocol under the bootrom.
Parameters: None.
Default: None.
Command mode: Boot Mode.
Usage Guide: In order to improve the transmission rate, the higher baud rate is suggested (baudrate command). After this command was enabled, the switch will enter into the xmodem reception status. In this time, the PC should run the xmodem transmission through the software which supports the xmodem.
Example: Make switch enter into the Xmodem mode.
[Boot]: xmodem
Ready for binary (xmodem) download to 0x04400000 at 9600 bps...

1.2 File System

1.2.1 cd

Command: cd <*directory*>
Function: Change the working directory for the storage device.
Parameters: *<directory>* is the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80.
Command Mode: Admin Mode.

Default Settings: The default working directory is Flash.

Usage Guide: After this command implemented, the current storage device will switch to the new working directory, which can be viewed by the “pwd” command.

Example: Change the working directory of the current storage device to flash.

Switch#cd flash:

Switch#pwd

flash:/

Switch#

1.2.2 copy

Command: copy <*source-file-url* > <*dest-file-url*>

Function: Copy a designated file on the switch and store it as a new file.

Parameters: ***<source-file-url>*** is the source file; ***<dest-file-url>*** is the destination file. When users operate on files stored in backup master board and line cards under IMG mode, URLs of the source file and the destination file should take such a form as described in the following requirements.

1. The prefix of the source file URL should be in one of the following forms:

- starting with “flash:/”
- “ftp://username:pass@server-ip/file-name”
- “tftp://server-ip/file-name”

2. The prefix of the destination file URL should be in one of the following forms:

- starting with “flash:/”
- “ftp://username:pass@server-ip/file-name”
- “tftp://server-ip/file-name”

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide:

1. In this command, when the prefix of the source file URL is ftp:// or tftp://, that of the destination file URL should not be either of them.

2. To use this command, the designated source file should exist, and the destination file should not be named the same as any existing directory or file, otherwise, there might be a prompt warning about a failed copy operation or an attempt to overwrite an existing file.

3. If the source and destination files are in different directories, with this command implemented, users can copy files from other directories into the current one.

URL Example: The URL of files in root directory of Flash devices on it should be flash:/nos.img.

Example: Copy the file “flash:/nos.img” and store it as “flash/ 6.1.11.0.img”.

Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img

Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y:N] y

Copyed file flash:/nos.img to flash:/nos-6.1.11.0.img.

1.2.3 delete

Command: delete <*file-url*>
Function: Delete the designate file on the storage device.
Parameters: ***<file-url>*** is the full path of the file to be deleted.
Command Mode: Admin Mode.
Default Settings: None.
Usage Guide: The designated file will be deleted after implementing this command.
Example: Delete file flash:/nos.img.
Switch#delete flash:/nos5.img
Delete file flash:/nos5.img?[Y:N]y
Deleted file flash:/nos.img.

1.2.4 dir

Command: dir [WORD|all]
Function: Display the information of the designated directory on the storage device.
Parameters: <WORD> is the name of the shown directory. There may be the following formats: directory name, slot-xx#directory name, flash:/directory name, cf:/directory name. The parameter all means to display the information under the directories of flash:/ and mmc:/.
Command Mode: Admin Configuration Mode.
Default Settings: No <WORD> means to display information of the current working directory.
Usage Guide: Implementing this command will display information of files and sub-directories in the designated directory.
Note: This command does not support a recursive display of all sub-directories.
Example: Display information of the directory "flash:/".
Switch#dir flash:/
nos.img 2,449,496 1980-01-01 00:01:06 ----
startup-config 2,064 1980-01-01 00:30:12 ----
Total 7, 932, 928 byte(s) in 4 file(s)， free 4, 966, 400 byte(s)
Switch#

1.2.5 Format

Command: copy <srcFileName> <desFileName>
Function: Copy the file in flash.
Parameters: ***<source-file-url>*** is the url of the source file, URLs of the source file can be relative or absolute; ***<dest-file-url>*** is the url of the destination file, URLs of the destination file can only be relative. The suffix name of destination file must be the same as the one of the source file.
Command mode: Boot Mode.
Default: None.
Usage guide: This command can be used to back up IMG files or cfg files.

Example: Copy the img file of .

1.2.6 mount

This command is not supported by the switch.

1.2.7 pwd

Command: pwd
Function: Display the current working directory.
Parameters: None.
Command Mode: Admin Mode.
Default Settings: The default directory is flash.
Example: Display the current working directory.
Switch#pwd
flash:/
Switch#

1.2.8 rename

Command: rename <*source-file-url*> <*new-filename* >
Function: Rename a designated file on the switch.
Parameters: ***<source-file-url>*** is the source file, in which whether specifying or not its path are both acceptable; ***<new-filename>*** is a filename without specifying its path.
Command Mode: Admin Mode.
Default Settings: None.
Usage Guide: When using this command, if the new file name is not used as that of any existing directory or file, the rename operation can be done, or a prompt will indicate its failure.
Example: Change the name of file “nos.img” in the current working directory to “nos-6.1.11.0.img”.
Switch# rename nos5.img nos-6.1.11.0.img
Rename flash:/nos5.img to flash:/nos-6.1.11.0.img ok！

1.2.9 unmount

This command is not supported by the switch.

1.3 Cluster

1.3.1 clear cluster nodes

Command: clear cluster nodes [nodes-sn <*candidate-sn-list*> | mac-address <*mac-addr*>]

Function: Clear the nodes in the candidate list found by the commander switch.

Parameters: candidate-sn-list: sn of candidate switches, ranging from 1 to 256. More than one candidate can be specified.

mac-address: mac address of the switches (including all candidates, members and other switches).

Default: No parameter means to clear information of all switches.

Command Mode: Admin Mode.

Usage Guide: After executing this command, the information of this node will be deleted from the chain list saved on commander switch. In 30 seconds, the commander will recreate a cluster topology and re-add this node. But after being read, the candidate id of the switch might change. The command can only be executed on commander switches

Example: Clear all candidate switch lists found by the commander switch.

Switch#clear cluster nodes

1.3.2 cluster auto-add

Command: cluster auto-add

no cluster auto-add

Function: When this command is executed in the commander switch, the newly discovered candidate switches will be added to the cluster as a member switch automatically; the "**no cluster auto-add**" command disables this function.

Command mode: Global Mode

Default: This function is disabled by default. That means that the candidate switches are not automatically added to the cluster.

Usage Guide: After enabling this command on a commander switch, candidate switches will be automatically added as members.

Example: Enable the auto adding function in the commander switch.

Switch(config)#cluster auto-add

1.3.3 cluster commander

Command: cluster commander [<*cluster-name*>]

no cluster commander

Function: Set the switch as a commander switch, and create a cluster.

Parameter: ***<cluster-name>*** is the cluster's name, no longer than 32 characters.

Command mode: Global Mode

Default: Default setting is no commander switch. cluster_name is null by default.

Usage Guide: This command sets the role of a switch as commander switch and creates a cluster, which can only be executed on non commander switches. The cluster_name cannot be changed after the switch becoming a commander, and “no cluster commander” should be executed first to do that. The no operation of this command will cancel the commander configuration of the switch.

Example: Set the current switch as the commander switch and name the cluster as switch.

Switch(config)#cluster commander switch

1.3.4 cluster ip-pool

Command: cluster ip-pool *<commander-ip>*

no cluster ip-pool

Function: Configure private IP address pool for member switches of the cluster.

Parameters：*commander-ip*: cluster IP address pool for allocating internal IP addresses of the cluster commander-ip is the head address of the address pool, of which the valid format is 10.x.x.x, in dotted-decimal notation; the address pool should be big enough to hold 128 members, which requires the last byte of addresses to be less than 126（254 – 128 = 126）. IP address pool should never be changed with commander configured. The change can only be done after the “no cluster commander” command being executed.

Command mode: Global Mode

Default: The default address pool is 10.254.254.1.

Usage Guide: When candidate switches becomes cluster members, the commander switch allocates a private IP address to each member for the communication within the cluster, and thus to realized its management and maintenance of cluster members. This command can only be used on non-commander switches. Once the cluster established, users can not modify its IP address pool. The NO command of this command will restore the address pool back to default value, which is 10.254.254.1.

Example: Set the private IP address pool used by cluster member devices as 10.254.254.10

Switch(config)#cluster ip-pool 10.254.254.10

1.3.5 cluster keepalive interval

Command: cluster keepalive interval *<second>*

no cluster keepalive interval

Function: Configure the interval of keepalive messages within the cluster.

Parameters: *<second>:* keepalive interval, in seconds, ranging from 3 to 30.

Default: The default value is 30 seconds.

Command Mode: Global Configuration Mode.

Usage Guide: After executing this command on a commander switch, the value of the parameter will be distributed to all member switches via the TCP connections between the commander and members.

After executing it on a non commander switch, the configuration value will be saved but not used until the switch becomes a commander. Before that, its keepalive interval is the one

distributed by its commander.

Commander will send DP messages within the cluster once in every keepalive interval. Members will respond to the received DP messages with DR messages.

The no operation of this command will restore the keepalive interval in the cluster back to its default value.

Example: Set the keepalive interval in the cluster to 10 seconds.

Switch(config)#cluster keepalive interval 10

1.3.6 cluster keepalive loss-count

Command: cluster keepalive loss-count*<loss-count>*

no cluster keepalive loss-count

Function: Configure the max number of lost keepalive messages in a cluster that can be tolerated.

Parameters: loss-count**:** the tolerable max number of lost messages, ranging from 1 to 10.

Default: The default value is 3.

Command Mode: Global Configuration Mode

Usage Guide: After executing this command on a commander switch, the value of the parameter will be distributed to all member switches via the TCP connections between the commander and members.

After executing it on a non commander switch, the configuration value will be saved but not used until the switch becomes a commander. Before that, its loss-count value is the one distributed by its commander.

commander calculates the loss-count after sending each DP message by adding 1 to the loss-count of each switch and clearing that of a switch after receiving a DR message from the latter. When a loss-count reaches the configured value (3 by default) without receiving any DR message, the commander will delete the switch from its candidate chain list.

If the time that a member fails to receive DP messages from the commander reaches loss-count, it will change its status to candidate.

The no operation of this command will restore the tolerable max number of lost keepalive messages in the cluster back to its default value: 3.

Example: Set the tolerable max number of lost keepalive messages in the cluster to 5.

Switch(config)#cluster keepalive loss-count 5

1.3.7 cluster member

Command: cluster member {nodes-sn *<candidate-sn-list>* | mac-address *<mac-addr>* [id *<member-id>*]}

no cluster member {id *<member-id>* | mac-address *<mac-addr>*}

Function: On a commander switch, manually add candidate switches into the cluster created by it. The no command deletes the specified member switch to change it as candidate.

Parameters: nodes-sn： all cluster member switches as recorded in a chain list, each with a node sn which can be viewed by “show cluster candidates” command. One or more candidates can be

added as member at one time. The valid range of candidate-sn-list is 1~256.

mac-address：the CPU Mac of candidate switches

member-id：A member id can be specified to a candidate as it becomes a member, ranging from 1 to 128, increasing from 1 by default.

nodes-sn is the automatically generated sn, which may change after the candidate becomes a member. Members added this way will be actually treated as those added in mac-addr mode with all config files in mac-addr mode.

If more than one switch is added as member simultaneously, no member-id is allowed; neither when using nodes-sn mode.

Default: None.

Command Mode: Global Mode

Usage Guide: After executing this command, the switch will add those identified in ***<nodes-sn>*** or ***<mac-address>*** into the cluster it belongs to. One or more candidates are allowed at one time, linked with '-' or ';'. A switch can only be member or commander of one cluster, exclusively. Attempts to execute the command on a non commander switch will return error. The no operation of this command will delete the specified member switch, and turn it back to a candidate.

Example: In the commander switch, add the candidate switch which has the sequence number as 1. In the commander switch, add the switch whose the mac address is 11-22-33-44-55-66 to member, and the member-id is 5.

Switch(config)#cluster member nodes-sn 1

Switch(config)#cluster member mac-address 11-22-33-44-55-66 id 5

1.3.8 cluster member auto-to-user

Command: cluster member auto-to-user

Function: All members will be deleted when configuring no cluster auto-add. Users need to change automatically added members to manually added ones to keep them.

Parameter: None.

Default: None.

Command Mode: Global Mode.

Usage Guide: Execute this command on a switch to change automatically added members to manually added ones.

Example: change automatically added members to manually added ones.

Switch(config)#cluster member auto-to-user

1.3.9 cluster reset member id

Command: cluster reset member [id *<member-id>* | *mac-address <mac-addr>*]

Function: In the commander switch, this command can be used to reset the member switch.

Parameter: member-id: ranging from 1 to 128. Use hyphen "-" or semicolon ";" to specify more than one member; if no value is provided, it means to reboot all member switches.

Default: Boot all member switches.

Command mode: Admin Mode.
Instructions: In the commander switch, users can use this command to reset a member switch. If this command is executed in a non-commander switch, an error will be displayed.
Example: In the commander switch, reset the member switch 1.
Switch#cluster reset member id 1

1.3.10 cluster run

Command: cluster run [key *<WORD>*] [vid *<VID>*]
no cluster run
Function: Enable cluster function; the "**no cluster run**" command disables cluster function.
Parameter: key： all keys in one cluster should be the same, no longer than 16 characters.
vid：vlan id of the cluster, whose range is 1-4094.
Command mode: Global Mode
Default: Cluster function is disabled by default, key: NULL(\0) vid：1.
Instructions: This command enables cluster function. Cluster function has to be enabled before implementing any other cluster commands. The "**no cluster run**" disables cluster function. It is recommended that users allocate an exclusive vlan for cluster（such as vlan100）
Note：Routing protocols should be disabled on the layer-3 interface where cluster vlan locates to avoid broadcasting private route of the cluster.
Example: Disable cluster function in the local switch.
Switch (config)#no cluster run

1.3.11 cluster update member

Command: cluster update member *<member-id> <src-url> <dst-filename>* [ascii | binary]
Function: Remotely upgrade member switches from the commander switch.
Parameters: member-id：ranging from 1 to 128. Use hyphen "-" or semicolon "；" to specify more than one member;
src-url：the location of source files to be copied;
dst-filename：the specified filename for saving the file in the switch flash;
ascii means that the file transmission follows ASCII standard; binary means that the file transmission follows binary standard, which is de default mode.
when src-url is a FTP address, its form will be: ftp://<username>:<password>@<ipaddress>/<filename>，in which <username> is the FTP username <password> is the FTP password <ipaddress> is the IP address of the FTP server,<filename> is the name of the file to be downloaded via FTP.
when src-url is a TFTP address, its form will be: tftp://<ipaddress>/<filename>，in which <ipaddress>is the IP address of the TFTP server <filename> is the name of the file to be downloaded via.
Special keywords used in filename:

Keywords	**source or destination address**
startup-config	start the configuration file

nos.img	system file

Command mode: Admin Mode

Usage Guide: The commander distributes the remote upgrade command to members via the TCP connections between them, causing the number to implement the remote upgrade and reboot. Trying to execute this command on a non-commander switch will return errors. If users want to upgrade more than one member, these switches should be the same type to avoid boot failure induced by mismatched IMG files.

Example: Remotely upgrade a member switch from the commander switch, with the member-id being 1, src-ul being ftp:// switch: switch @192.168.1.1/nos.img, and dst-url being nos.img

Switch#cluster update member 1 ftp:// switch: switch @192.168.1.1/nos.img nos.img

1.3.12 debug cluster

Command: debug cluster {statemachine | application | tcp}

no debug cluster {statemachine | application | tcp}

Function: Enable the application debug of cluster; the no operation of this command will disable that.

Parameters: statemachine: print debugging when the switch status changes.

application: print debugging when there are users trying to configure the switch after logging onto it via SNMP, WEB.

tcp: the TCP connection between the commander and the member.

Default: None.

Command Mode: Admin Mode.

Usage Guide: None.

Example: Enable the debug status changed on the switch.

Swtich#debug cluster statemachine

1.3.13 debug cluster packets

Command: debug cluster packets {DP | DR | CP} {receive | send}

no debug cluster packets {DP | DR | CP} {receive | send}

Function: Enable the debug; the no command disables the debug.

Parameters: DP: discovery messages.

DR: responsive messages.

CP: command messages.

receive: receive messages.

send: send messages.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Enable the debug of cluster messages. After enabling classification, all DP, DR and CP messages sent or received in the cluster will be printed.

Example: Enable the debug of receiving DP messages.

Switch#debug cluster packets DP receive

1.3.14 show cluster

Command: show cluster
Function: Display cluster information of the switch.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: None.
Example: Execute this command on different switches.
----in a commander----------
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role: commander
IP pool: 10.254.254.1
Cluster name: MIS_zebra
Keepalive interval: 30
Keepalive loss-count: 3
Auto add: Disabled
Number of Members: 0
Number of Candidates: 3
----in a member ----------
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role: Member
Commander Ip Address: 10.254.254.1
Internal Ip Address: 10.254.254.2
Commamder Mac Address: 00-12-cf-39-1d-90
---- a candidate ----------
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role: Candidate
---- disabled ----------
Switch#show cluster
Status: Disabled

1.3.15 show cluster members

Command: show cluster members [id <*member-id*> | mac-address <*mac-addr*>]
Function: Display member information of a cluster. This command can only apply to commander switches.
Parameters: member-id: member id of the switch.

mac-addr: the CPU mac addresses of member switches.

Default: No parameters means to display information of all member switches.

Command Mode: Admin and Configuration Mode.

Usage Guide: Executing this command on a commander switch will display the configuration information of all cluster member switches.

Example: Execute this command on a commander switch to display the configuration information of all and specified cluster member switches.

Switch#show cluster members

Member From : User config(U); Auto member (A)

ID	From	Status	Mac	Hostname	Description	Internal IP
xxx	x	xxxxxxxxxx12	xx-xx-xx-xx-xx-xx	xxxxxxxxxx12	xxxxxxxxxx12	xxx.xxx.xxx.xxx
1	U	Inactive	00-01-02-03-04-05	MIS_zebra	DCRS-6804	10.254.254.2
2	A	Active	00-01-02-03-04-05	MIS_bison	DCRS-6804	10.254.254.3
3	U	Active	00-01-02-03-04-05	SRD_jaguar	DCRS-9808	10.254.254.4
4	A	Inactive	00-01-02-03-04-05	HRD_puma	DCRS-5950-28T	10.254.254.5

Switch#show cluster members id 1

Cluster Members:

ID: 1

Member status: Inactive member (user_config)

IP Address: 10.254.254.2

MAC Address: 00-01-02-03-04-06

Description: DCRS-9808

Hostname: DSW102

1.3.16 show cluster candidates

Command: show cluster candidates [nodes-sn <*candidate-sn-list*> | mac-address <*mac-addr*>]

Function: Display the statistic information of the candidate member switches on the command switch

Parameter: candidate-sn-list：candidate switch sn, ranging from 1 to 256. More than one switch can be specified.

mac-address： mac address of the candidate switch

Default: No parameters means to display information of all member switches.

Command Mode: Admin and Configuration Mode.

Usage Guide: Executing this command on the switch will display the information of the candidate member switches.

Example: Display configuration information of all cluster candidate switches.

Switch#show cluster candidates

Cluster Candidates:

SN Mac Description Hostname

--- ----------------- ----------------------- -----------------------

xxx xx-xx-xx-xx-xx-xx xxxxxxxxxxxxxxxxxxxxxx24 xxxxxxxxxxxxxxxxxxxxx24

1 00-01-02-03-04-06 ES3528M

2 01-01-02-03-04-05 ES3528M MIS_zebra

1.3.17 show cluster topology

Command: show cluster topology [root-sn *<starting-node-sn>* | nodes-sn *<node-sn-list>* | mac-address *<mac-addr>*]

Function: Display cluster topology information. This command only applies to commander switches.

Parameters: starting-node-sn：the starting node of the topology.

node-sn-list：the switch node sn.

mac-addr：the CPU mac address of the switch.

No parameters means to display all topology information.

Command Mode: Admin and Configuration Mode.

Usage Guide: Executing this command on the commander switch will display the topology information with its starting node specified.

Example: Execute this command on the commander switch to display the topology information under different conditions.

Switch#show cluster topology

Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)

LV SN Description Hostname Role MAC_ADDRESS Upstream Upstream leaf

local-port remote-port node

== ========== ========== == ================ ========== ========== =

x xxx xxxxxxxxxx12 xxxxxxxxxx12 xx xx-xx-xx-xx-xx-xx xxxxxxxxxx12 xxxxxxxxxx12 x

1 1 ES4626H LAB_SWITCH_1 CM 01-02-03-04-05-01 -root- -root- -

2 ES4626H LAB_SWITCH_2 M 01-02-03-04-05-02 eth 1/0/1 eth 1/0/2 N

3 ES4626H LAB_SWITCH_3 CA 01-02-03-04-05-03 eth 1/0/1 eth 1/0/3 Y

4 ES4626H LAB_SWITCH_4 CA 01-02-03-04-05-04 eth 1/0/1 eth 1/0/4 Y

.....

2 2 ES4626H LAB_SWITCH_2 M 01-02-03-04-05-02 eth 1/0/1 eth 1/0/2 -

5 ES3528M LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/0/1 eth 1/0/2 Y

```
    6  ES3528M          LAB_SWITCH_1  OM  01-02-03-04-05-14  eth  1/0/1       eth  1/0/3
Y
-------------------------------------------------------
Switch#show cluster topology root-sn 2
Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)
SN  Description     Hostname          Role       MAC_ADDRESS       Upstream       Upstream
leaf
                                                                  local-port    remote-port node
==    ============ ============ == ================ ============ ============ =
*     2 ES4626H         LAB_SWITCH_2 M    01-02-03-04-05-02 eth 1/0/1       eth 1/0/2          -
    5  ES3528M          LAB_SWITCH_1  OC  01-02-03-04-05-13  eth  1/0/1       eth  1/0/2
Y
    6  ES3528M          LAB_SWITCH_1  OM  01-02-03-04-05-14  eth  1/0/1       eth  1/0/3
Y
----------------------------------------------
Switch#show cluster topology nodes-sn 2
Toplogy role:    Member
Member status: Active member (user-config)
SN:                  2
MAC Address: 01-02-03-04-05-02
Description: ES4626H
Hostname      : LAB_SWITCH_2
Upstream local-port: eth 1/0/1
Upstream node: 01-02-03-04-05-01
Upstream remote-port:eth 1/0/2
Upstream speed: 100full
Switch#
----------------------------------------------
Switch#show cluster topology mac-address 01-02-03-04-05-02
Toplogy role:    Member
Member status: Active member (user-config)
SN:                  2
MAC Address: 01-02-03-04-05-02
Description: ES4626H
Hostname      : LAB_SWITCH_2
Upstream local-port: eth 1/0/1
Upstream node: 01-02-03-04-05-01
Upstream remote-port: eth 1/0/2
Upstream speed: 100full
```

1.3.18 rcommand commander

Command: rcommand commander
Function: In the member switch, use this command to configure the commander switch.
Parameter: None.
Default: None.
Command mode: Admin Mode.
Instructions: This command is used to configure the commander switch remotely. Users have to telnet the commander switch by passing the authentication. The command "**exit**" is used to quit the configuration interface of the commander switch. This command can only be executed on member switches.
Example: In the member switch, enter the configuration interface of the commander switch.
Switch#rcommand commander

1.3.19 rcommand member

Command: rcommand member *<mem-id>*
Function: In the commander switch, this command is used to remotely manage the member switches in the cluster.
Parameter: ***<mem-id>*** commander the member id allocated by commander to each member, whose range is 1～128.
Default: None.
Command mode: Admin Mode.
Usage Guide: After executing this command, users will remotely login to a member switch and enter Admin Mode on the latter. Use exit to quit the configuration interface of the member. Because of the use of internal private IP, telnet authentication will be omitted on member switches. This command can only be executed on commander switches.
Example: In the commander switch, enter the configuration interface of the member switch with member-id 1.
Switch#rcommand member 1

1.4 USB

1.4.1 cd usb:

Command: cd usb:
Function: Enter the USB letter.
Command Mode: Admin Mode.

Default: None.
Usage Guide: When there is the U disk, enter the content of U disk and print “Change the current directory to “usb:/”!”. If there is no U disk, print “Device “usb:” has not inserted！”.
Example:
Switch#cd usb：
Change the current directory to “usb:/”!

1.4.2 dir

Command: dir
Function: Enter the content of U disk, show the information of it.
Command Mode: Admin Mode.
Default: None.
Usage Guide: Enter the content of U disk, print the file content under it. If there is no U disk, print the error information.
Example:
Switch#dir

drwx 4.0K 7.0tset
-rwx 1.2K bootex.log
drwx 4.0K crt
dr-x 4.0K recycler
drwx 8.0K reliability
drwx 4.0K test
-rwx 141.3K 186.pdf
drwx 4.0K new

Drive : usb:
Size:7.4G Used:227.6M Available:7.2G Use:3%

1.4.3 delete

Command: delete <filename>
Function: Delete the file content.
Command Mode: Admin Mode.
Default: None.
Example: Delete the log.txt under the usb letter.
Switch#delete log.txt
Delete file, Are you sure? (Y/N)?[N]y
Delete file ok.

1.4.4 rename

Command: rename <source> <destination>

Function: Rename the file name.

Command Mode: Admin Mode.

Default: None.

Usage Guide: source: source file name; destination: destination file name. if there is no U disk, the validity of the destination file name will be judged first, and then the validity of the source file name will be judged. If the inputting destination file name is null, print the error information.

Example: Rename log1.txt to be log2.txt.

Switch#rename log1.txt log2.txt

Rename log1.txt to log2.txt ok!

1.4.5 copy

Command: copy <source> <destination>

Function: Copy the source file to be the destination file.

Command Mode: Admin Mode.

Default: None.

Usage Guide: 1) Copy the U disk: **copy source.txt destination.txt** will copy the source.txt under the usb letter to be destination.txt;

2) **copy usb:/startup.cfg startup.cfg** can update the startup.cfg under the usb letter to the switch.
Reverse transmission is supported at the same time: **copy startup.cfg usb:/startup.cfg**

3) **copy usb:/boot.rom boot.rom** supports the boot.rom updating under the usb letter.
Reverse transmission is supported at the same time: **copy boot.rom usb:/boot.rom**

4) **copy usb:/nos.img nos.img** supports the nos.img updating under the usb letter.
Reverse transmission is supported at the same time: **copy nos.img usb:/nos.img**

5) The commands above support the unconditional and relative paths.

Example: When there is U disk, enable the copy configuration; if there is no U disk, print the different error information as below:

Switch#copy usb:/tt.txt usb:/tttt.txt

Device "usb:" has not inserted!

Read local file usb:/tt.txt error.

Switch #copy startup.cfg usb:/startup.cfg

Can't write in non-existent directory "usb:/"!

Write config usb:/startup.cfg error!

Write error.

Switch #

Switch #copy usb:/startup.cfg startup.cfg

Confirm to overwrite the existed destination file? [Y/N]:y

Get file "startup.cfg" length error!

Read local file usb:/startup.cfg error.

1.5 Device Management

1.5.1 debug devsm

Function: Display the situation of the device management sending and receiving message and the card status transition, the command no form off DEBUG display.

Parameter: The send displays the outgoing device management message.

receive Display the received equipment management message.

The state displays the board card status transition information of the board card.

Default situation: The default debugging switch is turned off.

Command mode: Privileged user configuration mode.

1.5.2 force runcfg-sync

Command: force runcfg-sync

Function: In the vsf process, force to synchronize the running-config sm.

Command Mode: Admin Mode.

Usage Guide: In stacking mode, the running configuration of AM is periodically synchronized to SM every 5 minutes by default. Executing this command will initiate an immediate synchronization.

1.5.3 force sync software-version

Command: force {sm|} sync software-version {enable|disable}

Function: In the vsf process, force to synchronize the nos version to sm or slave.

Command Mode: Admin Mode.

Usage Guide: In the vsf process, am can check if the new added line card is same with its own version. If they are different, its own img will be synchronized to the new added line card.

1.5.4 force switchover

Command: force switchover

Function: Forcefully switch SM to AM.

Command mode: Admin Mode.

Usage Guide: When a standby master exists, executing this command on the active master will trigger a master-slave switchover, with the original standby master becoming the new active master.

1.5.5 reset slot

Command: reset member <memID> slot <slotno>
Function: Reset one specified card.
Parameters: <memID> In stacking mode, the vsf member ID, range 1~16
Command mode: Admin Mode.
Usage Guide: Can only reset SM or slave card, can not reset AM card.

1.5.6 runcfg-sync

This **command is not *supported* by** the switch.

1.5.7 show fan

Command: show fan
Function: Shows whether the fan tray is in place and its running status, and shows the speed of the fan.
Parameters: None**.**
Default: No **display by default.**
Command mode: Admin Mode.
Usage Guide: This command shows the fan running status. Fan board Inserted means whether the fan tray is in place; fan status indicates whether the fan is running normally and fan speed means the working speed of the fan.
Example:
switch#show fan
Fan board information:

Fan No	Status	Speed
1	Normal	Medium
2	Normal	Medium
3	Normal	Medium
4	Normal	Medium
5	Normal	Medium

1.5.8 show power

Command: show power
Function: Shows if the power supply is in place and its running status.
Parameters: None.
Default: None.
Command mode: Admin Mode.
Usage Guide: power Inserted means whether the power supply is in place; power Status means whether it is running status.
Example:

Switch#show power
System power information:

Power No	Inserted	Status
1	YES	Normal
2	YES	Abnormal

1.5.9 show slot

Command**: show [member <member-id>] slot <slot-id>**

Function: Show basic information of each chip.

Parameter: ***<mem-id>*** is the member device number under the VSF mode, range is 1 to 16; ***<slot-id>*** is the number of the slot the chip resides, all the slots are 1 for the cassette devices.

Default: All chip information will be listed by default if mem-id and slot-id are not specified

Command Mode: Admin Mode.

Usage Guide: This command displays basic information of all boardcards. MCU state is the Micro-control-unit state (master or standby Micro-control-unit); MCU version is the version of the Micro-control-unit file; Uptime is the runtime since the system boots.

Example:

Switch#show member 13 slot 1

----------member :13----------
Inserted : YES
Module type : Switch
Work mode : STANDBY MASTER
Work state : RUNNING
Software package version : 7.0.3.0(R0075.0011)
Bootrom version : 7.2.2
CPLD version : N/A
Hardware version : 1.0.1
Part number : N110900062
Manufacture date : 2011/03/10
Temperature : 39C/102F
Uptime : 0 weeks, 0 days, 1 hours, 37 minutes

1.5.10 show manage-plane context

This command is not supported by switch.

1.5.11 debug cpmp

This command is not supported by switch.

1.5.12 pull out slot

This command is not supported by switch.

Chapter 2 Network Security

2.1 Network Security

2.1.1 default user password macbased

Command：service default user password macbased

no service default user password macbased

Function：The factory default password of the device is calculated by the device VLAN MAC address and generated by a specific combination. The no operation of this command is to restore the factory default password.

Parameter：none

The default situation：none

Command mode：Global configuration mode.

Operating guide：The command line is controlled by the vendor and is added to the default configuration of the vendor when required to enable it by upgrading the img file generated by the new vendor.

Example：none

2.1.2 first-login change password

Command：first-login change password

no first-login change password

Function：To force the default password, and the default operation of this command is not to force the default password.

Parameter：none

The default situation：none

Command mode：Global configuration mode.

Operating guide：The command line is controlled by the vendor and is added to the default configuration of the vendor when required to enable it by upgrading the img file generated by the new vendor.

Example：none

2.1.3 userpassword restriction

Command：userpassword restriction {min-length <1-32> | format-mix (<2-4>|)

| max-consecutive-char <2-32> | max-consecutive-identical-char <2-32>}

no userpassword restriction {min-length <1-32> | format-mix (<2-4>|)

| max-consecutive-char <2-32> | max-consecutive-identical-char <2-32> | }

Function： Configure the password strength check, the no operation of this command is to delete the password strength check.

Parameter：min-length <1-32>： Password minimum length <1-32>;

format-mix (<2-4>|)： The password format is mixed mode, the number of formats is <2-4>, and the default is 2 formats without parameters;

max-consecutive-char <2-32>： Maximum number of adjacent characters allowed by the password, <2-32>;

max-consecutive-identical-char <2-32>： The maximum number of continuous identical characters allowed by a password is <2-32>。

The default situation： none

Command mode： Global configuration mode.

Operating guide： If you need to check the user password strength, then configure the command line.

Example： The minimum length of the configuration password strength is 8, the minimum of three formats, the maximum number of consecutive identical characters is 3, and the maximum number of adjacent characters is 3

Switch#config terminal

Switch(config)#userpassword restriction min-length 8 format-mix 3

max-consecutive-identical-char 3 max-consecutive-char 3

2.1.4 password valid-time

Command：service user password valid-time <0-90>

no service user password valid-time

Function： Configure the user password validity period, the no operation of this command is to cancel the user validity life configuration.

Parameter：<0-90>： Expiry days <0-90>, 0 is permanent.

The default situation： none

Command mode： Global configuration mode.

Operating guide： If you need password expiration control, configure the command line.

Example： Configure the user shelf life for 30 days

Switch#config terminal

Switch(config)#service user password valid-time 30

2.1.5 user-login failed msg

Command：user-login failed msg neutral

no user-login failed msg neutral

Function： When the user login fails, the prompt information does not include the specific reasons of the authentication failure: password error, the user does not exist, etc., only prompts the neutral information of the login failure, and the no operation of this command restores the default prompt information.

Parameter： none

The default situation： Neutral information that prompts for a login failure.

Command mode： Global configuration mode.

Operating guide： The command line is configured if you need a neutral prompt after login failure.

Example： Configure prompt neutral information after user login failure

Switch#config terminal

Switch(config)#user-login failed msg neutral

2.1.6 password feedback

Command：password feedback (none|star)

no password feedback

Function： When the user logs in, the password is not displayed or *, the no operation of this command is to delete the rule.

Parameter：none： The password is not shown back;

star： The password displays the * number.

The default situation： The * number is displayed by default.

Command mode： Global configuration mode.

Operating guide： You can configure the command line if you need to configure the password display rule.

Example： The configuration password is displayed as empty

Switch#config terminal

Switch(config)#password feedback none

2.1.7 password security-config

Command：userpassword security-config

no userpassword security-config

Function： Configure the user password mandatory secure input, the no operation of this command is to cancel the mandatory user password secure input.

Parameter：none

The default situation： none

Command mode： Global configuration mode.

Operating guide： If a user password is required to force secure input, configure the command line.

Example： Configure the user password to force a secure entry

Switch#config terminal

Switch(config)#userpassword security-config

After configuring the command, you need to follow the following operations when entering the password.

Switch(config)#username user privilege 15 password

Password:*******

2.1.8 boot-file security check

Command：boot (img | startup-config) check enable

no boot (img | startup-config) check enable

Function：Configure the img and cfg files for the security verification, and the no operation of this command is to cancel the security verification of the img and cfg files.

Parameter：img：img document;

startup-config：cfg document.

The default situation：none

Command mode：Global configuration mode.

Operating guide：If you need a security check on the img, cfg files, you can configure the command line, which is an environment variable and can be viewed through show boot-files.

Example：Configure the img file for security verification

Switch#config terminal

Switch(config)#boot img check enable

2.1.9 ssh-server dst-port

Command：**ssh-server dst-port *<port-number>***

no ssh-server dst-port

Function：Configure / delete the port number of the SSH server. The no-command restores the default configuration.

Parameter：*<Port-number> is the port number of the set SSH server, range 1025 to 65535.*

Command mode：Global configuration mode.

The default situation：The default port number is 22.

Operating guide：The port number can be modified only when the SSH function is off, and the function off if enabled. After the port number of the SSH server is set, the port number can not be specified only when the connection port number is 22; otherwise, for another port number, the port number must be specified when the SSH client logs in.

Example：Configure the port number 1200 used by the SSH server.

Switch(config)# ssh-server dst-port 1200

2.1.10 telnet-server dst-port

Command：**telnet-server dst-port *<port-number>***

no telnet-server dst-port

Function：Configure / delete the port number of the Telnet server. The no-command restores the default configuration.

Parameter：*<port-number>* is the port number of the set Telnet server, range 1025 to 65535.

Command mode：Global configuration mode.

The default situation：The default port number is 23.

Operating guide：The port number can be modified only when the Telnet function is off, and if the function is turned off. After setting the port number of the Telnet server, the Telnet client can not specify the port number only when the port number is 23; otherwise, if it is another port number, the Telnet client must specify the port number.

Example：Configure the port number 1300 used by the Telnet server.

Switch(config)# telnet-server dst-port 1300

2.1.11 snmp-server dst-port

Command：**snmp-server dst-port <port-number>**

no snmp-server dst-port

Function：Configure / delete the port number used by the snmp service to the network connection. The no-command restores the default configuration.

Parameter：*<Port-number> is the port number for the set snmp service and network connection, range 1025 to 65535.*

Command mode：Global configuration mode.

The default situation：The default port number is 161.

Operating guide：The port number can be modified only when the snmp function is off, and if it is enabled, the function off before configuration. After configured the port number used to connect snmp to the network management device, the port number specified by the network management end must match the port number configured by the snmp-server dst-port command, otherwise the device cannot be connected.

Example: Configure the port number 1400 for the snmp service.

Switch(config)# snmp-server dst-port 1400

2.1.12 ip http secure- ciphersuite

Command：ip http secure-ciphersuite {aes128-gcm-sha256 | aes128-sha | aes128-sha256 | aes256-sha | aes256-sha256 | ecdhe-rsa-aes128-gcm-sha256 | ecdhe-rsa-aes128-sha | ecdhe-rsa-aes256-sha}

no ip http secure-ciphersuite

Function： Configure / delete the encryption suite used by the SSL. The no-command restores the default configuration.

compatibility :Modify command.

Modify Command: ip http secure-ciphersuite { aes128-gcm-sha256 | aes128-sha | aes128-sha256 | aes256-sha | aes256-sha256 | des-cbc3-sha | ecdhe-rsa-aes128-gcm-sha256 | ecdhe-rsa-aes128-sha | ecdhe-rsa-aes256-sha}

Parameter：aes128-gcm-sha256: Encryption algorithm AES128-GCM-SHA256.

aes128-sha: Encryption algorithm AES128-SHA.

aes128-sha256: Encryption algorithm AES128-SHA256.

aes256-sha: Encryption algorithm AES256-SHA.

aes256-sha256: Encryption algorithm AES256-SHA256.

ecdhe-rsa-aes128-gcm-sha256: Encryption algorithm ECDHE-RSA-AES128-GCM-SHA256.

ecdhe-rsa-aes128-sha: Encryption algorithm ECDHE-RSA-AES128-SHA.

ecdhe-rsa-aes256-sha: Encryption algorithm ECDHE-RSA-AES256-SHA.

Command mode： Global configuration mode.

The default situation： The default is not configured.

Operating guide：If the encryption suite is configured using this command, the encryption suite is negotiated using the configured encryption suite. Modification of the encryption suite requires a restart of the SSL function each time.

Example： Configure the encryption suite aes128-gcm-sha256 used by the SSL.

Switch(config)# ip http secure- ciphersuite aes128-gcm-sha256

2.1.13 ssh-server encryption-algorithm

Command：ssh-server encryption-algorithm (add | remove)｛aes128-cbc | 3des-cbc | aes128-ctr | aes256-ctr | aes256-cbc | 3des-ctr | all｝

no ssh-server encryption-algorithm

Function： Configure / remove the encryption algorithms on the SSH server side. The no-command restores the default configuration.

compatibility :Modify command.

Modify Command: ssh-server encryption-algorithm (add) ｛aes128-cbc | 3des-cbc | aes128-ctr | aes256-ctr | aes256-cbc | 3des-ctr | all｝

Parameter：add | remove: Add to or remove the algorithm.

aes128-cbc: Encryption algorithm AES128-CBC.

3des-cbc: Encryption algorithm 3DES-CBC.

aes128-ctr: Encryption algorithm AES128-CTR.

aes256-ctr: Encryption algorithm AES256-CTR.

aes256-cbc: Encryption algorithm AES256-CBC.

3des-ctr: Encryption algorithm 3DES-CTR.

all: Represents all of the encryption algorithms.

Command mode： Global configuration mode.

The default situation：Three algorithms are turned on by default：aes128-ctr，aes256-ctr，3des-ctr。

Operating guide： The encryption algorithm of the SSH server must include the algorithm of the SSH client, otherwise the negotiation failure will lead to the connection failure.

Example： Configure the SSH server-side to use all of the encryption algorithms.

Switch(config)# ssh-server encryption-algorithm add all

2.1.14 service password-encryption type user

Command： service password-encryption type user algo (md5|sha256|aes (salt|)|sm4 (salt|))

no service password-encryption type user

Function： Configuration password using sm4 / AES algorithm encryption output in the configuration file, to ensure the security of the device, with salt value configuration, to ensure the diversity of passwords.

Parameter： md5: The md 5 encryption algorithm

sha256: sha256 Encryption algorithm

sm4: sm4 national secret encryption algorithm

aes: aes encryption algorithm

salt: Salt value, using the salt value of the double encryption.

Command mode： Global configuration mode.

The default situation： The default is not enabled

Operating guide： You must configure service password-encryption before you can configure the current command to be effective.

Example： The configuration uses the password in the sm4 encryption configuration and carries salt values.

Switch(config)# service password-encryption type user algo sm4 salt

2.1.15 bfd authentication key md5

Command：*bfd authentication key <1-255> md5 (0 WORD |7 WORD|WORD|)*

no bfd authentication key *<1-255>*

compatibility :Modify command.

Modify Command： bfd authentication key <1-255> md5 <WORD>

no bfd authentication key <1-255>

Function： Configure BFD, using the key and md 5 mode encryption authentication string. The no command is to delete the configured key.

Parameter：<1-255> Key number, <WORD> Authenticated key string, with 1-16 bytes long. When setting the password, if the input option is 0, enter the clear text password; if the input option is 7, enter the encrypted string; enter the security mode.

The default situation: There default no key and authentication strings configured.

Command mode： Global configuration mode.

Operating guide： Configure the md 5 mode and authentication key string used by the BFD authentication. After you configure this command, the BFD will use the optional fields in the message for authentication, and the BFD will establish neighbors only when the key configuration at both ends of the BFD is consistent.

Example： MD5 encryption with key number 1 and the authentication string 123456.

s5(config)#in vlan 50

s5(config)#bfd authentication key 1 md5 123456

2.1.16 enable password

Command：enable password (level <1-15> |) (0 LINE|7 WORD|LINE|)

no enable password [level *<1-15>*]

compatibility :Modify command.

Modify Command：enable password [level <1-15>] [0 | 7] <password>
no enable password [level <1-15>]
Function：Modify the password for going from the normal user configuration mode to the privileged user configuration mode.
Parameter：**level <1-15> Use to specify the permission level, with the default to level 15.<WORD> <LINE> is the password set by the user. When setting the password, if the input option is 0, enter the clear text password without encryption the clear text password; if the input option is 7, enter the clear text password; enter the security mode.**
Command mode：Global configuration mode.
The default situation：The system default privileged user password is empty.
Operating guide：Configuring privileged user passwords can prevent illegal intrusion of non-privileged users. It is recommended that network administrators set the privileged user password when the switch is first configured. In addition, when the administrator needs to leave the terminal screen for a long time, it is best to execute the exit command to exit the privileged user configuration mode.

2.1.17 enable trustview key

Command：**enable trustview key (0 WORD|7 WORD|)**
no enable trustview key
compatibility :Modify command.
Modify Command：enable trustview key {0|7} <password>
no enable trustview key
Function：Configure the DES encryption key for private messages. This command is also a switch to enable the private message encryption / hashing function.
Parameter：*<WORD> is a string less than 16, used as the DES encryption key.0 means the key is displayed in plaintext, 7 means the key is displayed in ciphertext, and the car directly enters the safe mode to enter the password.*
Command mode：Global configuration mode.
The default situation：The switch does not have the DES encryption key configured by default, meaning that the switch does not enable the private message encryption / hashing function by default.
Operating guide：Switch and network security management background system through private message for private information transmission, by default, private message is passed in plain text, in order to prevent private message is hacked, can choose to encrypt the content of the private message, at the same time, the administrator also need to in the network security management background configuration of the same key.
Example：Encryption / hashing function to enable private messages.
Switch(config)#enable trustview key 0 test

2.1.18 ip ftp

Command：*ip ftp username <username>password (0 LINE|7 WORD|LINE|)*
no ip ftp username <*username*>
compatibility :Modify command.
Modify Command： ip ftp username <username> password [0 | 7] <password>
no ip ftp username <username>
Function：Configure the FTP login user name and login password; the no operation of this command is to delete the configured user name and also delete the password.
Parameter：***<username>*** The username of FTP connection, the value range does not exceed 32 characters; ***<LINE> <WORD>*** is the password used in FTP connection; when setting the password, enter the clear text password without encryption the clear text password; if the input option is 7, enter the clear text password; and enter the password in security mode.
The default situation：The system default is an anonymous FTP connection.
Command mode：Global configuration mode.
Example：Configure user name Switch and password superuser.
Switch#
Switch#config
Switch(config)#ip ftp username Switch password 0 superuser
Switch(config)#

2.1.19 ntp authentication-key

Command： ntp authentication-key <key-id> md5 (0 WORD | 7 WORD |)
no ntp authentication-key <*key-id*>
compatibility :Modify command.
Modify Command： ntp authentication-key <key-id> md5 <value>
no ntp authentication-key <key-id>
Function：Start / cancel the NTP authentication function and define the authentication key for the NTP authentication.
Parameter：***key-id***：Key number, range of 1-4294967295. WORD: Key value, 1-16 ascii code characters. Direct return of the car into the security mode to enter the password.
The default situation：An authentication key is not configured for NTP authentication.
Command mode：Global configuration mode.
Operating guide：none
Example：The validation key defining NTP authentication, with key-id 20 and md 5 abc.
Switch(config)#ntp authentication-key 20 md5 abc

2.1.20 password

Command： password (0 LINE|7 WORD|LINE|)
no password

compatibility :Modify command.
Modify Command： password [0 | 7] <password>
no password
Function：Set the password when the user enters the general user configuration mode on the console, which removes the configured password in the no form.
Parameter：***<LINE> <WORD>*** is the password set by the user. When setting the password, if the input option is 0, enter the plaintext password and do not encrypt the plaintext password; if the input option is 7, enter the plaintext password encrypted string; directly enter the security mode to enter the password.
Command mode：Global configuration mode.
The default situation：The system password is empty by default.
Operating guide：If the password is configured and the login is set, after the command, the password can enter the general user configuration mode.
Example：
Switch(config)#password 0 test
Switch(config)#login

2.1.21 radius-server accounting host

Command：radius-server accounting host {{vrf <vrf-name>| }<ipv4-address> | <ipv6-address>} ((port <port
number>|) (key (0 WORD|7 WORD| WORD)|) (primary|)|)
no radius-server accounting host {<*ipv4-address*> | <*ipv6-address*>}
compatibility :Modify command.
Modify Command： radius-server accounting host {<ipv4-address> | <ipv6-address>} [port <portnumber>] [key {0 | 7} <string>] [primary]
no radius-server accounting host {<ipv4-address> | <ipv6-address>}
Function： Set the RADIUS billing server IPv4 or IPv6 address and listening port number, whether to use the primary server; the no operation of this command is to delete the RADIUS billing server.
Parameter：**<vrf-name> is the specific VRF name ;{<*ipv4-address*> | <*ipv6-address*>}** is the IPv4, address, or IPv6 address of the server. ***<port-number>*** Is the listening port number of the server, taking the value range from 0 to 65535. ***<WORD>*** Is the key string. If the key type option is 0, then specify the clear text key and the value range will not exceed 64 characters; If the option is 7, the secret text string will not exceed 64 characters; enter the password in safe mode. **[primary]** Whether to set the primary server, when configure radius server, you can configure multiple, if you do not configure primary, find the radius server that can be used in the configuration order. If the configured primary, this radius server is used first.
Command mode：Global configuration mode.
The default situation：The system does not set up the RADIUS billing server.
Operating guide：This command is used to specify the IPv4, address or IPv6 address and port number of the RADIUS server charged with the switch. The parameter <port-number> is used to

specify the billing port number, which must be the same as the billing port number on the specified RADIUS server. The default is 1813. If the port number is configured as 0, the port is generated randomly, which may be invalid. This command can repeatedly configure multiple RADIUS servers to specify a communication relationship with the switch, which will send billing messages to all configured billing servers, which can act as backup servers to each other. If you configure primary, use this RADIUS server as the primary server. Only one RADIUS master server can be configured, whether it uses an IPv4 or an IPv6 address.

Example：Set RADIUS, the IPv6 address of the billing server is 2004:1:2:3:: 2, the port number is 3000, and make the primary server.

Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary

2.1.22 radius-server authentication host

Command：**radius-server authentication host {*<ipv4-address>* | *<ipv6-address>*} (port <0-65535>|)(primary|escape-server|) (access-mode (telnet|dot1x)|)(key (0 WORD |7 WORD| WORD|)|)**

no radius-server authentication host {*<ipv4-address>* | *<ipv6-address>*}

compatibility :Modify command.

Modify Command： radius-server authentication host {<ipv4-address> | <ipv6-address>} [port <port-number>][key {0 | 7} <string>] [primary] [access-mode {dot1x | telnet}]

no radius-server authentication host {<ipv4-address> | <ipv6-address>}

Function： Set the RADIUS authentication server IPv4, address or IPv6 address and listening port number, encryption key, whether the primary server, and usage mode; the no operation of this command is to delete the RADIUS server.

Parameter：**{*<ipv4-address>* | *<ipv6-address>*}** is the IPv4, address, or IPv6 address of the server. ***<port-number>*** is the listening port number of the server, and the value range is: 0 to 65535. ***<WORD>*** is the key string. If the key type option is 0, subsequently specify a plaintext key with a value range of no more than 64 characters; if the option is 7, the secret text key encrypted string is not more than 64 characters; enter the password. **[primary]**Whether to set the primary server, when configure radius server, you can configure multiple, if you do not configure primary, find the radius server that can be used in the configuration order. If the primary is configured, the radius server last configured is used first.**[access-mode {dot1x | telnet}]** Indicates that the current RADIUS server is only for 802.1x authentication or telnet remote authentication, and the default current RADIUS server is available for all services.

Command mode：Global configuration mode.

The default situation：The system does not set up the RADIUS authentication server.

Operating guide：This command is used to specify the IPv4, address or IPv6 address and port number, and the key string and access mode of the RADIUS server that authenticates with the switch. The parameter <port-number> is used to specify the authentication port number, which must be the same as the authentication port number on the specified RADIUS server. The default is 1812. If the port number is configured as port 0, it may be invalid. This command can repeatedly configure multiple RADIUS servers to specify multiple connections with the switch, in which order, when the first server responds (whether the authentication is successful or failed),

the switch does not send the authentication request to the next server. If you configure primary, use this RADIUS server as the primary server. If the current RADIUS server is not configured with key <string>, use the key configured globally with the command radius-server key <string>. Alternatively, you can specify that the current RADIUS server is only for 802.1x authentication or telnet remote authentication. The access-mode option is not configured by default, and the RADIUS server is available for all remote authentication services.

Example：Configure RADIUS, the IPv6 address of the authentication server is 2004:1:2:3:: 2.

Switch(config)#radius-server authentication host 2004:1:2:3::2

2.1.23 radius-server key

Command：radius-server key (0 WORD|7 WORD|)

no radius-server key

compatibility :Modify command.

Modify Command：radius-server key {0 | 7} <string>

no radius-server key

Function： Set up the key for the RADIUS server (including authentication and billing); the no operation of this command is to delete the key of the RADIUS server.

Parameter：***<WORD>*** is the key string for the RADIUS server. If the key type option is 0, then specify the clear text key and the value range will not exceed 64 characters; If the option is 7, the secret text string will not exceed 64 characters; enter the password in safe mode.

Command mode： Global configuration mode.

Operating guide： The key is used for the encrypted packet communication between the switch and the set RADIUS server. The key for this setting must be the same as on the RADIUS server for the switch set, otherwise correct RADIUS authentication and billing cannot be performed.

Example： Configure the RADIUS authentication key as a test.

Switch(config)#radius-server key 0 test

2.1.24 tacacs-server authentication host

Command：tacacs-server authentication host {{vrf <vrf-name>| } <ip-address>} [port <port-number>][timeout <seconds>][key (0 WORD|7 WORD|WORD|)][primary]

no tacacs-server authentication host <ip-address>

compatibility :Modify command.

Modify Command：tacacs-server authentication host <ip-address> [port <port-number>] [timeout <seconds>] [key {0 | 7} <string>] [primary]

no tacacs-server authentication host <ip-address>

Function： Set the TACACS + server IP address, listening port number, authentication server timeout time, key string; the no operation of this command is to delete the TACACS + authentication server.

Parameter：<vrf-name> is the specific VRF name；<ip-address> The IP address of the server; ***<port-number>*** is the listening port number of the server, The values ranged from 0 to 65535, Where 0 means that it is not used as an authentication server; ***<seconds>*** For the TACACS + authentication timeout timer value, In the units of seconds, Range from 1 to 60; ***<WORD>*** is key string, If the key type option is 0, Then specify the text key, Taking a value range of not more than 64 characters, If the option is a 7, Then the secret text string designated as text key encryption, Direct return to the car into the safe mode to enter the password; The corresponding plaintext length of the dense text string shall not exceed 64 characters; primary The master server.

Command mode：Global configuration mode.

The default situation：The system does not set up the TACACS + authentication server.

Operating guide： This command is used to specify the IP address, port number, authentication server timeout time, and the key string of the TACACS + server that authenticates with the switch. Where the parameter port is used to specify the authentication port number, This port number must be the same as the authentication port number on the specified TACACS + server, The default level is 49, Parameters, key and timeout, Set up separate keys and timeout for the server itself, If these two parameters are not configured, By default, you use the tacacs-server key <string>, tacacs-server timeout <seconds> Global configuration command; This command can repeatedly configure multiple TACACS + servers to specify multiple servers that establish relationships with the switch, Where the order of the switch authentication server is the order of configuration. If you configure primary, use this TACACS + server as the primary server.

Example：Configure the TACACS + authentication server address to 192.168.1.2 and uses the globally configured key.

Switch(config)#tacacs-server authentication host 192.168.1.2

2.1.25 tacacs-server key

Command：tacacs-server key (0 WORD|7 WORD|)

no tacacs-server key

compatibility :Modify command.

Modify Command： tacacs-server key {0 | 7} <string>

no tacacs-server key

Function： Set the key of the TACACS + authentication server; the no operation of this command is to delete the key of the TACACS + server.

Parameter：***<WORD>*** is the key string of the TACACS + server. If the key type option is 0, then specify the clear text key and the value range is less than 64 characters. If the option is 7, then specify the secret text string with clear text key encryption, enter the password, and the corresponding clear text length is not more than 64 characters.

Command mode： Global configuration mode.

Operating guide： The key is used for the encrypted packet communication between the switch and the TACACS + server. The key for this setting must be the same as that on the TACACS +

server, without correct TACACS + authentication. To ensure the security of TACACS + authentication data, it is recommended to configure the authentication server key.

Example： Configure the TACACS + server authentication key as a test.

Switch(config)# tacacs-server key 0 test

2.1.26 username

Command：username *<username>* [privilege *<privilege>*] [password (0 LINE|7 WORD|LINE|)]

no username *<username>*

compatibility :Modify command.

Modify Command： username <username> [privilege <privilege>] [password [0 | 7] <password>]

no username <username>

Function：Set set users and their priorities that log in with user name and password authentication.

Parameter：*<username>* is the username, the value range does not exceed 32 characters; ***<privilege>*** is the maximum level of the command executable by the user, 1-15, the default level is 1; ***<LINE> <WORD>*** is the user password; if the password, the input option is 0; if the input option 7, enter the plaintext string (MD5, encrypted 32-bit password); enter security mode.

Command mode：Global configuration mode.

Operating guide：Currently the commands registered in the system have two priorities 1 and 15. The command with a priority of 1 is registered in the general user configuration mode. The command with a priority of 15 is registered in a mode other than the general user configuration mode. This command allows a maximum of 16 local authentication users with a maximum password length of 32.Note: The user uses the command to configure the login user and priority to execute authentication line console login local, Command (local user verification enabling Console login mode), you must ensure that there is a user with a priority of 15 to be able to log in and enter privilege mode and global configuration mode to modify the configuration of the system. When the configured local user does not have a permission to reach 15, and the Console login verification mode is only configured with the Local mode, the Console can directly log into the switch without verification. When accessing the switch in HTTP mode, you must log on to the switch with a user with a command level of 15, and a user with a priority below 15 will be rejected.

Example：Configure an administrator user admin with a priority of 15, configure two ordinary users with a priority of 1, and enable local user name and password login authentication. Only user admin can log in to privilege mode through Telnet or Console, and user1 and user2 can only log in to general user configuration mode through Telnet or Console. HTTP login, only admin can log in successfully, user1 and user2 login rights.

Switch(config)#username admin privilege 15 password 0 admin

Switch(config)#username user1 privilege 1 password 7

4a7d1ed414474e4033ac29ccb8653d9b(This password is 0000 using MD5, encrypted 32-bit dark text password)

Switch(config)#username user2 password 0 user2

Switch(config)#authentication line console login local

Chapter 3 Commands for Layer 2 services

3.1 Port Configuration

3.1.1 Bandwidth

Command: bandwidth control <bandwidth> {transmit | receive | both}

no bandwidth control

Function: Enable the bandwidth limit function on the port; the no command disables this function.

Parameter: <bandwidth> is the bandwidth limit, which is shown in kbps ranging between 1-1000000K; both refers to the bandwidth limit when the port receives and sends data, receive refers to the bandwidth **limit** will only performed when the switch receives data from out side, while **transmit** refers to the function will be perform on sending only.

Command Mode: Port Mode.

Default: Bandwidth limit disabled by default.

Usage Guide: When the bandwidth limit is enabled with a size set, the max bandwidth of the port is determined by this **size other** than by 10/100/1000M. If **[**both | receive | transmit] keyword is not specified, the default is **both**.

Note: The bandwidth limit can not exceed the physic maximum speed on the port. For example, an 10/100M Ethernet port can not be set to a bandwidth limit at 101000K (or higher), but applicable on a 10/100/1000 port working at a speed of 100M. If the actual bandwidth is not a integral multiple of chip bandwidth granularity, it will be modified automatically. For example, a chip bandwidth granularity is 64K, but the input bandwidth is 50, the bandwidth will be modified as 64K.

Example: *Set the* bandwidth limit of 1/0/1-8 port is 40000K.

Switch(config)#interface ethernet 1/0/1-8

Switch(Config-If-Port-Range)#bandwidth control 40000 both

3.1.2 clear counters interface

Command: clear counters [interface {ethernet *<interface-list>* | vlan *<vlan-id>* | port-channel *<port-channel-number>* | *<interface-name>*}]

Function: Clears the statistics of the specified port.

Parameters: *<interface-list>* stands for the Ethernet port number; ***<vlan-id>*** stands for the VLAN interface number; ***<port-channel-number>*** for trunk interface number; ***<interface-name>*** for interface name, such as port-channel 1.

Command mode: Admin Mode.

Default: Port statistics are not cleared by default.
Usage Guide: If no port is specified, then statistics of all ports will be cleared.
Example: Clearing the statistics for Ethernet port1/0/1.
Switch#clear counters interface ethernet 1/0/1

3.1.3 description

Command: description *<string>*
no description
Function: Set name for specified port; the no command cancels this configuration.
Parameter: ***<string>*** is a character string, which should not exceeds 200 characters.
Command Mode: Port Mode.
Default: No port name by default.
Usage Guide: This command is for helping the user manage switches, such as the user assign names according to the port application, e.g. financial as the name of 1/0/1-2 ports which is used by financial department, engineering as the name of 1/0/9 ports which belongs to the engineering department, while the name of 1/0/12 ports is assigned with Server, which is because they connected to the server. In this way the port distribution state will be brought to the table.
Example: Specify the description of 1/0/1-2 port as financial.
Switch(config)#interface ethernet 1/0/1-2
Switch(Config-If-Port-Range)#description financial

3.1.4 flow control

Command: flow control
no flow control
Function: Enables the flow control function for the port: the "**no flow control"** command disables the flow control function for the port.
Command mode: Port Mode.
Default: Port flow control is disabled by default.
Usage Guide: After the flow control function is enabled, the port will notify the sending device to slow down the sending speed to prevent packet loss when traffic received exceeds the capacity of port cache. Ports support IEEE802.3X flow control; the ports work in half-duplex mode, supporting back-pressure flow control. If flow control results in serious HOL, the switch will automatically start HOL control (discarding some packets in the COS queue that may result in HOL) to prevent drastic degradation of network performance.
Note: Port flow control function is not recommended unless the users need a slow speed, low performance network with low packet loss. Flow control will not work between different cards in the switch. When enable the port flow control function, speed and duplex mode of both ends should be the same.
Example: Enabling the flow control function in ports 1/0/1-8.

Switch(config)#interface ethernet 1/0/1-8
Switch(Config-If-Port-Range)#flow control

3.1.5 hardware profile module fanout

This command **is not supported by the switch.**

3.1.6 interface ethernet

Command: interface ethernet *<interface-list>*
Function: Enters Ethernet Port Mode from Global Mode.
Parameters: *<interface-list>* stands for port number.
Command mode: Global Mode
Usage Guide: Run the **exit** command to exit the Ethernet Port Mode to Global Mode.
Example: Entering the Ethernet Port Mode for ports1/0/1，1/0/4-5，1/0/8。
Switch(config)#interface ethernet 1/0/1;1/0/4-5;1/0/8
Switch(Config-If-Port-Range)#

3.1.7 interface mode

Command: interface mode sgmii
Function: Configure the interface mode of the 1000M fiber port.
Parameters: **sgmii:** sgmii mode.
Command Mode: Port Mode.
Usage Guide: sgmii mode can only be configured under the 1000M fiber port, which allows the port to automatically negotiate 10m/100m/1000m speed and duplex when using the SFP-GE-T optical power module with internal phy ability. The no command restores the port to the default mode (that is, 1000Base-X).
Example: Configure the interface mode to sgmii:
Switch (config-if-ethernet1/0/22)#interface mode sgmii

3.1.8 loopback

Command: loopback
no loopback
Function: Enables the loopback test function in an Ethernet port; the no command disables the loopback test on an Ethernet port.
Command mode: Port Mode.
Default: Loopback test is disabled in Ethernet port by default.
Usage Guide: Loopback test can be used to verify the Ethernet ports are working normally. After loopback has been enabled, the port will assume a connection established to itself, and all traffic sent from the port will be received at the very same port.

Example: Enabling loopback test in Ethernet ports 1/0/1-8.
Switch(config)#interface ethernet 1/0/1-8
Switch(Config-If-Port-Range)#loopback

3.1.9 media-type

This command is not supported by the switch.

3.1.10 negotiation

Command: negotiation {on | off}
Function: Enables/Disables the auto-negotiation function of a 1000Base-FX port.
Parameters: on: enables the auto-negotiation; off: disable the auto-negotiation.
Command mode: Port configuration Mode.
Default: Auto-negotiation is enabled by default.
Usage Guide: This command applies to 1000Base-FX interface only. The negotiation command is not available for 1000Base-TX or 100Base-TX interface. For combo port, this command applies to the 1000Base-FX port only but has no effect on the 1000Base-TX port. To change the negotiation mode, speed and duplex mode of 1000Base-TX port, use speed-duplex command instead.
Example: Port 1 of Switch1 is connected to port 1 of Switch2, the following will disable the negotiation for both ports.
Switch1(config)#interface ethernet1/0/1
Switch1(Config-If-Ethernet1/0/1)#negotiation off
Switch2(config)#interface ethernet1/0/1
Switch2(Config-If-Ethernet1/0/1)#negotiation off

3.1.11 port-rate-statistics interval

Command: port-rate-statistics interval <interval-value>
Function: Set the interval of port-rate-statistics, ranging from 5 to 600.
Parameter: interval-value: The interval of port-rate-statistics, unit is second, ranging from 5 to 600 with the configuration step of 5.
Default: Only port-rate-statistics of 5 seconds and 5 minutes are displayed.
Command Mode: Global Mode
Usage Guide: None.
Example: Count the interval of port-rate-statistics as 20 seconds.
Switch(config)#port-rate-statistics interval 20

3.1.12 port-scan-mode

Command: port-scan-mode {interrupt | poll}

no port-scan-mode

Function: Configure the scan mode of the port as 'interrupt' or 'poll', the no command restores the default scan mode.

Parameter: interrupt: the interrupt mode; poll: the poll mode.

Command Mode: Global Mode.

Default: Poll mode.

Usage Guide: There are two modes that can respond up/down event of the port. The interrupt mode means that interrupt hardware to announce the up/down change, the poll mode means that software poll can obtain the port event, the first mode is rapid. If using poll mode, the convergence time of MRPP is several hundred **milliseconds, if using interrupt mode, the convergence time is less than 50 milliseconds.**

Notice: The scan mode of the port usually configured as poll mode, the interrupt mode is only used to the environment of the good performance, but the security of the poll mode is better.

Example: Configure the scan mode of the port as interrupt mode.

Switch(config)#port-scan-mode interrupt

3.1.13 port-status query interval

This command is not supported by the switch.

3.1.14 rate-violation

Command: rate-violation <200-2000000> [recovery <0-86400>]

no rate-violation

Function: Set the max packet reception rate of a port. If the rate of the received packet violates the packet reception rate, shut down this port and configure the recovery time, the default is 300s. The no command will disable the rate-violation function of a port.

The rate-violation means the port received all packets rate (the number of the received packets per second), do not distinguish the packet type.

Parameters: <200-2000000> the max packet reception rate of a port, the unit is packets/s.

<0-86400>: The interval of recovery after shutdown, the unit is s.

recovery: After a period of time the port can recover shutdown to up again. <0-86400> is the timeout of recovery. For example, if the shutdown of a port happens after the packet reception rate exceeding the limit, the port will be up again when the user-defined timeout expires. The default timeout is 300s, while 0 means the recovery will never happen.

Command Mode: Interface Mode

Default: There is no control operation for rate-violation.

Usage Guide: This command is mainly used to detect the abnormal port flow. For example, when there are a large number of broadcast messages caused by a loopback, which affect the processing of other tasks, the port will be shut down to ensure the normal processing of the switch.

Example: Set the rate-violation of port 1/0/8-10 (GB ports) of the switch as 10000pps and the port recovery time as 1200 seconds.

Switch(config)#interface ethernet 1/0/8-10
Switch(Config-Port-Range)#rate-violation 10000 recovery 1200

3.1.15 rate-violation control

This command is not supported by the **switch.**

3.1.16 remote-statistics interval

This command is not supported by the switch.

3.1.17 show interface

Command: show interface [ethernet <interface-number> | port-channel <port-channel-number> | loopback <*loopback-id*> | *vlan* <vlan-id> | tunnel <tunnel-id> | <*interface-name*>] [detail]
show interface ethernet status
show interface ethernet counter {packet | rate}

Function: Show information of layer 3 or layer 2 port on the switch

Parameter: ***<vlan-id>*** is the VLAN interface number, the value range from 1 to 4094. ***<tunnel-number>*** is the tunnel number, the value range **from** 1 to 50. <loopback-id> is the loop back number**, the value range from** 1 to 1024. <interface-number> is the port number of the Ethernet***, status*** show important information of all the layer 2 ***ports.*** counter {packet | rate} show package number or **rate statistics** of all layer 2 ports. <port-channel-number**>** is the number of the aggregation interface, ***<interface-name>*** is the name of the interface such as port-channel1. **[detail]** show the detail of the port.

Command Mode: Admin and Configuration Mode.

Default: Information not displayed by default

Usage Guide: While for vlan interfaces, the port MAC address, IP address and the statistic state of the data packet will be shown; for tunnel port, this command will show tunnel interface state and the statistic state of control layer receives/sends tunnel data packet, about the statistic data of physics interface receiving/sending data packet, please refer to show interface ethernet command; for loopback port, this command will show the interface statistic state of IP address and receiving/sending data packet; As for Ethernet port, this command will show port speed rate, duplex mode, flow control switch state, broadcast storm suppression of the port and the statistic state of the data packets; for aggregated port, port speed rate, duplex mode, flow control switch state, broadcast storm suppression of the port and the statistic state of the data packets will be displayed. The information of all ports on the switch will be shown if no port is specified.

Using [detail] to show the detail information for ethernet port and port-channel port, the information is related with the type of switch, board card.

For ethernet port, using status to show important information of all the layer 2 ports by list format. each port is a row, the showing information include port number, Link, Protocl status,

Speed, Duplex, Vlan, port type and port name; counter packets show package number statistics of all ethernet ports, include layer 2 unicast, broadcast, multicast, error of input and output redirection package number; counter rate show the rate statistics of all ethernet ports, input and output package number, byte number in 5 minutes and 5 seconds.

statistic field name	**description**
input errors	total statistic of CRC 、undersize、fragments、jabber field
CRC	the total number of packets received that had a length of between 64 and 1518 octets, inclusive, but had either FCS Error or Alignment Error
frame alignment	total number of packets received that had a bad FCS with a non-integral number of octets (Alignment Error)
undersize	total number of packets received that were less than 64 octets
jabber	total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
fragments	total number of packets received that were less than 64 octets in length and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
pause frame（input）	number of 802.3x Flow Control frames received
output errors	total statistic of collisions and late collisions
collisions	The best estimate of the total number of collisions on this Ethernet segment
late collisions	The number of times that a collision is detected on a particular interface later than one slotTime into the transmission of a packet
pauseframe (output)	number of 802.3x Flow Control frames send

Example: Show the information of VLAN 1

Switch#show interface vlan 1

Vlan1 is up, line protocol is up, dev index is 2005

Device flag 0x1003(UP BROADCAST MULTICAST)

IPv4 address is:

192.168.10.1 255.255.255.0 (Primary)

Hardware is EtherSVI, address is 00-00-00-00-00-01

MTU is 1500 bytes , BW is 0 Kbit
Encapsulation ARPA, loopback not set
5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
The last 5 second input rate 0 bytes/sec, 0 packets/sec
The last 5 second output rate 0 bytes/sec, 0 packets/sec
Input packets statistics:
Input queue 0/600, 0 drops
0 packets input, 0 bytes, 0 no buffer
0 input errors, 0 CRC, 0 frame alignment, 0 overrun
0 ignored, 0 abort, 0 length error
Output packets statistics:
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 late collisions
Show the information of loopback 1:
Switch#show interface loopback 1
Loopback1 is up, line protocol is up, dev index is 2006
  Device flag 0x100b(UP BROADCAST LOOP MULTICAST)
  IPv4 address is:
    1.1.1.1 255.255.255.255 (Primary)
  MTU is 1500 bytes , BW is 0 Kbit
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  The last 5 second input rate 0 bytes/sec, 0 packets/sec
  The last 5 second output rate 0 bytes/sec, 0 packets/sec
  Input packets statistics:
    Input queue 0/600, 0 drops
    0 packets input, 0 bytes, 0 no buffer
    0 input errors, 0 CRC, 0 frame alignment, 0 overrun
    0 ignored, 0 abort, 0 length error
  Output packets statistics:
    0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 late collisions
Show the information of tunnel 1
Switch#show interface tunnel 1
Tunnel1 is up, line protocol is up, dev index is 2007
  Device flag 0x91(UP P2P NOARP)
  IPv4 address is:
    (NULL)
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  The last 5 second input rate 0 bytes/sec, 0 packets/sec
  The last 5 second output rate 0 bytes/sec, 0 packets/sec

Input packets statistics:
Input queue 0/600, 0 drops
0 packets input, 0 bytes, 0 no buffer
0 input errors, 0 CRC, 0 frame alignment, 0 overrun
0 ignored, 0 abort, 0 length error
Output packets statistics:
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 late collisions

Show the information of port 1/0/1.

```
Switch#show interface e1/0/1
Ethernet1/0/1 is up, line protocol is down
Ethernet1/0/1 is layer 2 port, alias name is (null), index is 1
Hardware is Gigabit-TX, address is 00-03-0f-02-fc-01
PVID is 1
MTU 1500 bytes, BW 10000 Kbit
Encapsulation ARPA, Loopback not set
Auto-duplex: Negotiation half-duplex,    Auto-speed: Negotiation 10M bits
FlowControl is off, MDI type is auto
  5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
The last 5 second input rate 0 bytes/sec, 0 packets/sec
The last 5 second output rate 0 bytes/sec, 0 packets/sec
  Input packets statistics:
0 input packets, 0 bytes, 0 no buffer
0 unicast packets, 0 multicast packets, 0 broadcast packets
0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored
0 abort, 0 length error, 0 pause frame
  Output packets statistics:
0 output packets, 0 bytes, 0 underruns
0 unicast packets, 0 multicast packets, 0 broadcast packets
0 output errors, 0 collisions, 0 late collisions, 0 pause frame
```

Show the important information of all layer 2 ports:

```
Switch#show interface ethernet status
Codes: A-Down - administratively down, a - auto, f - force, G - Gigabit

Interface    Link/Protocol        Speed        Duplex    Vlan   Type        Alias Name
1/0/1        UP/UP            f-100M     f-full      1         G-TX
1/0/2            UP/UP              a-100M     a-full     trunk    G-TX
1/0/3            UP/DOWN          auto        auto       1         G-TX
1/0/4            A-Down/DOWN    auto   auto       1         G-TX
…
```

Show the package number statistics information of all layer 2 ports:

Switch#Show interface ethernet counter packet

Interface		Unicast(pkts)	BroadCast(pkts)	MultiCast(pkts)	Err(pkts)
1/0/1	IN	12,345,678	12,345,678,9	12,345,678,9	4,567
	OUT	23,456,789	34,567,890	5,678	0
1/0/2	IN	0	0	0	0
	OUT	0	0	0	0
1/0/3	IN	0	0	0	0
	OUT	0	0	0	0
1/0/4	IN	0	0	0	0
	OUT	0	0	0	0

…

Show the rate statistics information of all layer 2 ports:

Switch#Show interface ethernet counter rate

Interface		IN(pkts/s)	IN(bytes/s)	OUT(pkts/s)	OUT(bytes/s)
1/0/1	5m	13,473	12,345,678	12,345	1,234,567
	5s	135	65,800	245	92,600
1/0/2	5m	0	0	0	0
	5s	0	0	0	0
1/0/3	5m	0	0	0	0
	5s	0	0	0	0
1/0/4	5m	0	0	0	0
	5s	0	0	0	0

3.1.18 shutdown

Command: shutdown

no shutdown

Function: Shuts down the specified Ethernet port; the no command opens the port.

Command mode: Port Mode.

Default: Ethernet port is open by default.

Usage Guide: When Ethernet port is shut down, no data frames are sent in the port, and the port status displayed when the user types the "**show interface**" command is "down".

Example: Opening ports 1/0/1-8.

Switch(config)#interface ethernet1/0/1-8

Switch(Config-If-Port-Range)#no shutdown

3.1.19 speed-duplex

Command: speed-duplex {auto [10 [100 [1000]] [auto | full | half |]] | force10-half | force10-full | force100-half | force100-full | force100-fx [module-type {auto-detected |

no-phy-integrated | phy-integrated}] | {{force1g-half | force1g-full} [nonegotiate [master | slave]]}| force10g-full}

no speed-duplex

Function: Sets the speed and duplex mode for 1000Base-TX, 100Base-TX or 100Base-FX ports; the no command restores the default speed and duplex mode setting, i.e., auto speed negotiation and duplex.

Parameters: auto is the auto speed and duplex negotiation, 10 is 10Mbps speed, 100 is 100Mbps speed, 1000 is 1000Mbps speed, auto is duplex negotiation, full is full-duplex, half is half-duplex; **force10-half** is the forced 10Mbps at half-duplex mode; **force10-full** is the forced 10Mbps at full-duplex mode; **force100-half** is the forced 100Mbps at half-duplex mode; **force100-full** is the forced 100Mbps at full-duplex mode; **force100-fx** is the forced 100Mbps at full-duplex mode; **module-type** is the type of 100Base-FX module; **auto-detected:** automatic detection; **no-phy-integrated:** there is no phy-integratd 100Base-FX module; **phy-integrated:** phy-integratd 100Base-FX module; **force1g-half** is the forced 1000Mbps speed at half-duplex mode; **force1g-full** is the forced 1000Mbps speed at full-duplex mode; **nonegotiate** disables auto-negotiation forcibly for 1000Mb port; **master** forces the 1000Mb port to be **master** mode; **slave** forces the 1000Mb port to be **slave** mode. **force10g-full** is the forced 10000Mbps speed at full-duplex mode.

Command mode**:** Port Mode.

Default: Auto-negotiation for speed **and** duplex mode is set **by** default.

Usage **Guide**: This command is **configures** the port speed and duplex mode. When configuring port speed **and** duplex mode, the speed and duplex mode **must** be the same as the setting of the remote end, i.e., if the remote device is set to auto-negotiation, then auto-negotiation should be set at the local port. If **the** remote end is in forced mode, the **same** should be set **in** the local end. **1000Gb** ports are **by** default **master** when configuring **nonegotiate** mode. If one end is set to master **mode**, the other end must be set to slave **mode**.

force1g-half is not supported yet.

Example: Port 1 of Switch1 is **connected** to port 1 of Switch2, the following will set both ports **in** forced 100Mbps at half-duplex mode.

Switch1(config)**#interface** ethernet1/0/1

Switch1(Config-If-Ethernet1/0/1)#speed-duplex force100-half

Switch2(config)#interface ethernet1/0/1

Switch2(Config-If-Ethernet1/0/1)#speed-duplex force100-half

3.1.20 storm-control

Command: storm-control {unicast | broadcast | multicast} <*packets*>

no storm-control {unicast | broadcast | multicast}

Function: Sets the traffic limit for broadcasts, multicasts and unknownnnnn destination unicasts on all ports in the switch; the no command disables this traffic throttle function on all ports in the switch, i.e., enables broadcasts, multicasts and unknownnnnn destination unicasts to pass through the switch at line speed.

Parameters: use **unicast** to limit unicast traffic for unknownnnnn destination; **multicast** to limit multicast traffic; **broadcast** to limit broadcast traffic. ***<packets>*** is the limit of packet number, ranging from 1 to 1488905. For non-10GB ports, the unit of <packets> is PPS, that is, the value of <packets**>** is the number of packets allowed to pass per second; for 10GB ports, the unit is KPPS, that is, the value of <packets> multiplies 1000 makes the number of packets allowed, so the value should be less than 14880.

Command mode: Port Mode.

Default: No limit is set by default. So, broadcasts, multicasts and unknownnnnn destination unicasts are allowed to pass at line speed.

Usage Guide: All ports in the switch belong to a same broadcast domain if no VLAN has been set. The switch will send the above mentioned three traffics to all ports in the broadcast domain, which may result in broadcast storm and so may greatly degrade the switch performance. Enabling Broadcast Storm Control can better protect the switch from broadcast storm. Note the difference of this command in 10Gb ports and other ports. If the allowed traffic is set to 3, this means allow 3,120 packets per second and discard the rest for 10Gb ports. However, the same setting for non-10Gb ports means to allow 3 broadcast packets per second and discard the rest.

Example: Setting ports 1/0/8-10 (1000Mbps) allow 3 broadcast packets per second.

Switch(config)#interface ethernet 1/0/8-10

Switch(Config-Port-Range)#storm-control broadcast 3

3.1.21 virtual-cable-test

Command: virtual-cable-test interface (ethernet |)IFNAME

Function: Test the link of the twisted pair cable connected to the Ethernet port. The response may include: well, short, open, fail. If the test information is not well, the location of the error will be displayed (how many meters it is away from the port).

Parameter: <*interface-list*>: Port ID

Command Mode: Admin Mode.

Default Settings: No link test.

Usage Guide: The RJ-45 port connected with the twisted pair under test should be in accordance with the wiring sequence rules of IEEE802.3, or the wire pairs in the test result may not be the actual ones. On a 100M port, only two pairs are used: (1, 2) and (3, 6), whose results are the only effective ones. If a 1000M port is connected to a 100M port, the results of (4, 5) and (7, 8) will be of no meaning. The result may have deviations according to the type of the twisted pair, the temperature, working voltage and other conditions. When the temperature is 20 degree Celsius, and the voltage is stable without interference, and the length of the twisted pair is not longer than 100 meters, a deviation of +/-2 meters is allowed. When the port is at Link UP status, a deviation of +/-10 meters is allowed. Notice: the test procedure will block all data flow on the line for 5-10 seconds, and then restore the original status.

Notice: combo port supports VCT function detection only at copper cable port mode, 100M port does not diagnose the link length at Link UP status.

568A wiring sequence: (1 green white, 2 green), (3 orange white, 6 orange), (4 blue, 5 blue white),

(7 brown white, 8 brown).
568B wiring sequence: (1 orange white, 2 orange), (3 green white, 6 green), (4 blue, 5 blue white), (7 brown white, 8 brown).
Example: Test the link status of the twisted pair connected to the 1000M port 1/0/25.
Switch#virtual-cable-test interface ethernet 1/0/25
Interface Ethernet1/0/25:

Cable pairs	Cable status	Error length (meters)
(1, 2)	open	5
(3, 6)	open	5
(4, 5)	open	5
(7, 8)	short	5

3.1.22 switchport discard packet

Command：switchport discard packet { tag | untag }
no switchport discard packet { tag | untag }
Function：Configure the port not to receive the packet of tag or untag; the no command cancel the restriction of discard, it means the port is allowed to receive the packet of tag or untag.
Parameters：all means it does not receive the packet of tag. untag means it does not receive untag.
Command Mode：Port Mode
Default：The default does not have the restriction.
Usage Guide：None.
Example：Configure the port of1/0/8 not to receive the packet of tag.
Switch(config)#interface ethernet 1/0/8
Switch(config-if-ethernet1/0/8)#switchport discard packet tag

3.1.23 switchport flood-control

Command: switchport flood-control { bcast|mcast|ucast }
no switchport flood-control { bcast|mcast|ucast }
Function: Configure that switch does not transmit broadcast, unknownnnnn multicast or unknownnnnn unicast packets any more to the specified port; no command restores the default configuration.
Parameter: bcast: prevents that broadcast packets cannot be transmitted to the specified port; mcast: prevents that unknownnnnn multicast packets cannot be transmitted to the specified port; ucast: prevents that unknownnnnn unicast packets cannot be transmitted to the specified port.
Command Mode: Port configuration mode.

Default: Switch transmits broadcast, unknownnnnn multicast and unknownnnnn unicast packets to other port in broadcast domain.

Usage Guide: This command takes effect for 100M and 1000M ports; it is also takes effect for Access, Trunk and Hybrid ports. When this command is valid, the port will allow unicast or multicast flow to pass after port learned the corresponding unicast mac or multicast mac.

This command only control that broadcast, multicast and unknownnnnn unicast packets sent by other ports cannot be transmitted to the specified port, but it cannot control these packets from the specified port. Switchport flood-control mcast is generally used in combination with ip igmp snooping. For example, set switchport flood-control bcast command in port 1/0/1, broadcast packets cannot be transmitted from other ports to port 1/0/1, but port 1/0/1 can receive and transmit broadcast packets.

Example: Configure flood-control of bcast and mcast for port 1/0/1 or port 1/0/8-10 respectively.

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#switchport flood-control bcast

Switch(config)#interface ethernet 1/0/8-10

Switch(config-if-port-range)#switchport flood-control mcast

3.1.24 switchport flood-forwarding

Command: switchport flood-forwarding mcast

no switchport flood-forwarding mcast

Function: Configure that switch transmit unknownnnnn multicast or unknownnnnn unicast packets to the specified port; no command restores the default configuration.

Parameters: mcast: prevents that unknownnnnn multicast packets can be transmitted to the specified port.

Command Mode: Port Mode.

Default: Switch transmits unknownnnnn multicast packets to other port in broadcast domain.

Usage Guide: This command takes effect for 100M and 1000M ports; it is also takes effect for Access, Trunk and Hybrid ports. The command is usually combined with ip imgp snooping, ip imgp snooping does not supports unknownnnnn multicast and broadcast, it can transfer unknownnnnn multicast flow after configure switchport flood-forwarding mcast.

Example: Set switch 1/0/1 port broadcast flood-forwarding.

switch#

switch#confi

switch(config)#interface ethernet 1/0/1

switch(config-if-ethernet1/0/1)# switchport flood-forwarding mcast

switch(config-if-ethernet1/0/1)#exit

switch(config)#

3.2 Port Isolation

3.2.1 isolate-port group

Command: isolate-port group <*WORD*>

no isolate-port group <*WORD*>

Function: Set a port isolation group, which is the scope of isolating ports; the no operation of this command will delete a port isolation group and remove all ports out of it.

Parameters: <*WORD*> is the name identification of the group, no longer than 32 characters.

Command Mode: Global Mode.

Default: None.

Usage Guide: Users can create different port isolation groups based on their requirements. For example, if a user wants to isolate all downlink ports in a vlan of a switch, he can implement that by creating a port isolation group and adding all downlink ports of the vlan into it. No more than 30 port isolation groups can a switch have. When the users need to change or redo the configuration of the port isolation group, he can delete the existing group with the no operation of this command.

Example: Create a port isolation group and name it as ”test”.

Switch>enable

Switch#config

Switch(config)#isolate-port group test

3.2.2 isolate-port group switchport interface

Command: isolate-port group <*WORD*> switchport interface [ethernet | port-channel] <*IFNAME*>

no *isolate-port* group <*WORD*> switchport interface [ethernet | *port-channel*] <*IFNAME*>

Function: Add one *port* or a group of ports *into* a *port* isolation group to isolate, which will become isolated from the other ports in the group. The no operation of this command will remove one port or a group of ports out of a port isolation group, which will be able to communicate will ports in that group normally. If the ports removed from the group still belong to another port isolation group, they will remain isolated from the ports in that group. If an Ethernet port is a member of a convergence group, it should not be added into a port isolation group, and vice versa, a member of a port isolation group should not be added into an aggregation group. But one port can be a member of one or more port isolation groups.

Parameters: <***WORD>*** is the name identification of the group, no longer than 32 characters. If there is no such group with the specified name, create one; **ethernet** means that the ports to be isolated is Ethernet ones, followed by a list of Ethernet ports, supporting symbols like '' and '-'. For example: 'ethernet 1/0/1;3;4-7;8'; port-channel means that the ports to be isolated is aggregation ports; ***<IFNAME>*** is the name of the interface, such as e1/0/1. If users use interface name, the parameter of ethernet will not be required.

Command Mode: Global *Mode*.

Default: None.

Usage **Guide: Users *can* add** Ethernet ports into or remove them from a port isolation group according to their requirements. When an Ethernet port is a member of more than one port isolate group, it will be isolated from every port of all groups it belongs to.

Example: Add Ethernet ports 1/0/1-2 and 1/0/5 into a port isolation group named as 'test'.

Switch(config)#isolate-port group test switchport interface ethernet 1/0/1-2; 1/0/5

3.2.3 isolate-port apply

Command: isolate-port apply [<l2|l3|all>]

Function: This command will apply the port isolation configuration to isolate layer-2 flows, layer-3 flows or all flows.

Parameters: <l2|l3|all> the flow to be isolated, l2 means isolating layer-2 flows, l3 means isolating layer-3 flows, all means isolating all flows.

Command Mode: Global Mode.

Default: Isolate all flows.

Usage Guide: User can apply the port isolation configuration to isolate layer-2 flows, layer-3 flows or all flows according to their requirements.

Example: Only apply port isolation to layer-2 flows on the switch.

Switch(config)#isolate-port apply l2

3.2.4 show isolate-port group

Command: show isolate-port group [<*WORD*>]

Function: Display the configuration of port isolation, including all configured port isolation groups and Ethernet ports in each group.

Parameters: <*WORD*> the name identification of the group, no longer than 32 characters; no parameter means to display the configuration of all port isolation groups.

Command Mode: Admin Mode and Global Mode.

Default: Display the configuration of all port isolation groups.

Usage Guide: Users can view the configuration of port isolation with this command.

Example: Display the port isolation configuration of the port isolation group named as “test”.

Switch(config)#show isolate-port group test

Isolate-port group test

The isolate-port Ethernet1/0/5

The isolate-port Ethernet1/0/2

3.3 Port Loopback Detection

3.3.1 debug loopback-detection

Command: debug loopback-detection

Function: After enabling the loopback detection debug on a port, BEBUG information will be generated when sending, receiving messages and changing states.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled by default.

Usage Guide: Display the message sending, receiving and state changes with this command.

Example:

Switch#debug loopback-detection

%Jan 01 00:07:45:106 2006 Send loopback detection probe packet:dev Ethernet1/0/5, vlan id 1

%Jan 01 00:07:45:107 2006 Send loopback detection probe packet:dev Ethernet1/0/5, vlan id 1

%Jan 01 00:07:45:110 2006 Loopback detected on port Ethernet1/0/5, VLAN 1

3.3.2 loopback-detection control

Command: loopback-detection control {shutdown |block| learning}

no loopback-detection control

Function: Enable the function of loopback detection control on a port, the no operation of this command will disable the function.

Parameters: shutdown set the control method as shutdown, which means to close down the port if a port loopback is found.

block set the control method as block, which means to block a port by allowing bpdu and loopback detection messages only if a port loopback is found.

learning disable the control method of learning MAC addresses on the port, not forwarding traffic and delete the MAC address of the port.

Default: Disable the function of loopback diction control.

Command Mode: Port Mode.

Usage Guide: If there is any loopback, the port will not recovery the state of be controlled after enabling control operation on the port. If the overtime is configured, the ports will recovery normal state when the overtime is time-out. If the control method is block, the corresponding relationship between instance and vlan id should be set manually by users, it should be noticed when be used.

Example: Enable the function of loopback detection control under port1/0/2 mode.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#loopback-detection control shutdown

Switch(Config-If-Ethernet1/0/2)#no loopback-detection control

3.3.3 loopback-detection control-recovery timeout

Command: loopback-detection control-recovery timeout <0-3600>

Function: This command is used to recovery to uncontrolled state after a special time when a loopback being detected by the port entry be controlled state.

Parameters: <0-3600> second is recovery time for be controlled state, 0 is not recovery state.

Default: The recovery is not automatic by default.

Command Mode: Global Configuration Mode.

Usage Guide: When a port detects a loopback and works in control mode, the ports always work in control mode and not recover. The port will not sent packet to detection in shutdown mode, however, the port will sent loopback-detection packet to detection whether have loopback in block or learning mode. If the recovery time is configured, the ports will recovery normal state when the overtime is time-out. The recovery time is a useful time for shutdown control mode, because the port can keep on detection loopback in the other modes, so suggest not to use this command.

Examples: Enable automatic recovery of the loopback-detection control mode after 30s.

Switch(config)#loopback-detection control-recovery timeout 30

3.3.4 loopback-detection interval-time

Command: loopback-detection interval-time *<loopback> <no-loopback>*

no loopback-detection interval-time

Function: Set the loopback detection interval. The no operate closes the loopback detection interval function.

Parameters: *<loopback >* the detection interval if any loopback is found, ranging from 5 to 300, in seconds.

<no-loopback > the detection interval if no loopback is found, ranging from 1 to 30, in seconds.

Default: The default value is 5s with loopbacks existing and 3s otherwise.

Command Mode: Global Mode.

Usage Guide: When there is no loopback detection, the detection interval can be relatively shorter, for too short a time would be a disaster for the whole network if there is any loopback. So, a relatively longer interval is recommended when loopbacks exist.

Example: Set the loopback diction interval as 35, 15.

Switch(config)#loopback-detection interval-time 35 15

3.3.5 loopback-detection trap enable

Command: loopback-detection trap enable

no loopback-detection trap enable

Function: Enable the function of loopback detection send trap packet to SNMP server; the no operation of this command will disable the function.

Parameters: None

Default: Disable by default.
Command Mode: Global Mode.
Usage Guide: After enabling the loop detection and TRAP message sending function, send SNMP TRAP messages when a loop is detected under the port**.**
Example: Enable the function of loopback detection send trap packet.
Switch(config)# loopback-detection trap enable

3.3.6 loopback-detection specified-vlan

Command: loopback-detection specified-vlan *<vlan-list>*
no loopback-detection specified-vlan [*<vlan-list>*]
Function: Enable the function of loopback detection on the port and specify the VLAN to be checked; the no operation of this command will disable the function of detecting loopbacks through this port or the specified VLAN.
Parameters: *<vlan-list>* the list of VLANs allowed passing through the port. Given the situation of a trunk port, the specified VLANs can be checked. So this command is used to set the vlan list to be checked.
Default: Disable the function of detecting the loopbacks through the port.
Command Mode: Port Mode.
Usage Guide: If a port can be a TRUNK port of multiple Vlans, the detection of loopbacks can be implemented on the basis of port+Vlan, which means the objects of the detection can be the specified Vlans on a port. If the port is an ACCESS port, only one Vlan on the port is allowed to be checked despite the fact that multiple Vlans can be configured. This function is not supported under Port-channel.
Example: Enable the function of loopback detection under port 1/0/2 mode.
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#switchport mode trunk
Switch(Config-If-Ethernet1/0/2)#switchport trunk allowed vlan all
Switch(Config-If-Ethernet1/0/2)#loopback-detection specified-vlan 1;3;5-20
Switch(Config-If-Ethernet1/0/2)#no loopback-detection specified-vlan 1;3;5-20

3.3.7 loopback-detection send packet number

Command: loopback-detection send packet number *<1-10>*
no loopback-detection send packet number
Function: Configure the number of packets sent by the port in each detection cycle; The 'no' operation of this command is to restore the default value.
Parameters: *<1-10>* packets
Default: Default 1 packet。
Command Mode: Port Mode.
Usage Guide: After enabling loopback detection, the number of packets sent by the port in each detection cycle is 1. If a loop is generated, the bandwidth of the port may be occupied due to broadcast storms or other factors, resulting in the loss of loop detection

packet. In this case, the number of detection packets can be adjusted to avoid the inability to detect loops on the port in a timely manner due to packet loss.

Example:

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# loopback-detection send packet number 2

3.3.8 show loopback-detection

Command: show loopback-detection [interface *<interface-list>*]

Function: Display the state of loopback detection on all ports if no parameter is provided, or the state and result of the specified ports according to the parameters.

Parameters: *<interface-list>* the list of ports to be displayed, for example: ethernet 1/0/1.

Command Mode: Admin and Configuration Mode.

Usage Guide: Display the state and result of loopback detection on ports with this command.

Example: Display the state of loopback detection on port 4.

Switch(config)#show loopback-detection interface Ethernet 1/0/4

loopback detection config and state information in the switch!

PortName	Loopback Detection	Control Mode	Is Controlled
Ethernet1/0/4	Enable	Shutdown	No

3.4 ULDP

3.4.1 debug uldp

Command: debug uldp (hello | probe | echo | unidir | all) [receive | send] interface [ethernet] IFNAME

no debug uldp (hello | probe | echo | unidir | all) [receive | send] interface [ethernet] IFNAME

Function: Enable the debugging for receiving and sending the specified packets or all ULDP packets on port. After enable the debugging, show the information of the received and sent packets in terminal. The no command disables the debugging.

Parameters: hello: packet's type is hello, it's announcement packet, including common announcement packet, RSY and Flush packet

probe: packet's type is probe, it's detection packet

echo: packet's type is echo, it means response of detection packet

unidir: packet's type is unidir, it's announcement packet that discover the single link

all: All ULDP packets

Command mode: Admin mode

Default: Disable.
Usage Guide: With this command, user can check probe packets received by port 1/0/2.
Switch#debug uldp probe receive interface ethernet 1/0/2

3.4.2 debug uldp error

Command: debug uldp error
no debug uldp error
Function: Enable the error message debug function, the no form command disable the function.
Parameter: None.
Command Mode: Admin Mode.
Default: Disabled.
Usage Guide: Use this command to display the error message.
Example: Display the error message.
Switch#debug uldp error

3.4.3 debug uldp event

Command: debug uldp event
no debug uldp event
Function: Enable the message debug function to display the event; the no form command disables this function.
Parameter: None.
Command Mode: Admin Mode.
Default: Disabled.
Usage Guide: Use this command to display all kinds of event information.
Example: Display event information.
Switch#debug uldp event

3.4.4 debug uldp fsm interface ethernet

Command: debug uldp fsm interface ethernet <*IFname*>
no debug uldp fsm interface ethernet <*IFname*>
Function: To enable debugging information for ULDP for the specified interface. The no form of this command will disable the debugging information.
Parameters: <*IFname*> is the interface name.
Command Mode: Admin Configuration Mode.
Default: Disabled by default.
Usage Guide: This command can be used to display the information about state transitions of the specified interfaces.
Example: Print the information about state transitions of interface ethernet 1/0/1.
Switch#debug uldp fsm interface ethernet 1/0/1

3.4.5 debug uldp interface ethernet

Command: debug uldp {hello|probe|echo|unidir|all} [receive|send] interface ethernet <*IFname*>

no debug uldp {hello|probe|echo|unidir|all} [receive|send] interface ethernet <*IFname*>

Function: Enable the debug function of display the packet details. After that, display some kinds of the packet details of terminal interface.

Parameter: <*IFname*>: Name of the interface.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use this command to display the Hello packet details receiving on the interface Ethernet 1/0/1.

Switch#debug uldp hello receive interface Ethernet 1/0/1

3.4.6 debug uldp packet

Command: debug uldp packet [receive|send]

no debug uldp packet [receive|send]

Function: Enable receives and sends packet debug function, after that. Display the type and interface of the packet which receiving and sending on the client. The no form command disables this function.

Parameter: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use this command to display the packet that receiving on each interface.

Switch#debug uldp packet receive

3.4.7 uldp aggressive-mode

Command: uldp aggressive-mode

no uldp aggressive-mode

Function: To configure ULDP to work in aggressive mode. The no form of this command will restore the normal mode.

Parameters: None.

Command Mode: Global Configuration Mode and Port Configuration Mode.

Default: Normal mode.

Usage Guide: The ULDP working mode can be configured only if it is enabled globally. When ULDP aggressive mode is enabled globally, all the existing fiber ports will work in aggressive mode. For the copper ports and fiber ports which are available after the configuration is available, aggressive mode should be enabled in port configuration mode.

Example: To enable ULDP aggressive mode globally.

Switch(config)#uldp aggressive-mode

3.4.8 uldp enable

Command: uldp enable

Function: ULDP will be enabled after issuing this command. In global configuration mode, this command will enable ULDP for the global. In port configuration mode, this command will enable ULDP for the port.

Parameters: None.

Command Mode: Global Configuration Mode and Port Configuration Mode.

Default: By default ULDP is not configured.

Usage Guide: ULDP can be configured for the ports only if ULDP is enabled globally. If ULDP is enabled globally, it will be effect for all the existing fiber ports. For copper ports and fiber ports which are available after ULDP is enabled, this command should be issued in the port configuration mode to make ULDP be effect.

Example: Enable ULDP in global configuration mode.

Switch(config)#uldp enable

3.4.9 uldp disable

Command: uldp disable

Function: To disable ULDP configuration through this command.

Parameters: None.

Command Mode: Global Configuration Mode and Port Configuration Mode.

Default: By default ULDP is not configured.

Usage Guide: When ULDP is disabled globally, then ULDP in all the ports will be disabled.

Example: To disable the ULDP configuration in global configuration mode.

Switch(config)#uldp disable

3.4.10 uldp hello-interval

Command: uldp hello-interval <*integer*>

no uldp hello-interval

Function: To configure the interval for ULDP to send hello messages. The no form of this command will restore the default interval for the hello messages.

Parameters: <*integer*>: The interval for the Hello messages, with its value limited between 5 and 100 seconds, 10 seconds by default.

Command Mode: Global Configuration Mode.

Default: 10 seconds by default.

Usage Guide: Interval for hello messages can be configured only if ULDP is enabled globally, its value limited between 5 and 100 seconds.

Example: To configure the interval of Hello messages to be 12 seconds.

Switch(config)#uldp hello-interval 12

3.4.11 uldp manual-shutdown

Command: uldp manual-shutdown

no uldp manual-shutdown

Function: To configure ULDP to work in manual shutdown mode. The no command will restore the automatic mode.

Parameters: None.

Command Mode: Global Configuration Mode.

Default: Auto mode.

Usage Guide: This command can be issued only if ULDP has been enabled globally.

Example: To enable manual shutdown globally.

Switch(config)#uldp manual-shutdown

3.4.12 uldp recovery-time

Command: uldp recovery-time*<integer>*

no uldp recovery-time

Function: To configure the interval for ULDP recovery timer. The no form of this command will restore the default configuration.

Parameters: *<integer>*: the time out value for the ULDP recovery timer. Its value is limited between 30 and 86400 seconds.

Command Mode: Global Configuration Mode.

Default: 0 is set by default which means the recovery is disabled.

Usage Guide: If an interface is shutdown by ULDP, and the recovery timer times out, the interface will be reset automatically. If the recovery timer is set to 0, the interface will not be reset.

Example: To set the recovery timer to be 600 seconds.

Switch(config)#uldp recovery-time 600

3.4.13 uldp reset

Command: uldp reset

Function: To reset the port when ULDP is shutdown.

Parameters: None.

Command Mode: Globally Configuration Mode and Port Configuration Mode.

Default: None.

Usage Guide: This command can only be effect only if the specified interface is disabled by ULDP.

Example: To reset all the port which are disabled by ULDP.

Switch(config)#uldp reset

3.4.14 show uldp

Command: show uldp [interface ethernet*<interface-name>*]

Function: To show the global ULDP configuration and status information of interface. If

<interface-name> is specified, ULDP configuration and status about the specified interface as well as its neighbors' will be displayed.

Parameters: ***<interface-name>*** is the interface name.

Command Mode: Admin and Configuration Mode.

Default: None.

Usage Guide: If no parameters are appended, the global ULDP information will be displayed. If the interface name is specified, information about the interface and its neighbors will be displayed along with the global information.

Example: To display the global ULDP information.

Switch(config)#show uldp

3.5 LLDP

3.5.1 clear lldp remote-table

Command: clear lldp remote-table

Function: Clear the Remote-table on the port.

Parameters: None.

Default: Do not clear the entries.

Command Mode: Port Configuration Mode.

Usage Guide: Clear the Remote table entries on this port.

Example: Clear the Remote table entries on this port.

Switch(Config-If-Ethernet 1/0/1)# clear lldp remote-table

3.5.2 debug lldp

Command: debug lldp

no debug lldp

Function: Enable the debug information of LLDP function, the no operation of this command will disable the debug information of LLDP function.

Parameters: None.

Default: Disable the debug information of LLDP function.

Command Mode: Admin Mode.

Usage Guide: When the debug switch is enabled, users can check the receiving and sending of packets and other information.

Example: Enable the debug switch of LLDP function on the switch.

Switch#debug lldp

3.5.3 debug lldp packets

Command: debug lldp packets interface ethernet <*IFNAME*>

no debug lldp packets interface ethernet <*IFNAME*>

Function: Display the message-receiving and message-sending information of LLDP on the port; the no operation of this command will disable the debug information switch.

Parameters: None.

Default: Disable the debug information on the port.

Command Mode: Admin Mode.

Usage Guide: When the debug switch is enabled, users can check the receiving and sending of packets and other information on the port.

Example: Enable the debug switch of LLDP function on the switch.

Switch#debug lldp packets interface ethernet 1/0/1

%Jan 01 00:02:40 2006 LLDP-PDU-TX PORT= ethernet 1/0/1

3.5.4 lldp enable

Command: lldp enable

lldp disable

Function: Globally enable LLDP function; **disable** command globally disables LLDP function.

Parameters: None.

Default: Disable LLDP function.

Command Mode: Global Mode.

Usage Guide: If LLDP function is globally enabled, it will be enabled on every port.

Example: Enable LLDP function on the switch.

Switch(config)#lldp enable

3.5.5 lldp enable (Port)

Command: lldp enable

lldp disable

Function: Enable the LLDP function module of ports in port configuration mode; **disable** command will disable the LLDP function module of port.

Parameters: None.

Default: the LLDP function module of ports is enabled by default in port configuration mode.

Command Mode: Port Configuration Mode.

Usage Guide: When LLDP is globally enabled, it will be enabled on every port, the switch on a port is used to disable this function when it is unnecessary on the port.

Example: Disable LLDP function of port on the port ethernet 1/0/5 of the switch.

Switch(config)#in ethernet 1/0/5

Switch(Config-If-Ethernet1/0/5)#lldp disable

3.5.6 lldp management-address tlv

This command **is not supported by the switch.**

3.5.7 lldp mode

Command: lldp mode <*send | receive | both | disable*>

Function: Configure the operating state of LLDP function of the port.

Parameters: send: Configure the LLDP function as only being able to send messages.

receive: Configure the LLDP function as only being able to receive messages.

both: Configure the LLDP function as being able to both send and receive messages.

disable: Configure the LLDP function as not being able to send or receive messages.

Default: The operating state of the port is “both”.

Command Mode: Port Configuration Mode.

Usage Guide: Choose the operating state of the lldp Agent on the port.

Example: Configure the state of port ethernet 1/0/5 of the switch as “receive”.

Switch(config)#in ethernet 1/0/5

Switch(Config-If-Ethernet1/0/5)#lldp mode receive

3.5.8 lldp msgTxHold

Command: lldp msgTxHold <*value*>

no lldp msgTxHold

Function: Set the multiplier value of the aging time carried by update messages sent by the all ports with LLDP function enabled, the value ranges from 2 to 10.

Parameters: <*value*> is the aging time multiplier, ranging from 2 to 10.

Default: the value of the multiplier is 4 by default.

Command Mode: Global Mode.

Usage Guide: After configuring the multiplier, the aging time is defined as the product of the multiplier and the interval of sending messages, and its maximum value is 65535 seconds.

Example: Set the value of the aging time multiplier as 6.

Switch(config)#lldp msgTxHold 6

3.5.9 lldp neighbors max-num

Command: lldp neighbors max-num <*value*>

no lldp neighbors max-num

Function: Set the maximum number of entries can be stored in Remote MIB.

Parameters: <*value*> is the configured number of entries, ranging from 5 to 500.

Default: The maximum number of entries can be stored in Remote MIB is 100.

Command Mode: Port Configuration Mode.

Usage Guide: The maximum number of entries can be stored in Remote MIB.

Example: Set the Remote as 200 on port ethernet 1/0/5 of the switch.

Switch(config)#in ethernet 1/0/5

Switch(Config-If-Ethernet1/0/5)# lldp neighbors max-num 200

3.5.10 lldp notification interval

Command: lldp notification interval <*seconds*>

no lldp notification interval

Function: When the time interval ends, the system is set to check whether the Remote Table has been changed. If it has, the system will send Trap to the SNMP management end.

Parameters: <*seconds*>is the time interval, ranging from 5 to 3600 seconds.

Default: The time interval is 5 seconds.

Command Mode: Global Mode.

Usage Guide: After configuring the notification time interval, a “trap” message will be sent at the end of this time interval whenever the Remote Table changes.

Example: Set the time interval of sending Trap messages as 20 seconds.

Switch(config)#lldp notification interval 20

3.5.11 lldp tooManyNeighbors

Command: lldp tooManyNeighbors {discard | delete}

Function: Set which operation will be done when the Remote Table is full.

Parameters: discard: discard the current message.

delete: Delete the message with the least TTL in the Remoter Table.

Default: Discard.

Command Mode: Port Configuration Mode.

Usage Guide: When the Remote MIB is full, Discard means to discard the received message; Delete means to the message with the least TTL in the Remoter Table.

Example: Set port ethernet 1/0/5 of the switch as delete.

Switch(config)#in ethernet 1/0/5

Switch(Config-If-Ethernet1/0/5)#lldp tooManyNeighbors delete

3.5.12 lldp transmit delay

Command: lldp transmit delay <*seconds*>

no lldp transmit delay

Function: Since local information might change frequently because of the variability of the network environment, there could be many update messages sent in a short time. So a delay is required to guarantee an accurate statistics of local information.

When transmit delay is the default value and tx-interval is configured via some commands, transmit delay will become one fourth of the latter, instead of the default 2.

Parameters: <*seconds*>is the time interval, ranging from 1 to 8192 seconds.

Default: The interval is 2 seconds by default.

Command Mode: Global Mode.

Usage Guide: When the messages are being sent continuously, a sending delay is set to prevent the Remote information from being updated repeatedly due to sending messages simultaneously.

Example: Set the delay of sending messages as 3 seconds.
Switch(config)#lldp transmit delay 3

3.5.13 lldp transmit optional tlv

Command: lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]
no lldp transmit optional tlv
Function: Configure the type of optional TLV of the port.
Parameters: portDesc: the description of the port; **sysName:** the system name; **sysDesc:** The description of the system; **sysCap:** the capability of the system.
Default: The messages carry no optional TLV by default.
Command Mode: Port Configuration Mode.
Usage Guide: When configuring the optional TLV, each TLV can only appear once in a message, **portDesc** optional TLV represents the name of local port; **sysName** optional TLV represents the name of local system; **sysDesc** optional TLV represents the description of local system; **sysCap** optional TLV represents the capability of local system.
Example: Configure that port ethernet 1/0/5 of the switch carries portDesc and sysCap TLV.
Switch(config)#in ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)# lldp transmit optional tlv portDesc sysCap

3.5.14 lldp trap

Command: lldp trap <*enable* | *disable*>
Function: enable: configure to enable the Trap function on the specified port; **disable:** configure to disable the Trap function on the specified port.
Parameters: None.
Default: The Trap function is disabled on the specified port by default.
Command Mode: Port Configuration Mode.
Usage Guide: The function of sending Trap messages is enabled on the port.
Example: Enable the Trap function on port ethernet 1/0/5 of the switch.
Switch(config)#in ethernet1/0/5
Switch(Config-If-Ethernet1/0/5)#lldp trap enable

3.5.15 lldp tx-interval

Command: lldp tx-interval <*integer*>
no lldp tx-interval
Function: Set the interval of sending update messages on all the ports with LLDP function enabled, the value of which ranges from 5 to 32768 seconds and is 30 seconds by default.
Parameters: ***<integer>*** is the interval of sending updating messages, ranging from 5 to 32768 seconds.
Default: 30 seconds.
Command Settings: Global Mode.

Usage Guide: After configuring the interval of sending messages, LLDP messages can only be received after a period as long as configured. The interval should be less than or equal with half of aging time, for a too long interval will cause the state of being aged and reconstruction happen too often; while a too short interval will increase the flow of the network and decrease the bandwidth of the port. The value of the aging time of messages is the product of the multiplier and the interval of sending messages. The maximum aging time is 65535 seconds.
When tx-interval is the default value and transmit delay is configured via some commands, tx-interval will become four times of the latter, instead of the default 40.
Example: Set the interval of sending messages as 40 seconds.
Switch(config)#lldp tx-interval 40

3.5.16 show debugging lldp

Command: show debugging lldp
Function: Display all ports with lldp debug enabled.
Parameters: None.
Default: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: With show debugging lldp, all ports with lldp debug enabled will be displayed.
Example: Display all ports with lldp debug enabled.
Switch(config)#show debugging lldp
====BEGINNING OF LLDP DEBUG SETTINGS====
debug lldp
debug lldp packets interface Ethernet1/0/1
debug lldp packets interface Ethernet1/0/2
debug lldp packets interface Ethernet1/0/3
debug lldp packets interface Ethernet1/0/4
debug lldp packets interface Ethernet1/0/5
==========END OF DEBUG SETTINGS==========

3.5.17 show lldp

Command: show lldp
Function: Display the configuration information of global LLDP, such as the list of all the ports with LLDP enabled, the interval of sending update messages, the configuration of aging time, the interval needed by the sending module to wait for re-initialization, the interval of sending TRAP, the limitation of the number of the entries in the Remote Table.
Parameters: None.
Default: Do not display the configuration information of global LLDP.
Command Mode: Admin Mode, Global Mode.
Usage Guide: Users can check all the configuration information of global LLDP by using 'show lldp'.
Example: Check the configuration information of global LLDP after it is enabled on the switch.

```
Switch(config)#show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP enabled port : Ethernet 1/0/1
LLDP interval :30
LLDP txTTL :120
LLDP txShutdownWhile :2
LLDP NotificationInterval :5
LLDP txDelay :20
-------------END------------------
```

3.5.18 show lldp interface ethernet

Command: show lldp interface ethernet *<IFNAME>*

Function: Display the configuration information of LLDP on the port, such as: the working state of LLDP Agent.

Parameters: <*IFNAME*>: Interface name.

Default: Do not display the configuration information of LLDP on the port.

Command Mode: Admin Mode, Global Mode.

Usage Guide: Users can check the configuration information of LLDP on the port by using "show lldp interface ethernet XXX".

Example: Check the configuration information of LLDP on the port after LLDP is enabled on the switch.

```
Switch(config)#show lldp interface ethernet 1/0/1
Port name :      ethernet 1/0/1
  LLDP Agent Adminstatus: Both
  LLDP Operation TLV: portDecs   sysName   sysDesc   sysCap
  LLDP Trap Status: disable
  LLDP maxRemote: 100
  LLDP Overflow handle: discard
  LLDP interface remote status : Full
```

3.5.19 show lldp neighbors interface ethernet

Command: show lldp neighbors interface ethernet < *IFNAME* >

Function: Display the LLDP neighbor information of the port.

Parameters: None.

Default: Do not display the LLDP neighbor information of the port.

Command Mode: Admin Mode, Global Mode.

Usage Guide: Users can check the LLDP neighbor information of the port by using "show lldp neighbors interface ethernet XXX".

Example: Check the LLDP neighbor information of the port after LLDP is enabled on the port.

```
Switch(config)#show lldp neighbors interface ethernet 1/0/1
```

3.5.20 show lldp traffic

Command: show lldp traffic

Function: Display the statistics of LLDP data packets.

Parameters: None.

Default: Do not display the statistics of LLDP data packets.

Command Mode: Admin Mode, Global Mode.

Usage Guide: Users can check the statistics of LLDP data packets by using “show lldp traffic”.

Example: Check the statistics of LLDP data packets after LLDP is enabled on the switch.

Switch(config)#show lldp traffic

PortName	Ageouts	FramesDiscarded	FramesInErrors	FramesIn	FramesOut	TLVsDiscarded	TLVsUnrecognized
Ethernet1/0/1	0	0	0	0	7	0	0

3.6 LLDP-MED

3.6.1 civic location

Command: civic location {dhcp server | switch | endpointDev} *<country-code>*

no civic location

Function: Configure device type and country code of the location with Civic Address LCI format and enter Civic Address LCI address mode. The no command cancels all configurations of the location with Civic Address LCI format.

Parameters: dhcp server: Set device type to be DHCP server

switch: Set device type to be Switch

endpointDev: Set device type to be LLDP-MED Endpoint

country-code: Set country code which consist of 2 letters, such as DE or US, it should accord the country code of ISO 3166 standard.

Default: No location with Civic Address LCI format is configured on the port.

Command Mode: Port mode

Usage Guide: Configure device type and country code of the location with Civic Address LCI format and enter Civic Address LCI address mode to configure the more detailed location.

Example: Configure device type as switch and country code as US for the location with Civic Address LCI format on Ethernet 19.

Switch(Config-If-Ethernet1/0/19)# civic location switch US

Switch(Med-Civic)#

3.6.2 {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}

Command: {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo} <*address*>
no {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}
Function: Configure the detailed location after enter Civic Address LCI address mode of the port.
Parameters: description-language: language for describing location, such as 'English'
province-state: state, canton, region, province prefecture, and so on, such as 'clara'
city: city, such as 'New York'
county: county, parish, such as 'santa clara'
street: street, such as '1301 Shoreway Road'
locationNum: house number, such as '9'
location: name and occupant of a location, such as 'Carrillo's Holiday Market'
floor: floor number, such as '13'
room: room number, such as '1308'
postal: postal/zip code, such as '10027-1234'
otherInfo: Additional location information, such as 'South Wing'
address: detailed address information, it cannot exceed 250 characters
Default: No detailed information of the location with Civic Address LCI is configured on the port.
Command Mode: Civic Address LCI address mode
Usage Guide: With this command, configure the detailed information of the location with Civic Address LCI on the port, it is able to configure 10 kinds of address types at most.
Example: Configure the detailed location information in Civic Address LCI address mode.
Switch(Med-Civic)# city example
Switch(Med-Civic)# street shangdi

3.6.3 ecs location

Command: ecs location <*tel-number*>
no ecs location
Function: Configure the location with ECS ELIN format on the port, the no command cancels the configured location.
Parameter: <*tel-number*>: location characters with ECS ELIN format, such as emergent telephone number, it is character string with the length between 10 and 25.
Default: No location with ECS ELIN format is configured.
Command Mode: Port mode
Usage Guide: Length range of the location character string between 10 and 25 with ECS ELIN format.

Example: Configure the location of ECS ELIN format on port 19.
Switch(Config-If-Ethernet1/0/19)# ecs location 880-445-3381

3.6.4 lldp med fast count

Command: lldp med fast count <*value*>
no lldp med fast count
Function: When the fast LLDP-MED startup mechanism is enabled, it needs to fast send LLDP packets with LLDP-MED TLV, this command sets the value of sending the packets fast, the no command restores the default value.
Parameter: value: The number of sending the packets fast, its range from 1 to 10, unit is entries.
Default: 4.
Command Mode: Global mode
Usage Guide: With this command, set the number for sending the packets fast.
Example:
Switch(config)#lldp med fast count 5

3.6.5 lldp med trap

Command: lldp med trap {enable | disable}
Function: Configure the specified port to enable or disable the function for sending TRAP message when LLDP-MED network topology is changed.
Parameters: enable: Enable LLDP-MED TRAP for the port
disable: Disable LLDP-MED TRAP for the port
Default: Disable LLDP-MED TRAP.
Command Mode: Port mode
Usage Guide: Enable or disable LLDP-MED TRAP of the port.
Example: Enable LLDP-MED TRAP of the port 19.
Switch(Config-If-Ethernet1/0/19)# lldp med trap enable

3.6.6 lldp transmit med tlv all

Command: lldp transmit med tlv all
no lldp transmit med tlv all
Function: Configure the specified port to send all LLDP-MED TLVs, the no command disables the function.
Parameter: None.
Default: Port does not enable the function for Sending LLDP-MED TLV.
Command Mode: Port mode
Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED TLV supported by all switches. However, LLDP packets sent by the port without any LLDP-MED TLV after the switch configured the corresponding no command.
Example: Port 19 enables the function for sending LLDP-MED TLV.

Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv all

3.6.7 lldp transmit med tlv capability

Command: lldp transmit med tlv capability
no lldp transmit med tlv capability
Function: Configure the specified port to send LLDP-MED Capability TLV. The no command disables the capability.
Parameter: None.
Default: The function is disabled for sending LLDP-MED Capability TLV.
Command Mode: Port mode
Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED Capability TLV. However, LLDP packets sent by the port without LLDP-MED Capability TLV after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV is the important LLDP-MED TLV, if do not configure the port to send LLDP-MED Capability TLV firstly, other LLDP-MED TLV will not be sent.
Example: Port 19 enables the function for sending LLDP-MED Capability TLV.
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv capability

3.6.8 lldp transmit med tlv extendPoe

Command: lldp transmit med tlv extendPoe
no lldp transmit med tlv extendPoe
Function: Configure the specified port to send LLDP-MED Extended Power-Via-MDI TLV. The no command disables the capability.
Parameter: None.
Default: The function is disabled for sending LLDP-MED Extended Power-Via-MDI TLV.
Command Mode: Port mode
Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Extended Power-Via-MDI TLV sent by the port. However, LLDP packets without LLDP-MED Extended Power-Via-MDI TLV sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Extended Power-Via-MDI TLV, or else the configuration cannot be successful. If the device does not support PoE or PoE function of the port is disabled, although configuring this command, LLDP-MED Extended Power-Via-MDI TLV will not be sent.
Example: Port 19 enables the function for sending LLDP-MED Extended Power-Via-MDI TLV.
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv extendPoe

3.6.9 lldp transmit med tlv location

Command: lldp transmit med tlv location
no lldp transmit med tlv location
Function: Configure the specified port to send LLDP-MED Location Identification TLV. The no

command disables this capability.
Parameters: None.
Default: Disable.
Command Mode: Port Mode.
Usage Guide: Configure the specified port to send LLDP-MED Location Identification TLV. After configured this command, if the port has the capability of sending LLDP-MED TLV, the LLDP packets sent from the port will include LLDP-MED Location Identification TLV. Otherwise, the LLDP packets sent from the port will not include LLDP-MED Location Identification TLV by the no command even if the port has the capability of sending LLDP-MED TLV. Notice: Before configuring this function, the capability of sending LLDP-MED Capability TLV must be configured. If the device does not support POE or the POE function of the port is disabled by the command, this TLV will not be sent.
Example: Enable the port 19 to send LLDP-MED Location Identification TLV.
Switch(Config-If-Ethernet1/0/19)#lldp transmit med tlv location

3.6.10 lldp transmit med tlv inventory

Command: lldp transmit med tlv inventory
no lldp transmit med tlv inventory
Function: Configure the specified port to send LLDP-MED Inventory Management TLVs aggregation, TLVs aggregation includes 7 TLVs, they are Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV, Asset ID TLV. The no command disables the capability.
Parameter: None.
Default: The function is disabled for sending LLDP-MED Inventory Management TLVs.
Command Mode: Port mode
Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Inventory Management TLVs sent by the port. However, LLDP packets without LLDP-MED Inventory Management TLVs sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Inventory Management TLVs, or else the configuration cannot be successful.
Example: Port 19 enables the function for sending LLDP-MED Inventory Management TLVs.
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv inventory

3.6.11 lldp transmit med tlv networkPolicy

Command: lldp transmit med tlv networkPolicy
no lldp transmit med tlv networkPolicy
Function: Configure the specified port to send LLDP-MED Network Policy TLV. The no command disables the capability.
Parameter: None.
Default: The function is disabled for sending LLDP-MED Network Policy TLV.

Command Mode: Port mode

Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Network Policy TLV sent by the port. However, LLDP packets without LLDP-MED Network Policy TLV sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Network Policy TLV, or else the configuration cannot be successful.

Example: Port 19 enables the function for sending LLDP-MED Network Policy TLV.

Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv networkPolicy

3.6.12 network policy

Command: network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} [status {enable | disable}] [tag {tagged | untagged}] [vid {*<vlan-id>* | dot1p}] [cos <*cos-value*>] [dscp <*dscp-value*>]

no network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming- video | video-signaling}

Function: Configure the network policy of the port, including VLAN ID, the supported application (such as voice and video), the application priority and the used policy, and so on.

Parameters: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video and video-signaling: the application types are supported by the port.

status: Whether the network policy is usable.

enable: Network Policy of the specified application type has been defined, enable is the default value of the network policy.

disable: Network Policy of the specified application type is unknownnnnn, the fields (such as VLAN ID, L2 priority and DSCP) are ignored, network connection device will not send TLV of the specified application type.

tag: Configure the specified application to uses **tagged** or **untagged** VLAN method.

tagged: Configure the flow of the specified application to use the tagged vlan method, here, the fields (such as VLAN ID, Layer2 priority and DSCP value) are take effect.

untagged: Configure the flow without tag for the specified application, the fields (such as VLAN ID, Layer2 priority) are ignored, only DSCP value field takes effect. Untagged is the default value of VLAN method.

vid: Configure VLAN ID that the specified application belongs to. When the peer sends the flow of the specified application, it will tag the notified VLAN ID, or else the vlan-id value is 1.

vlan-id: Configure the value of VLAN ID, its range from 1 to 4094.

dot1p: Configure the specified application to tag the flow by using 802.1p priority, at the same time, use vlan 0 to load the flow.

cos: Configure the priority of Ethernet frame for VLAN.

cos-value: Configure the value of Ethernet frame priority for VLAN, its range from 0 to 7, the default value is 5.

dscp: Configure DSCP of VLAN.

dscp-value: DSCP value input by the user, its range from 0 to 63, the default value is 46.
Default: No network policy is configured on the port.
Command Mode: Port mode
Usage Guide: User is able to configure the network policy of many kinds on a port, but their application types cannot repeat, and a kind of network policy corresponds to a LLDP-MED network policy TLV. If user configures multi-policy for a port, it will send multi-LLDP-MED network policy TLV to a LLDP packet. If user does not configure any network policy, no LLDP-MED network policy TLV is sent to LLDP packet.
Example: Configure the network policy with the application type of voice on port 19.
Switch(Config-If-Ethernet1/0/19)# network policy voice tag tagged vid 2 cos 6 dscp 23

3.6.13 show lldp

Command: show lldp
Function: Show the global LLDP and LLDP-MED configuration.
Parameter: None.
Default: None.
Command Mode: Admin mode
Usage Guide: None.
Example: Show the global LLDP and LLDP-MED configuration.
Switch#show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP has been enabled globally.
LLDP enabled port : Ethernet1/0/19
LLDP interval :5
LLDP txTTL :20
LLDP NotificationInterval :5
LLDP txDelay :1
LLDP-MED FastStart Repeat Count :4
----------END----------

3.6.14 show lldp [interface ethernet <IFNAME>]

Command: show lldp [interface ethernet <IFNAME>]
Function: Show LLDP and LLDP-MED configurations on the current port.
Parameter: [interface ethernet <IFNAME>]: Port name
Command Mode: Admin mode
Default: None.
Usage Guide: None.
Example: Show LLDP and LLDP-MED configuration of the port 19.
Switch#show lldp interface ethernet 1/0/19

Port name :Ethernet1/0/19

LLDP Agent Adminstatus : Both
LLDP Operation TLV : default
LLDP Trap Status : disable
LLDP maxRemote :100
LLDP Overflow handle : discard
LLDP interface remote status : Free

MED Optional TLV : capabilities networkPolicy location power inventory
MED Trap Status:Enable
MED TLV Transmit Status:Disable
MED Fast Transmit Status:Disable

3.6.15 show lldp neighbors

Command: show lldp neighbors [interface ethernet <*IFNAME*>]
Function: Show LLDP and LLDP-MED information of the neighbors for the port.
Parameter: None.
Default: None.
Command Mode: Admin mode
Usage Guide: With this command, checking LLDP and LLDP-MED information of the neighbors after the port received LLDP packets sent by the neighbors.
Example: Show the neighbor information on port 1.
Switch #show lldp neighbors interface ethernet 1/0/1

Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :00-03-0f-00-00-02
PortIdSubtype :Local
PortId :3
PortDesc :Ethernet1/0/1
SysName :switch
SysDesc :switch Device, Compiled Feb 12 17:39:53 2011
SoftWare Version 6.2.30.0
BootRom Version 4.0.1
HardWare Version
Device serial number
Copyright (C) 2001-2011 by Vendor.
All rights reserved

3.6.16 show lldp traffic

Command: show lldp traffic

Function: Show the statistics of the sent and received packets of LLDP and LLDP-MED.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: After the port received the LLDP packets from the neighbor, this command can be used to view the statistics of the sent and received packets of LLDP and LLDP-MED.

Example: View the statistics of the sent and received packets after the LLDP function is enabled.

```
Switch(config)#show lldp traffic
PortName    Ageouts    FramesDiscarded    FramesInErrors    FramesIn    FramesOut
TLVsDiscarded    TLVsUnrecognized
-----------    -------    ---------------    --------------    --------    ---------
-------------    ----------------
Ethernet1/0/1    0    0    0    0    7
0    0
```

3.7 Port Channel

3.7.1 debug port-channel

Command: debug port-channel <*port-group-number*> {all | event | fsm | packet | timer}

no debug port-channel [<*port-group-number*>]

Function: Open the debug switch of port-channel.

Parameters: <*port-group-number*> is the group number of port channel, ranging from 1～125

all: all debug information

event: debug event information

fsm: debug the state machine

packet: debug LACP packet information

timer: debug the timer information

Command mode: Admin mode.

Default: Disable the debugging of port-channel.

Usage Guide: Open the debug switch to check the debug information of port-channel.

Example:

(1)debug the state machine for port-group 1.

Switch#debug port-channel 1 fsm

(2) debug LACP packet information for port-group 2.

Switch#debug port-channel 2 packet

(3) debug all for port-group 1.

Switch#debug port-channel 1 all

3.7.2 interface port-channel

Command: interface port-channel *<port-channel-number>*

Function: Enters the port channel configuration mode

Command mode: Global Mode

Usage Guide: On entering aggregated port mode, configuration to GVRP or spanning tree modules will apply to aggregated ports; if the aggregated port does not exist (i.e., ports have not been aggregated), an error message will be displayed and configuration will be saved and will be restored until the ports are aggregated. Note such restoration will be performed only once, if an aggregated group is ungrouped and aggregated again, the initial user configuration will not be restored. If it is configuration for modules, such as shutdown configuration, then the configuration to current port will apply to all member ports in the corresponding port group.

Example: Entering configuration mode for port-channel 1.

Switch(config)#interface port-channel 1

Switch(Config-If-Port-Channel1)#

3.7.3 lacp port-priority

Command: lacp port-priority <*port-priority*>

no lacp port-priority

Function: Set the port priority of LACP protocol.

Parameters: <*port-priority*>: the port priority of LACP protocol, the range from 0 to 65535.

Command mode: Port Mode.

Default: The default priority is 32768 by system.

Usage Guide: Use this command to modify the port priority of LACP protocol, the no command restores the default value.

Example: Set the port priority of LACP protocol.

Switch(Config-If-Ethernet1/0/1)# lacp port-priority 30000

3.7.4 lacp system-priority

Command: lacp system-priority <*system-priority*>

no lacp system-priority

Function: Set the system priority of LACP protocol.

Parameters: <*system-priority*>: The system priority of LACP protocol, ranging from 0 to 65535.

Command mode: Global Mode

Default: The default priority is 32768.

Usage Guide: Use this command to modify the system priority of LACP protocol, the no command restores the default value.

Example: Set the system priority of LACP protocol.

Switch(config)#lacp system-priority 30000

3.7.5 lacp timeout

Command: lacp timeout {short | long}

no lacp timeout

Function: Set the timeout mode of LACP protocol.

Parameters: The timeout mode includes long and short.

Command mode: Port Mode

Default: Long.

Usage Guide: Set the timeout mode of LACP protocol.

Example: Set the timeout mode as short in LACP protocol.

Switch(Config-If-Ethernet1/0/1)#lacp timeout short

3.7.6 load-balance

Command: load-balance {dst-src-mac | dst-src-ip | dst-src-mac-ip}

Function: Set load-balance mode for switch, it takes effect for port-group and ECMP at the same time.

Parameter: dst-src-mac performs load-balance according to the source and destination MAC

dst-src-ip performs load-balance according to the destination and source IP

dst-src-mac-ip performs load-balance according to the destination and source MAC, the destination and source IP

Command mode: Global mode.

Default: Perform load-balance according to the source and destination MAC.

Usage Guide**:** Use port-channel or ECMP to implement load-balance, user can configure the load-balance mode according to the requirements. If the specific load-balance mode of the command line is different with the current load-balance mode, then modify the load-balance as the specific load-balance of command line; otherwise return a message to notice that the current mode is already configured.

Example: Set load-balance mode.

Switch(config)#load-balance src-mac-ip

3.7.8 load-balance hash-random

Command: load-balance hash-random

Function: Randomly generate hash factors that do not rely on message fields, i.e. do not rely on traffic samples.

Parameters: none.

Command mode: Gloeble Mode

Default: Not enabled.

Usage Guide: Increase the load mode of PRNG (Pseudo Random Number Generator), which randomly generates hash factors and does not rely on message fields, i.e. does not rely on traffic samples. The disadvantage is that the path order cannot be guaranteed, for example, if only a fixed traffic is entered, it will also be randomly shared.

Example:
Switch(config)#load-balance hash-random

3.7.9 load-balance ingress-port

Command: load-balance ingress-port
Function: Load sharing based on the input port as a hash factor.
Parameters: none.
Command mode: Gloeble Mode
Default: Not enabled.
Usage Guide: Load sharing based on the input port as a hash factor.
Example:
Switch(config)#load-balance ingress-port

3.7.10 load-balance hash-shift

Command: load-balance hash-shift { ipv4 | ipv6 } { dstip| srcip} value <0-3>
Function: When performing load sharing based on the IP field, determine the field where the IP header is offset to the right.
Parameters: none.
Command mode: Gloeble Mode
Default: Not enabled.
Usage Guide: When performing load sharing based on the IP field, determine the field where the IP header is offset to the right.
Example:
Switch(config)#lload-balance hash-shift ipv6 dstip value 1

3.7.11 load-balance enhanced profile

This command is not supported by the switch.

3.7.12 l2 field

This command is not supported by the switch.

3.7.13 l2 mpls field l2payload

This command is not supported by the switch.

3.7.14 l2 mpls field l3payload

This command is not supported by the switch.

3.7.15 ipv4 field

This command is not supported by the switch.

3.7.16 ipv6 field

This command is not supported by the switch.

3.7.17 l3 mpls field

This command is not supported by the switch.

3.7.18 mpls tunnel field

This command is not supported by the switch.

3.7.19 mim field l2payload

This command is not supported by the switch.

3.7.20 mim field l3payload

This command is not supported by the switch.

3.7.21 mim tunnel field

This command is not supported by the switch.

3.7.22 trill field l2payload

This command is not supported by the switch.

3.7.23 trill field l3payload

This command is not supported by the switch.

3.7.24 trill tunnel field l2payload

This command is not supported by the switch.

3.7.25 trill tunnel field l3payload

This command is not supported by the switch.

3.7.26 trill tunnel field outerl2

This command is not supported by the switch.

3.7.27 port-group

Command: port-group <*port-group-number*>
no port-group <*port-group-number*>
Function: Creates a port group. The no command deletes that group.
Parameters: <*port-group-number*> is the group number of a port channel from 1～125.
Default: There is no port-group.
Command mode: Global Mode

Example: Creating a port group.
Switch(config)# port-group 1
Delete a port group.
Switch(config)#no port-group 1

3.7.28 port-group mode

Command: port-group <*port-group-number*> mode {active | passive | on}
no port-group
Function: Add a physical port to port channel, the no operation removes specified port from the port channel.
Parameters: <*port-group-number*> is the group number of port channel, from 1～125; **active** enables LACP on the port and sets it in Active mode; **passive** enables LACP on the port and sets it in Passive mode; **on** forces the port to join a port channel without enabling LACP.
Command mode: Port Mode.
Default: Switch ports do not belong to a port channel by default; LACP not enabled by default.
Usage Guide: Every port joined the port-group must be consistent on the rate, configuration and physical property. If the specified port group does not exist, then print a error message. All ports in a port group must be added in the same mode, i.e., all ports use the mode used by the first port added. Adding a port in “on” mode is a “forced” action, which means the local end switch port aggregation does not rely on the information of the other end, port aggregation will succeed as long as all ports have consistent VLAN information. Adding a port in “active” or “passive” mode enables LACP. Ports of at least one end must be added in “active” mode, if ports of both ends are added in “passive” mode, the ports will never aggregate.

Example: Under the Port Mode of Ethernet1/0/1, add current port to “port-group 1” in “active”

mode.
Switch(Config-If-Ethernet1/0/1)#port-group 1 mode active

3.7.29 show port-group

Command: show port-group [*<port-group-number>*] {brief | detail |}
Function: Display the specified group number or the configuration information of all port-channel which have been configured.
Parameters: ***<port-group-number>*** is the group number of port channel to be displayed, from 1～125; **brief** displays summary information; **detail** displays detailed information.
Command mode: All Configuration Mode.
Usage Guide: If the user does not input port-group-number, that means the information of all the existent port-group are showed; if the port channel corresponds to port-group-number parameter and is not exist, then print a error message, otherwise display the current port-channel information of the specified group number.

Example: 1. Display summary information for port-group 1.
Switch#show port-group brief
ID: port group number; Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
the first is selected ports number, the second is standby ports number, and
the third is unselected ports number.

```
ID    Mode    Partner ID                        Ports        Load-balance
-----------------------------------------------------------------------------------
1     active    0x8000,00-12-cf-4d-e1-a1    8,1,1        dst-src-mac
10    passive 0x8000,00-12-cf-4d-e1-b2    8,2,0        dst-src-ip
20    on                                        8,0,0        dst-src-mac-ip
```

2. Display the detailed information of port-group 1.
Switch#show port-group 1 detail
Flags: A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted, H -- Expired

Port-group number: 1, Mode: active, Load-balance: dst-src-mac
Port-group detail information:
System ID: 0x8000,00-03-0f-0c-16-6d
Local:

```
Port                Status        Priority   Oper-Key    Flag
-----------------------------------------------------------
   Ethernet1/0/1        Selected      32768        1          {ACDEF}
   Ethernet1/0/2        Selected      32768        1          {ACDEF}
```

```
   Ethernet1/0/3        Selected      32768       1          {ACDEF}
   Ethernet1/0/4        Selected      32768       1          {ACDEF}
   Ethernet1/0/5        Selected      32768       1          {ACDEF}
   Ethernet1/0/6        Selected      32768       1          {ACDEF}
   Ethernet1/0/7        Selected      32768       1          {ACDEF}
   Ethernet1/0/8        Selected      32768       1          {ACDEF}
   Ethernet1/0/20       Unselected    32768       1          {ACG}
Ethernet1/0/23       Standby       32768       1          {AC}

Remote:
Actor                Partner   Priority   Oper-Key    SystemID                        Flag
-----------------------------------------------------------------------------
Ethernet1/0/1        1          32768       1          0x8000,00-03-0f-01-02-04       {CDEF}
   Ethernet1/0/2        2          32768       1          0x8000,00-03-0f-01-02-04       {CDEF}
   Ethernet1/0/3        3          32768       1          0x8000,00-03-0f-01-02-04       {CDEF}
   Ethernet1/0/4        4          32768       1          0x8000,00-03-0f-01-02-04       {CDEF}
   Ethernet1/0/5        5          32768       1          0x8000,00-03-0f-01-02-04       {CDEF}
   Ethernet1/0/6        6          32768       1          0x8000,00-03-0f-01-02-04       {CDEF}
   Ethernet1/0/7        7          32768       1          0x8000,00-03-0f-01-02-04       {CDEF}
   Ethernet1/0/8        8          32768       1          0x8000,00-03-0f-01-02-04       {CDEF}
   Ethernet1/0/23       23         32768       1          0x8000,00-03-0f-01-02-04       {C}
Switch#
```

3.7.30 show load-balance enhanced-profile

This command is not supported by the switch.

3.8 MTU

3.8.1 mtu

Command: mtu [<mtu-value>]

no mtu

Function: Enable the mtu receiving function. The no command restores to the normal frame range of 64--1518.

Parameter: mtu-value: the MTU value of frames that can be received, in byte, ranging from <1500-9000>. The corresponding frame size is <1518/1522-9018/9022>. Without setting is

parameter, the allowed max frame size is 9018/9022.

Default: MTU function not enabled by default.

Command Mode: Global Mode

Usage Guide: Set switch of both ends mtu necessarily, or mtu frame will be dropped at the switch has not be set.

Example: Enable the mtu function of the switch.

Switch(config)#mtu

3.9 bpdu-tunnel

3.9.1 bpdu-tunnel dmac

Command: bpdu-tunnel dmac <mac>

no bpdu-tunnel dmac

Function: Configure the tunnel MAC address globally, the no command restores the default tunnel MAC address.

Parameter: <mac>: MAC address

Command Mode: Global mode

Default: Default MAC address.

Usage Guide: Configure the tunnel MAC address globally, use the configured MAC (it must be multicast MAC address) to forward the specified protocol across the tunnel.

Example: Configure the tunnel MAC address.

Switch(Config)# bpdu-tunnel dmac 01-02-03-04-05-06

3.9.2 bpdu-tunnel stp

Command: bpdu-tunnel stp

no bpdu-tunnel stp

Function: Configure the specified port to forward stp packets across the tunnel, the no command cancels the operation.

Parameter: None.

Command Mode: Port mode

Default: Port does not forward any protocol packets across the tunnel.

Usage Guide: Disable stp function on the port before configuring this command.

Example: Configure Ethernet 1/0/5 to forward stp packets across the tunnel.

Switch(Config)#in Ethernet 1/0/5

Switch(Config-if-ethernet 1/0/5)#bpdu-tunnel stp

3.9.3 bpdu-tunnel gvrp

Command: bpdu-tunnel gvrp
no bpdu-tunnel gvrp
Function: Configure the specified port to forward gvrp packets across the tunnel, the no command cancels the operation.
Parameter: None.
Command Mode: Port mode
Default: Port does not forward any protocol packets across the tunnel.
Usage Guide: Disable gvrp function on the port before configuring this command.
Example: Configure Ethernet 1/0/5 to forward gvrp packets across the tunnel.
Switch(Config)#in ethernet 1/0/5
Switch(Config-if-ethernet 1/0/5)#bpdu-tunnel gvrp

3.9.4 bpdu-tunnel uldp

Command: bpdu-tunnel uldp
no bpdu-tunnel uldp
Function: Configure the specified port to forward uldp packets across the tunnel, the no command cancels the operation.
Parameter: None.
Command Mode: Port mode
Default: Port does not forward any protocol packets across the tunnel.
Usage Guide: Disable uldp function on the port before configuring this command.
Example: Configure Ethernet 1/0/5 to forward uldp packets across the tunnel.
Switch(Config)#in ethernet 1/0/5
Switch(Config-if-ethernet 1/0/5)#bpdu-tunnel uldp

3.9.5 bpdu-tunnel lacp

Command: bpdu-tunnel lacp
no bpdu-tunnel lacp
Function: Configure the specified port to forward lacp packets across the tunnel, the no command cancels the operation.
Parameter: None.
Command Mode: Port mode
Default: Port does not forward any protocol packets across the tunnel.
Usage Guide: Disable lacp function on the port before configuring this command.
Example: Configure Ethernet 1/0/5 to forward lacp packets across the tunnel.
Switch(Config)#in ethernet 1/0/5
Switch(Config-if-ethernet 1/0/5)#bpdu-tunnel lacp

3.9.6 bpdu-tunnel dot1x

Command: bpdu-tunnel dot1x
no bpdu-tunnel dot1x
Function: Configure the specified port to forward dot1x packets across the tunnel, the no command cancels the operation.
Parameter: None.
Command Mode: Port mode
Default: Port does not forward any protocol packets across the tunnel.
Usage Guide: Disable dot1x function on the port before configuring this command.
Example: Configure Ethernet 1/0/5 to forward dot1x packets across the tunnel.
Switch(Config)#in ethernet 1/0/5
Switch(Config-if-ethernet 1/0/5)#bpdu-tunnel dot1x

3.9.7 bpdu-tunnel-protocol

This command is not supported by the switch.

3.9.8 bpdu-tunnel-protocol group-mac

This command is not supported by the switch.

3.9.9 bpdu-tunnel-protocol protocol-mac

This command is not supported by the switch.

3.9.10 bpdu-tunnel-protocol ethernetii

This command is not supported by the switch.

3.9.11 bpdu-tunnel-protocol snap

This command is not supported by the switch.

3.9.12 bpdu-tunnel-protocol llc

This command is not supported by the switch.

3.10 DDM

3.10.1 clear transceiver threshold-violation

Command: clear transceiver threshold-violation [interface ethernet <interface-list>]
Function: Clear the threshold violation of the transceiver monitoring.
Parameter: interface ethernet <interface-list>: The interface list that the threshold violation of the transceiver monitoring needs to be cleared.
Command Mode: Admin mode
Default: None.
Usage Guide: None.
Example: Clear he threshold violation of the transceiver monitoring on port 21, 25, 26, 28.
Switch#clear transceiver threshold-violation interface ethernet 1/0/21;25-26;28

3.10.2 debug transceiver

Command: debug transceiver {on | off}
Function: Enable/disable DDM debugging.
Parameter: on/off: Enable or disable the debugging.
Command Mode: Admin mode
Default: Off.
Usage Guide: Disable the DDM debugging with ctrl+o.
Example: Enable DDM debugging.
Switch#debug transceiver on

3.10.3 show transceiver

Command: show transceiver [interface ethernet <interface-list>] [detail]
Function: Show the monitoring of the transceiver.
Parameter: interface ethernet <interface-list>: The interface list that the monitoring of the transceiver needs to be shown.
detail：Show the detailed monitoring of the transceiver.
Command Mode: User mode, admin mode and global mode
Default: None.
Usage Guide: Temperature can be accurate to the integer, other values can be accurate to the second bit after the radix point. When the parameter exceeds the warning threshold, it is shown with 'W+' or 'W-', when the parameter exceeds the alarm threshold, it is shown with 'A+' or 'A-', no tagged parameter is normal.
Example: Show the brief DDM information of all ports.
Switch#show transceiver

Interface	Temp（℃）	Voltage（V）	Bias（mA）	RX Power（dBM）	TX Power（dBM）
1/0/25	33	3.31	6.11	-30.54(A-)	-6.01

1/0/26	33	5.00（W+）	6.11	-20.54(W-)	-6.02

3.10.4 show transceiver threshold-violation

Command: show transceiver threshold-violation [interface ethernet <interface-list>]

Function: Show the transceiver monitoring.

Parameter: interface ethernet <interface-list>: The interface list that the transceiver monitoring needs to be shown.

Command Mode: Admin mode and global mode

Default: None.

Usage Guide: None.

Example: Show the transceiver monitoring.

Switch(config)#show transceiver threshold-violation interface ethernet 1/0/25-26

Ethernet 1/0/25 transceiver threshold-violation information：Transceiver monitor is enabled. Monitor interval is set to 30 minutes.

The current time is Jan 02 12:30:50 2010.

The last threshold-violation time is Jan 01 1:30:50 2010.

Brief alarm information:

RX loss of signal

RX power low

Detail diagnostic and threshold information:

	Diagnostic			Threshold	
	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn
	----------	----------	----------	----------	---------
Temperature（℃）	33	70	0	70	0
Voltage（V）	7.31	10.00	0.00	5.00	0.00
Bias current（mA）	3.11	10.30	0.00	5.00	0.00
RX Power（dBM）	-30.54(A-)	9.00	-25.00（-34）	9.00	-25.00
TX Power（dBM）	-1.01	9.00	-12.05	9.00	-10.00

Ethernet 1/0/22 transceiver threshold-violation information:

Transceiver monitor is disabled. Monitor interval is set to 30 minutes.

The last threshold-violation doesn’t exist.

3.10.5 transceiver-monitoring

Command: transceiver-monitoring {enable | disable}

Function: Enable/ disable the transceiver monitoring.

Parameter: enable/ disable: Enable or disable the function.

Command Mode: Port mode

Default: Disable.

Usage Guide: None.

Example: Enable the transceiver monitoring of ethernet1/0/1.
Switch(config-if-ethernet1/0/1)#transceiver-monitoring enable

3.10.6 transceiver-monitoring interval

Command: transceiver-monitoring interval <minutes>
no transceiver-monitoring interval
Function: Set the interval of the transceiver monitoring. The no command sets the interval to be the default interval of 15 minutes.
Parameter: <minutes>: The interval of the transceiver monitoring needs to be set.
Command Mode: Global mode
Default: 15 minutes.
Usage Guide: None.
Example: Set the interval of the transceiver monitoring as 1 minute.
Switch(config)#transceiver-monitoring interval 1

3.10.7 transceiver threshold

Command: transceiver threshold {default | {temperature | voltage | bias | rx-power | tx-power} {high-alarm | low-alarm | high-warn | low-warn} {<value> | default}}
Function: Set the threshold defined by the user.
Parameters: default: Restore the threshold as the default threshold set by the manufacturer. If the monitoring index is not specified, restore all thresholds, if the monitoring index is specified, restore the corresponding threshold only.
temperature：The monitoring index—temperature
voltage：The monitoring index—voltage
bias：The monitoring index—bias current
rx-power：The monitoring index—receiving power
tx-power：The monitoring index—sending power
high-alarm：High-alarm of the monitoring index, namely there is alarm with A+ if exceeding the threshold.
low-alarm：Low-alarm of the monitoring index, namely there is alarm with A- if exceeding the threshold.
high-warn：High-warn of the monitoring index, namely there is warning with W+ if exceeding the threshold.
low-warn：Low-warn of the monitoring index, namely there is warning with W- if exceeding the threshold.
Command Mode: Port mode
Default: The threshold is set by the manufacturer.
Usage Guide: The range of the threshold parameters is shown for each monitoring index in the following:
Temperature: -128.00~128.00 ℃
Voltage: 0.00~7.00 V

Bias current: 0.00~140.00 mA

x-power: -50.00~9.00 dBM

tx-power: -50.00~9.00 dBM

The maximum length of the threshold parameter configured by the user is 20 bits. After the user configured a parameter threshold, the threshold set by the manufacturer will be labeled with the bracket when showing the threshold, and decide whether give an alarm according to the user's configuration.

Example: Configure tx-power threshold of the fiber module, the low-warn threshold is configured as -12 on ethernet1/0/1.

Switch(config-if-ethernet1/0/1)#transceiver threshold tx-power low-warn -12

3.10.8 optician monitor enable|disable

Command: optician monitor enable|disable

Function: Enable or disable tsfpmonitor thread.

Parameters: None.

Command Mode: Global mode.

Default: Enable.

Usage Guide: None.

Example: Enable the monitor of tsfpmonitor thread.

Switch(config)#optician monitor enable

Insert optical module**:**

%MODULE-1-INSERT: connector of Ethernet1/0/48 is inserted!

Pull out optical module**:**

%MODULE-1-INSERT: connector of Ethernet1/0/48 is removed!

Switch(config)#optician monitor disable

Insert optical module, it will have no output prompts.

3.11 EFM OAM

3.11.1 clear ethernet-oam

Command: clear ethernet-oam [interface {ethernet |} <*IFNAME*>]

Function: Clear the statistic information of packets and link event on specific or all ports for OAM.

Parameters: <*IFNAME*>, the name of the port needs to clear OAM statistic information

Command Mode: Admin mode

Default: N/A.

Usage Guide: N/A.

Example: Clear the statistic information of OAM packets and link event on all ports.

Switch#clear ethernet-oam

3.11.2 debug ethernet-oam error

Command: debug ethernet-oam error [interface {ethernet |} <*IFNAME*>]

no debug ethernet-oam error [interface {ethernet |} <*IFNAME*>]

Function: Enable the debugging of OAM error information, no command disables it.

Parameters: <*IFNAME*>: name of the port that the debugging will be enabled or disabled.

Command Mode: Admin mode

Default: Disable.

Usage Guide: N/A.

Example: Enable the debugging of OAM error information for ethernet1/0/1.

Switch#debug ethernet-oam error interface ethernet1/0/1

3.11.3 debug ethernet-oam event

This command is not supported by the switch.

3.11.4 debug ethernet-oam fsm

Command: debug ethernet-oam fsm {all | Discovery | Transmit} [interface {ethernet |} <*IFNAME*>]

no debug ethernet-oam fsm {all | Discovery | Transmit} [interface {ethernet |} <*IFNAME*>]

Function: Enable the debugging of OAM state machine, no command disables it.

Parameters: <IFNAME>: name of the port that the debugging will be enabled or disabled

Command Mode: Admin mode

Default: Disable.

Usage Guide: N/A.

Example: Enable the debugging of Discovery state machine for ethernet1/0/1.

Switch#debug ethernet-oam fsm Discovery interface ethernet1/0/1.

3.11.5 debug ethernet-oam packet

Command: debug ethernet-oam packet [detail] {all | send | receive} [interface {ethernet |} <*IFNAME*>]

no debug ethernet-oam packet [detail] {all | send | receive} interface {ethernet |} <*IFNAME*>

Function: Enable the debugging of packets received or sent by OAM, no command disables the debugging.

Parameters: <*IFNAME*>: name of the port that the debugging will be enabled or disabled

Command Mode: Admin mode

Default: Disable.

Usage Guide: N/A.

Example: Enable the debugging of packets received or sent for ethernet1/0/1.

Switch#debug ethernet-oam packet detail all interface ethernet1/0/1

3.11.6 debug ethernet-oam timer

Command: debug ethernet-oam timer {all | pdu_timer | local_lost_link_timer} [interface {ethernet |} <IFNAME>]

no debug ethernet-oam timer {all | pdu_timer | local_lost_link_timer} [interface {ethernet | } <IFNAME>]

Function: Enable the debugging of refreshing information for specific or all timers, no this command disables the debugging.

Parameters: <*IFNAME*>: name of the port that the debugging will be enabled or disabled

Command Mode: Admin mode

Default: Disable.

Usage Guide: N/A.

Example: Enable the debugging of refreshing information for all timers of ethernet1/0/1.

Switch#debug ethernet-oam timer all interface ethernet1/0/1

3.11.7 ethernet-oam

Command: ethernet-oam

no ethernet-oam

Function: Enable ethernet-oam of ports, no command disables ethernet-oam of ports.

Parameters: None.

Command Mode: Port mode

Default: Disable.

Usage Guide: N/A.

Example: Enable ethernet-oam of Ethernet 1/0/4.

Switch(config)#interface ethernet 1/0/4

Switch(Config-If-Ethernet1/0/4)#ethernet-oam

3.11.8 ethernet-oam errored-frame threshold high

Command: ethernet-oam errored-frame threshold high {<*high-frames*> | none}

no ethernet-oam errored-frame threshold high

Function: Configure the high threshold of errored frame event, no command restores the default value.

Parameters: <*high-frames*>, the high detection threshold of errored frame event, ranging from 2 to 4294967295.

none, cancel the high threshold configuration.

Command Mode: Port mode

Default: none.

Usage Guide: During the specific detection period, serious link event is induced if the number of errored frame is larger than or equal to the high threshold and the device notifies the peer by

sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold can not be less than the low threshold.

Example: Configure the high threshold of errored frame event on Ethernet 1/0/4 to be 3000.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold high 3000

3.11.9 ethernet-oam errored-frame threshold low

Command: ethernet-oam errored-frame threshold low <*low-frames*>

no ethernet-oam errored-frame threshold low

Function: Configure the low threshold of errored frame event, no command restores the default value.

Parameters: <*low-frames*>, the low detection threshold of errored frame event, ranging from 1 to 4294967295.

Command Mode: Port mode

Default: 1.

Usage Guide: During the specific detection period, errored frame event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold can not be larger than the high threshold.

Example: Configure the low threshold of errored frame event on Ethernet 1/0/4 to 100.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold low 100

3.11.10 ethernet-oam errored-frame window

Command: ethernet-oam errored-frame window <*seconds*>

no ethernet-oam errored-frame window

Function: Configure the detection period of errored frame event, no command restores the default value.

Parameters: <*seconds*> is the time for counting the specified frame number, its range from 5 to 300, unit is 200ms.

Command Mode: Port mode

Default: 5.

Usage Guide: Detect the errored frame number of the port after the time of specific detection period. If the number of errored frame is larger than or equal to the threshold, bring the corresponding event and notify the peer through OAMPDU.

Example: Configure the detection period of errored frame event on port1/0/4 to be 20s.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame window 100

3.11.11 ethernet-oam errored-frame-period threshold high

Command: ethernet-oam errored-frame-period threshold high {<*high-frames*> | none}

no ethernet-oam errored-frame-period threshold high

Function: Configure the high threshold of errored frame period event, no command restores the default value.

Parameters: <*high-frames*>, the high detection threshold of errored frame period event, ranging from 2 to 4294967295.

none, cancel the high threshold configuration.

Command Mode: Port mode

Default: none.

Usage Guide: During the specific detection period, serious link event is induced if the number of errored frame is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold can not be less than the low threshold.

Example: Configure the high threshold of errored frame period event on port 1/0/4 to be 3000.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-period threshold high 3000

3.11.12 ethernet-oam errored-frame-period threshold low

Command: ethernet-oam errored-frame-period threshold low <*low-frames*>

no ethernet-oam errored-frame-period threshold low

Function: Configure the low threshold of errored frame period event, no command restores the default value.

Parameters: <*low-frames*>, the low detection threshold of errored frame period event, ranging from 1 to 4294967295 frames.

Command Mode: Port mode

Default: 1.

Usage Guide: During the specific detection period, errored frame period event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.

Example: Configure the low threshold of errored frame period event on port 1/0/4 to be 100.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-period threshold low 100

3.11.13 ethernet-oam errored-frame-period window

Command: ethernet-oam errored-frame-period window <*seconds*>

no ethernet-oam errored-frame-period window

Function: Configure the detection period of errored frame period event, no command restores the default value.

Parameters: <*seconds*> is the time for counting the specified frame number, its range from 1 to 300, unit is 200ms.

Command Mode: Port mode

Default: 5.

Usage Guide: Detect errored frame of the port after the time of specific detection period. If the number of errored frame is larger than or equal to the threshold, corresponding event is induced and the device notifies the peer through OAMPDU. When sending the packets, the maximum number of frames is filled as the value of window in errored frame period event. The conversion rule is maximum number of frames= interface bandwidth×detection period of errored frame period event(s)÷(64×8), of which the detection period is the number of seconds in window of the configuration.

Example: Configure the detection period of errored frame period event on port 1/0/4 to be 10s.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-period window 50

3.11.14 ethernet-oam errored-frame-seconds threshold high

Command: ethernet-oam errored-frame-seconds threshold high {<*high-seconds*> | none}

no ethernet-oam errored-frame-seconds threshold high

Function: Configure the high threshold of errored frame seconds event, no command restores the default value.

Parameters: <*high-seconds*>, the high detection threshold of errored frame seconds event, ranging from 2 to 65535 seconds.

none, cancel the high threshold configuration.

Command Mode: Port mode

Default: none.

Usage Guide: During the specific detection period, serious link event is induced if the number of errored frame seconds is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold should not be less than the low threshold. The definition of errored frame seconds is the second in which errored frame is received.

Example: Configure the high threshold of errored frame seconds event on port 1/0/4 to be 3000.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold high 3000

3.11.15 ethernet-oam errored-frame-seconds threshold low

Command: ethernet-oam errored-frame-seconds threshold low <*low-seconds*>

no ethernet-oam errored-frame-seconds threshold low

Function: Configure the low threshold of errored frame seconds event, no command restores the default value.

Parameters: <*low-seconds*>, the low detection threshold of errored frame seconds event, ranging from 1 to 65535 seconds.

Command Mode: Port mode

Default: 1.

Usage Guide: During the specific detection period, errored frame seconds event is induced if the number of errored frame seconds is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold should not be larger than the high threshold. The definition of errored frame seconds is the second in which errored frame is received.

Example: Configure the low threshold of errored frame seconds event on port 1/0/4 to be 100.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold low 100

3.11.16 ethernet-oam errored-frame-seconds window

Command: ethernet-oam errored-frame-seconds window <*seconds*>

no ethernet-oam errored-frame-seconds window

Function: Configure the detection period of errored frame seconds event, no command restores the default value.

Parameters: <*seconds*> is the time for counting the specified frame number, its range from 50 to 4500, unit is 200ms.

Command Mode: Port mode

Default: 300.

Usage Guide: Detect errored frame seconds of the port after the time of specific detection period. If the number of errored frame seconds is larger than or equal to the threshold, corresponding event is induced and the device notified the peer through OAMPDU.

Example: Configure the detection period of errored frame seconds event on port 1/0/4 to be 120s.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds window 600

3.11.17 ethernet-oam errored-symbol-period threshold high

Command: ethernet-oam errored-symbol-period threshold high {<*high-symbols*> | none}

no ethernet-oam errored-symbol-period threshold high

Function: Configure the high threshold of errored symbol event, no command restores the default value.

Parameters: <*high-symbols*>, the high detection threshold of errored symbol event, ranging from 2 to 18446744073709551615 symbols.

none, cancel the high threshold configuration.

Command Mode: Port mode

Default: none.

Usage Guide: During the specific detection period, serious link event is induced if the number of errored symbols is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold should not be less than the low threshold.

Example: Set the high threshold of errored symbol event on port 1/0/4 to none.
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold high none

3.11.18 ethernet-oam errored-symbol-period threshold low

Command: ethernet-oam errored-symbol-period threshold low <*low-symbols*>
no ethernet-oam errored-symbol-period threshold low

Function: Configure the low threshold of errored symbol event, no command restores the default value.

Parameters: <*low-symbols*>, the low threshold of errored symbol event, ranging from 1 to 18446744073709551615 symbols.
none, cancel the high threshold configuration.

Command Mode: Port mode

Default: 1.

Usage Guide: During the specific detection period, errored symbol event is induced if the number of errored symbols is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.

Example: Set the low threshold of errored symbol event on port 1/0/4 to be 5.
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold low 5

3.11.19 ethernet-oam errored-symbol-period window

Command: ethernet-oam errored-symbol-period window <*seconds*>
no ethernet-oam errored-symbol-period window

Function: Configure the detection period of errored symbol event, no command restores the default value.

Parameters: <*seconds*> is the time for counting the specified frame number, its range from 5 to 300, unit is 200ms.

Command Mode: Port mode

Default: 5.

Usage Guide: Detect errored symbols of the port after the time of specific detection period. If the number of errored symbols is larger than or equal to the threshold, corresponding event is induced and the device notified the peer through OAMPDU.

Example: Set the detection period of errored symbol event on port 1/0/4 to be 2s.
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period window 10

3.11.20 ethernet-oam link-monitor

Command: ethernet-oam link-monitor
no ethernet-oam link-monitor

Function: Enable link monitor, no command disables the function.
Parameters: None.
Command Mode: Port mode
Default: Enable.
Usage Guide: Enable OAM to monitor local link errors. Generally link monitor is enabled when enabling OAM function of the port. When OAM link monitor is disabled, although local link error is not monitored, Event information OAMPDU from the peer is still normally received and processed.
Example: Enable the link monitor of port 1/0/4.
Switch(Config-If-Ethernet1/0/4)#ethernet-oam link-monitor

3.11.21 ethernet-oam mode

Command: ethernet-oam mode {active | passive}
no ethernet-oam mode
Function: Configure the mode of OAM function, no command restores the default value.
Parameters: active, active mode
passive, passive mode
Command Mode: Port mode
Default: active mode.
Usage Guide: At least one of the two connected OAM entities should be configured to active mode. Once OAM is enabled, the working mode of OAM cannot be changed and you need to disable OAM function if you have to change the working mode.
Example: Set the mode of OAM function on ethernet 1/0/4 to passive mode.
Switch(Config-If-Ethernet1/0/4)#ethernet-oam mode passive

3.11.22 ethernet-oam period

Command: ethernet-oam period <*seconds*>
no ethernet-oam mode
Function: Configure the transmission period of Information OAMPDU, no command restores the default value.
Parameters: <*seconds*>, sending period, ranging from 1 to 2 seconds.
Command Mode: Port mode
Default: 1s.
Usage Guide: Use this command to configure the transmission interval of Information OAMPDU which keep OAM connection normally.
Example: Set the transmission interval of Information OAMPDU for ethernet 1/0/4 to be 2s.
Switch(Config-If-Ethernet1/0/4)# ethernet-oam period 2

3.11.23 ethernet-oam remote-failure

Command: ethernet-oam remote-failure

no ethernet-oam remote-failure

Function: Enable remote failure indication of OAM, no command disables the function.

Parameters: None.

Command Mode: Port mode

Default: Enable.

Usage Guide: With remote failure indication is enabled, if critical-event or link fault event is occurred locally, it will notify the peer by sending Information OAMPDU, log the fault information and send SNMP trap warning. When the remote failure indication is disabled, although local critical-event or link fault event is not monitored, failure indication information from the peer is still normally received and processed.

Example: Enable remote failure indication of ethernet 1/0/4.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-failure

3.11.24 ethernet-oam remote-loopback

Command: ethernet-oam remote-loopback

no ethernet-oam remote-loopback

Function: Local OAM entity sends remote loopback request to enable the remote end to enter OAM loopback mode, no command disables remote loopback.

Parameters: None.

Command Mode: Port mode

Default: Disable.

Usage Guide: Only OAM entities working in active mode can launch remote loopback request but the ones in passive mode cannot. When remote OAM entities work in loopback mode, all packets except OAMPDU return to the local port according to the original paths (note that normal communication cannot be performed in OAM loopback mode.) and network administrators can detect link delay, jitter and throughput through remote loopback. Remote loopback can only be achieved after OAM connection is established and the loopback will be automatically cancelled if OAM connection is disconnected during the loopback process. This command is mutually exclusive with **ethernet-oam remote-loopback supported** command.

Example: Enable remote OAM entity of ethernet 1/0/4 to enter remote loopback mode.

Switch(Config-If-Ethernet1/0/4)# ethernet-oam remote-loopback

Normal forwarding will be suspended during the remote-loopback, are you sure to start remote-loopback? [Y/N]

3.11.25 ethernet-oam remote-loopback supported

Command: ethernet-oam remote-loopback supported

no ethernet-oam remote-loopback supported

Function: Enable OAM loopback support of the port, no command disables it.

Parameters: None.

Command Mode: Port mode

Default: Disable.

Usage Guide: only ports with remote loopback support enabled can accept OAM loopback request and enter loopback mode. Therefore, make sure the remote end has configured loopback support when enabling it to enter OAM loopback. This command is mutually exclusive with **ethernet-oam remote-loopback** command.

Example: Enable OAM loopback support of ethernet 1/0/4.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback supported

3.11.26 ethernet-oam timeout

Command: ethernet-oam timeout *<seconds>*

no ethernet-oam timeout

Function: Configure the timeout of OAM connection, no command restores the default value.

Parameters: <*seconds*>, the timeout ranging from 5 to 10 seconds.

Command Mode: Port mode

Default: 5s.

Usage Guide: OAM connection will be disconnected if no OAMPDU is received after specified timeout.

Example: Set the timeout of OAM connection for ethernet 1/0/4 to be 6 seconds.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam timeout 6

3.11.27 show ethernet-oam

Command: show ethernet-oam [{local | remote} interface {ethernet |} <*IFNAME*>]

Function: Show Ethernet OAM connection of specified or all ports.

Parameters: Overview information of all Ethernet OAM connections will be shown if no parameters is input

local, show detailed information of local OAM connection

remote, show detailed information of remote OAM connection

<*IFNAME*>, the port that OAM connection information will be shown

Command Mode: Admin mode

Default: N/A.

Usage Guide: N/A.

Example: Show overview information of Ethernet OAM connection.

Switch#show ethernet-oam

Remote-Capability codes: L - Link Monitor, R - Remote Loopback

U - Unidirection, V - Variable Retrieval

Interface	Local-Mode	Local-Capability	Remote-MAC-Addr	Remote-Mode	Remote-Capability
1/0/1	active	L R	0003.0f02.2e5d	active	L R
1/0/2	active	L R	0003.0f19.3a3e	avtive	L R
1/0/4	active	L R	0003.0f26.480c	passive	L R
1/0/5	active	L R	0003.0f28.020a	active	L R

Field	Description
Interface	port with Ethernet OAM enabled
Local-Mode	Working mode of the local port OAM.
Local-Capability	Functions are supported by local port OAM L - Link Monitor, R - Remote Loopback U - Unidirection, V - Variable Retrieval
Remote-MAC-Addr	MAC address of the peer
Remote-Mode	OAM working mode of the peer
Remote-Capability	Functions are supported by OAM of the peer L - Link Monitor, R - Remote Loopback U - Unidirection, V - Variable Retrieval

Show detailed information of local OAM entity for ethernet 1/0/2:

```
Switch#show ethernet-oam local interface ethernet1/0/2
Ethernet1/0/2 oam local Information：
oam_status=enable
local _mode=active
period=1s
timeout=8s
Loopback Supported=YES
Unidirectional Support=YES
Link Events=YES
Remote Failure=YES
local_pdu=INFO
local_mux_action=FWD
local_par_action=DISCARD
Max_OAMPDU_Size=1518
---------------------------------------------------------------------------
OAM_local_flags_field：
Link Fault=0        Dying Gasp=0       Critical Events=0
---------------------------------------------------------------------------
Packet statistic：
Packets                 Send                    Receive
OAMPDU                  553                     21
Information             552                     21
Event Notification      1                       0
Loopback Control        0                       0
---------------------------------------------------------------------------
```

Field	Description
oam_status	Status of Ethernet OAM: enable, OAM is enabled; disable, OAM is not enabled.

local _mode	Working mode of Ethernet OAM: active, the port is set as active mode; passive, the port is set as passive mode.
Period	Transmission period of packets
Timeout	Timeout of connection
local_pdu	The way in which the local end processes Ethernet OAMPDUs: RX_INFO, the port only receives Information OAMPDUs and does not send any Ethernet OAMPDUs. LF_INFO, the port only sends Information OAMPDU packets without Information TLV and with their link error flag bits being set. INFO, the port only sends and receives Information OAMPDU packets. ANY, the port sends and receives any OAMPDU packets.
local_mux_action	Working mode of the local transmitter: FWD, the port can send any packets; DISCARD, the port only sends OAMPDU packets and discards others.
local_par_action	Working mode of the local receiver in the following: FWD, receiving any packets is allowed; DISCARD, only OAMPDU packets is received while others are discarded; LB, OAM remote loopback is enabled on the port. In this case, all the packets except OAMPDU packets received are returned to their sources along the ways they come.
Loopback Supported	Whether support remote loopback: YES for support and NO for not.
Unidirectional Support	Whether support unidirectional transmission: YES for support and NO for not.
Link Events	Whether support general link events: YES for support and NO for not.
Remote Failure	Whether support severe link events (remote failure indication): YES for support and NO for not.
Link Fault	Whether occur a Link Fault event: 0 for no and 1 for yes.
Dying Gasp	Whether occur a Dying Gasp event: 0 for no and 1 for yes.
Critical Event	Whether occur a Critical Event: 0 for no and 1 for yes.
Max_OAMPDU_Size	The maximum length of OAMPDU is supported.
OAMPDU	Show the number of the OAMPDU packets sent and received which is the sum of three kinds of packets.
Information	Show the number of the Information OAMPDU packets sent and received
Event Notification	Show the number of the Event Notification OAMPDU packets sent and received

Loopback Control	Show the number of the Loopback Control OAMPDU packets sent and received

Display detailed information of remote OAM entity for Ethernet 1/0/2
Switch#show ethernet-oam remote interface ethernet1/0/2
Ethernet1/0/2 oam remote Information：
Remote_Mac_Address=0003.0f19.3a3e
local _mode=active
---
local_pdu=INFO
local_mux_action=FWD
local_par_action=DISCARD
Loopback Supported=YES
Unidirectional Support=NO
Link Events=YES
Remote Failure=YES
Max_OAMPDU_Size=1518

OAM Remote Flags Field：
Link Fault=0 Dying Gasp=0 Critical Event=0

Field	Description
Remote_Mac_Address	MAC address of remote OAM entity
local _mode	Working mode of Ethernet OAM: active, the port is set as active mode; passive, the port is set as passive mode.
local_pdu	The way in which the local end processes Ethernet OAMPDUs: RX_INFO, the port only receives Information OAMPDUs and does not send any Ethernet OAMPDUs. LF_INFO, the port only sends Information OAMPDU packets without Information TLV and with their link error flag bits being set. INFO, the port only sends and receives Information OAMPDU packets. ANY, the port sends and receives any OAMPDU packets.
local_mux_action	Working mode of the local transmitter: FWD, the port can send any packets; DISCARD, the port only sends OAMPDU packets and discards others.
local_par_action	Working mode of the local receiver in the following: FWD, receiving any packets is allowed; DISCARD, only OAMPDU packets is received while others are discarded;

	LB, OAM remote loopback is enabled on the port. In this case, all the packets except OAMPDU packets received are returned to their sources along the ways they come.
Loopback Supported	Whether support remote loopback: YES for support and NO for not.
Unidirectional Support	Whether support unidirectional transmission: YES for support and NO for not.
Link Events	Whether support general link events: YES for support and NO for not.
Remote Failure	Whether support severe link events: YES for support and NO for not.
Max_OAMPDU_Size	The maximum length of OAMPDU is supported.
Link Fault	Whether occur a Link Fault event: 0 for no and 1 for yes.
Dying Gasp	Whether occur a Dying Gasp event: 0 for no and 1 for yes.
Critical Event	Whether occur a Critical Event: 0 for no and 1 for yes.

3.11.28 show ethernet-oam events

Command: show ethernet-oam events {local | remote} [interface {ethernet |} <*IFNAME*>]

Function: Shows the statistic information of link events on specified or all ports with OAM enabled, including general link events and severe link events.

Parameters: local, show the detailed information of the local events;

remote, show the detailed information of the remote events;

<IFNAME>, the port that the statistic information of OAM link events needs to be shown, the statistic information of OAM link events for all ports will be shown if this parameter is not specified.

Command Mode: Admin mode

Default: N/A.

Usage Guide: N/A.

Example: Show the statistic information of link events on Ethernet 1/0/1.

```
Switch#show ethernet-oam events local interface eth 1/0/1
ethernet1/0/1 link-events：
OAM_local_errored-symbol-period-events:
---------------------------------------------------------------------------------------------
event time stamp：3539                    errored symbol window(200ms)：5
errored symbol low threshold：1           errored symbol high threshold：none
errored symbol：1200120                   errored running total：2302512542
event running total：232

OAM_local_errored-frame-period-events:
---------------------------------------------------------------------------------------------
event time stamp：3539                    errored frame window(200ms)：50
```

errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：52

OAM_local_errored-frame-events:
---
event time stamp：3539 errored frame window(200ms)：5
errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：75

OAM_local_errored-frame-seconds-summary-events:
---
event time stamp：3520 errored frame seconds summary window(200ms)：300
errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：232

OAM_local_link-fault：0
OAM_local_dying gasp：0
OAM_local_critical event：0

Field	Description
OAM_local_errored-symbol-period-events	Statistic information of the local errored symbol events
OAM_local_errored-frame-period-events	Statistic information of the local errored frame period events
OAM_local_errored-frame-events	Statistic information of the local errored frame events
OAM_local_errored-frame-seconds-summary-events	Statistic information of the local errored frame seconds events
event time stamp	Time stamp of the event
window	Detection period of the event
low threshold	Low threshold of events detection
high threshold	High threshold of events detection
errored frame	the number of errored frames
errored symbol	the number of errored symbols
errored running total	Total number of errors occurred since the reset of OAM function
event running total	Total number of error events occurred since the reset of OAM function
OAM_local_link-fault	The number of the local link-fault faults
OAM_local_dying gasp	The number of the local dying-gasp faults

OAM_local_critical event	The number of the local critical-event faults

3.11.29 show ethernet-oam link-events-configuration

Command: show ethernet-oam link-events-configuration [interface {ethernet | } <*IFNAME*>]

Function: Show configuration of link events on specified or all ports with OAM enabled, including detection period and threshold of the events and so on.

Parameters: <*IFNAME*>, the port that the statistic information of OAM link events needs to be shown, the statistic information of OAM link events for all ports will be shown if this parameter is not specified.

Command Mode: Admin mode

Default: N/A.

Usage Guide: N/A.

Example: Show configuration of link events on ethernet 1/0/1.

```
Switch#show ethernet-oam link-events-configuration interface ethernet 1/0/1
Ethernet1/0/1 link-monitor configuration：
event                                  high-threshold      low-threshold      window(200ms)
-----------------------------------------------------------------------------------------------
Err-symbol-Period                          none                1                  2
Err-frame-Period                           none                1                 10
Err-frame                                   none                2                  5
Err-frame-second-summary                   none                2                600
-----------------------------------------------------------------------------------------------
```

Field	Description
Event	Event type
Err-symbol-Period	Errored symbol event
Err-frame-Period	Errored frame period event
Err-frame	Errored frame event
Err-frame-second-summary	Errored frame seconds event
high-threshold	High threshold
low-threshold	Low threshold
window(200ms)	Detection period, unit is 200ms

3.11.30 show ethernet-oam loopback-status

Command: show ethernet-oam loopback status [interface {ethernet |} <IFNAME>]

Function: Show OAM loopback status of specified or all ports.

Parameters: <IFNAME>, the port that OAM loopback status needs to be shown, OAM loopback status for all ports will be shown if this parameter is not specified.

Command Mode: Admin mode
Default: N/A.
Usage Guide: N/A.
Example: Show OAM loopback status of all ports.
Switch(config)#show ethernet-oam loopback status
OAM Loopback **Status：**
ethernet 1/0/1：disable
ethernet1/0/2：loopback_enable_waiting
ethernet1/0**/3：loopback**_disable_waiting
ethernet1/0/4：loopback_control
ethernet1/0/5：loopback_underControl

Field	Description
Disable	OAM loopback support is not enabled
loopback_enable_waiting	The local side is the loopback control end with remote loopback request sent and is waiting for the confirmation packets
loopback_disable_waiting	The local side is the loopback control end with remote loopback cancellation request sent and is waiting for the confirmation packets
loopback_control	The local side is the loopback control end and is in the loopback process
loopback_undercontrol	The local side is the loopback control end and is in the loopback process
no_loopback	OAM loopback support is enabled but no loopback request is received

3.12 PORT SECURITY

3.12.1 clear port-security

Command: clear port-security {all | configured | dynamic | sticky} [[address <*mac-addr*> | interface <*interface-id*>] [vlan <*vlan-id*>]]
Function: Clear the secure MAC entries for the interfaces.
Parameter: all：All secure MAC entries on the interfaces
configured：The configured secure MAC
dynamic：The dynamic secure MAC learnt by the interface
sticky：The secure MAC of sticky
mac-addr：The specified secure MAC address
interface-id：The secure MAC entries of the specified interface

vlan-id：The specified VLAN

Default: None.

Command Mode: Admin mode

Usage Guide: None.

Example: Clear all secure MACs on the interface.

Switch#clear port-security all

3.12.2 show port-security

Command: show port-security [interface <*interface-id*>] [address]

Function: Show port-security configuration.

Parameter: interface-id：Show port-security configuration of the interface.

address: Show the secure address of the interface.

Default: None.

Command Mode: Any modes

Usage Guide: None.

Example: Show all secure MACs on the interfaces.

Switch# show port-security address interface ethernet 1/0/1

3.12.3 switchport port-security

Command: switchport port-security

no switchport port-security

Function: Configure port-security function for the interface, the no command disables port-security.

Parameter: None.

Default: Disable.

Command Mode: Port mode

Usage Guide: Clear all dynamic MACs after the interface enabled port-security, and all MACs learnt from the interfaces are tagged with FDB_TYPE_PORT_SECURITY_DYNAMIC. After disabling port-security of the interfaces, clear all secure MACs or change them into the dynamic MACs.

Example: Enable port-security on the interface.

Switch(config-if- ethernet1/0/1)#switchport port-security

3.12.4 switchport port-security aging

Command: switchport port-security aging {static | time <*value*> | type {absolute | inactivity}}

no switchport port-security violation aging {static | time | type}

Function: Enable the aging entries of port-security, and specify the aging time and type on the interface.

Parameter: static：**Enable** the aging of the static MAC address configured on the specified interface.

time <*value*>：Specify MAC aging time of the interface, its range from 1 to 1440mins.

The default value is 0, that means disable the aging.

type：Specify the aging type

absolute：The expiration of the aging timer on the interface, all secure MACs of the interfaces will get aged and be removed from the MAC table.

inactivity：The expiration of the aging timer on the interface, the entries will get aged without the traffic, the entries are still kept in the aging period with the traffic.

Default: Do not enable port-security aging, the default aging time is 0.

Aging mode is absolute by default.

The static entries are not aged by default.

Command Mode: Port mode

Usage Guide: None.

Example: Configure the aging time of the secure MAC as 1 second on the interface.

Switch (config-if- ethernet1/0/1)# switchport port-security aging time 1

3.12.5 switchport port-security mac-address

Command: switchport port-security mac-address <*mac-address*> [vlan <*vlan-id*>]

no switchport port-security mac-address <*mac-address*> [vlan <*vlan-id*>]

Function: Configure the static secure MAC on the interface, the no command cancels the configuration.

Parameter: mac-address： Configure the specified MAC address as the static secure MAC.

vlan-id： The specified VLAN of the MAC address, it only takes effect on trunk and hybrid interfaces.

Default: No secure MAC is bound by the interface.

Command Mode: Port mode

Usage Guide: When configuring the static secure MAC, pay attention to the number of the current secure MAC whether exceed the maximum MAC limit allowed by the interface. If exceeding the maximum MAC limit, it will result in violation operation.

Example: Configure the secure MAC address on the interface.

Switch (config-if- ethernet1/0/1)# switchport port-security mac-address 00-00-00-00-00-01

3.12.6 switchport port-security mac-address sticky

Command: switchport port-security mac-address sticky [*mac-address*] [vlan <*vlan-id*>]

no switchport port-security mac-address sticky [*mac-address*] [vlan <*vlan-id*>]

Function: Configure the static secure MAC with the sticky type on the interface, the no command cancels the configured secure MAC.

Parameter: mac-address：Configure the specified MAC address as the static secure MAC with the sticky type.

vlan-id：The specified VLAN of the MAC address, it only takes effect on trunk and hybrid interfaces.

Default: No secure MAC is bound by the interface with the sticky type.

Command Mode: Port mode

Usage Guide: When configuring the static secure MAC with sticky type, pay attention to the number of the current secure MAC whether exceed the maximum MAC limit allowed by the interface. If exceeding the maximum MAC limit, it will result in violation operation.

Example: Configure the secure MAC address on the interface.

Switch(config-if-ethernet1/0/1)#switchport port-security mac-address sticky 00-00-00-00-00-01

3.12.7 switchport port-security maximum

Command: switchport port-security maximum <*value*> [vlan <*vlan-list*>]

no switchport port-security maximum <*value*> [vlan <*vlan-list*>]

Function: Configure the maximum number of the secure MAC allowed by the interface, if specifying VLAN parameter, it means the maximum number in the configured VLANs. The no command cancels the maximum number of the secure MAC configured by the interface.

Parameter: value： Configure the maximum number of the secure MAC allowed by the interface, its range between 1 and 128. It is determined by the maximum MAC number of the device.

vlan-id: Configure the maximum value for the specified VLAN, it only takes effect on trunk and hybrid interfaces.

Default: After enabling port-security, if there is no other configuration, the maximum number of the secure MAC is 1 on the interface. The interface number in VLAN is no limit by default

Command Mode: Port mode

Usage Guide: Pay attention to the coupling relation about the number between the interface and VLAN, set the maximum number configured by the interface as the standard firstly.

Example: Configure the maximum number of the secure MAC on the interface.

Switch(config-if- ethernet1/0/1)# switchport port-security maximum 100

3.12.8 switchport port-security violation

Command: switchport port-security violation {protect | recovery | restrict | shutdown}

no switchport port-security violation

Function: When exceeding the maximum number of the configured MAC addresses, MAC address accessing the interface does not belongs to this interface in MAC address table or a MAC address is configured to several interfaces in same VLAN, both of them will violate the security of the MAC address.

Parameter: protect：Protect mode, it will trigger the action that do not learn the new MAC, drop the package and do not send the warning.

recovery：After triggering the violation action of the port, the mac learning function can be recovered.

restrict：Restrict mode, it will trigger the action that do not learn the new MAC, drop the package, send snmp trap and record the configuration in syslog.

shutdown：Shutdown mode is the default mode. Under this condition, the interface is disabled directly, send snmp trap and record the configuration in syslog.

Default: Shutdown.

Command Mode: Port mode
Usage Guide: None.
Example: Configure violation mode as protect for the interface.
Switch(config-if-ethernet1/0/1)#switchport port-security violation protect

3.13 VLAN

3.13.1 vlan

Command: vlan WORD
no vlan WORD
Function: Create VLANs and enter VLAN configuration mode. If using ';' and '-' connect with multi-VLANs, then only create these VLANs. If only existing VLAN, then enter VLAN configuration mode; if the VLAN is not exist, then create VLAN and enter VLAN configuration mode. In VLAN Mode, the user can set VLAN name and assign the switch ports to the VLAN. The no command deletes specified VLANs.
Parameter: WORD is the VLAN ID to be created/deleted, valid range is 1 to 4094, connect with ';' and '-'.
Command mode: Global Mode.
Default: Only VLAN1 is set by default.
Usage Guide: VLAN1 is the default VLAN and cannot be configured or deleted by the user. The maximal VLAN number is 4094. It should be noted that dynamic VLANs learnt by GVRP cannot be deleted by this command.
Example: Create VLAN100 and enter the configuration mode for VLAN 100.
Switch(config)#vlan 100
Switch(Config-Vlan100)#

3.13.2 vlan internal

Command: vlan <2-4094> internal
Function: Specify the internal VLAN ID. After an ID is specified as the internal VLAN ID, it is not allowed to be used by other VLAN. Internal VLAN is only used to LOOPBACK interface and can not add physical port. New internal VLAN ID takes effect after save the configuration and reboot the switch.
Parameter: <*vlan-id*>: The ID is specified as internal VLAN ID, the range is 2 to 4094.
Command mode: Global Mode.
Default: 1006.
Usage Guide: Set 1006 as the default internal VLAN ID, the internal VLAN ID needs to be modified when the network set 1006 as VLAN ID. Internal VLAN ID must select an unused ID or else affect

other VLAN. This command takes effect after save the configuration and reboot the switch.
Example: Set 100 as the internal VLAN ID.
Switch(config)#vlan 100 internal

3.13.3 vlan ingress enable

Command: vlan ingress enable
no vlan ingress enable
Function: Enable the VLAN ingress filtering for a port; the "**no vlan ingress enable**" command disables the ingress filtering.
Command mode: Port Mode
Default: Enable VLAN ingress filtering function.
Usage Guide: After VLAN ingress filtering is enabled on the port, when the system receives data it will check source port first, and forwards the data to the destination port if it is the VLAN member port, or else drop the data.
Example: Disable VLAN ingress rules on the port.
Switch(Config-If-Ethernet1/0/1)# no vlan ingress enable

3.13.4 switchport trunk native vlan

Command: switchport trunk native vlan <*vlan-id*>
no switchport trunk native vlan
Function: Set the PVID for Trunk port; the "**no switchport trunk native vlan**" command restores the default setting.
Parameter: <*vlan-id*> is the PVID for Trunk port.
Command mode: Port Mode.
Default: The default PVID of Trunk port is 1.
Usage Guide: PVID concept is defined in 802.1Q. PVID in Trunk port is used to tag untagged frames. When an untagged frame enters a Trunk port, the port will tag the untagged frame with the native PVID set with this commands for VLAN forwarding.
Example: Set the native VLAN for a Trunk port to 100.
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode trunk
Switch(Config-If-Ethernet1/0/5)#switchport trunk native vlan 100
Switch(Config-If-Ethernet1/0/5)#exit

3.13.5 switchport trunk allowed vlan

Command: switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD | none}
no switchport trunk allowed vlan
Function: Set trunk port to allow VLAN traffic; the "**no switchport trunk allowed vlan**" command restores the default setting.

Parameter: WORD: specified VIDs; keyword;
all: all VIDs, the range from 1 to 4094;
add: add assigned VIDs behind **allow vlan**;
except: all VID add to **allow vlan** except assigned VIDs;
remove: delete assigned **allow vlan** from **allow vlan** list;
none: Discard all VLAN traffic.
Command mode: Port Mode.
Default: Trunk port allows all VLAN traffic by default.
Usage Guide: The user can use this command to set the VLAN traffic allowed to passthrough the Trunk port; traffic of VLANs not included are prohibited.
Example: Set Trunk port to allow traffic of VLAN1, 3, 5-20.
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode trunk
Switch(Config-If-Ethernet1/0/5)#switchport trunk allowed vlan 1;3;5-20
Switch(Config-If-Ethernet1/0/5)#exit

3.13.6 switchport mode trunk allow-null

Command: switchport mode trunk allow-null
Function: Add a port as trunk mode. When enabling GVRP, the mode that adds the ports with trunk mode to all VLANs is not appropriate. Therefore, add a port as trunk port and does not join any VLANs by default for enabling GVRP on trunk port is appropriate. It is recommended to configure a port as trunk with this command before enabling GVRP. This command can also be used when a port has been configured as trunk already, which equals to clearing allow-list and quits all VLANs.
Parameters: None
Command Mode: Port mode
Default: access mode.
Usage Guide: Configure the port as trunk, enable it to leave all VLANs and clear allow-list.
Example: Switch(config-if-ethernet1/0/1)#switchport mode trunk allow-null

3.13.7 switchport mode

Command: switchport mode {trunk | access | **hybrid}**
Function: Set the port in access mode, trunk mode or hybrid mode.
Parameter: trunk means the port allows traffic of multiple VLAN; **access** indicates the port belongs to one VLAN only; **hybrid** means the port allows the traffic of multi-VLANs to pass with tag or untag mode.
Command mode: Port Mode.
Default: The port is in Access mode by default.
Usage Guide: Ports in trunk mode is called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through. VLAN in different switches can be interconnected with the Trunk ports. Ports under access mode are called Access ports. An access port can be assigned to one and only

one VLAN at a time. Hybrid ports can allow traffic of multiple VLANs to pass through, receive and send the packets of multiple VLANs, used to connect switch, or user's computer. When Hybrid ports and Trunk ports receive the data, the deal way is same, but the deal way is different in sending the data. Because Hybrid ports can allow the packets of multiple VLANs to send with no tag, however, Trunk ports can only allow the packets of the default VLAN to send with no tag. The attribute of ports can not directly convert between Hybrid and Trunk, it must configure to be access at first, then configure to be Hybrid or Trunk. When the Trunk or Hybrid attribute is cancelled, the port attribute restores the default (access) attribute and belongs to vlan1.

Example: Set port 5 to trunk mode and port 8 to access mode, port 10 to hybrid mode.

Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode trunk
Switch(Config-If-Ethernet1/0/5)#exit
Switch(config)#interface ethernet 1/0/8
Switch(Config-If-Ethernet1/0/8)#switchport mode access
Switch(Config-If-Ethernet1/0/8)#exit
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/10)#exit

3.13.8 switchport interface

Command: switchport interface [ethernet | portchannel] [<interface-name | interface-list>]

no switchport interface [ethernet | portchannel] [<interface-name | interface-list>]

Function: Specify Ethernet port to VLAN; the no command deletes one or one set of ports from the specified VLAN.

Parameter: ethernet is the Ethernet port to be added. **portchannel** means that the port to be added is a link-aggregation port. **interface-name** port name, such as e1/0/1. If this option is selected, ethernet or portchannel should not be. **interface-list** is the port list to be added or deleted, ";" and "-" are supported, for example: ethernet1/0/1;3;4-7;8.

Command mode: VLAN Mode.

Default: A newly created VLAN contains no port by default.

Usage Guide: Access ports are normal ports and can join a VLAN, but a port can only join one VLAN for a time.

Example: Assign Ethernet port 1，3，4-7，8 of VLAN100.

Switch(Config-Vlan100)#switchport interface ethernet 1/0/1;3;4-7;8

3.13.9 switchport hybrid native vlan

Command: switchport hybrid native vlan <*vlan-id*>

no switchport hybrid native vlan

Function: Set the PVID for Hybrid port; the "**no switchport hybrid native vlan**" command restores the default setting.

Parameter: <*vlan-id*> is the PVID of Hybrid port.

Command mode: Port Mode.

Default: The default PVID of Hybrid port is 1.

Usage Guide: When an untagged frame enters a Hybrid port, it will be added a tag of the native PVID which is set by this command, and is forwarded to the native VLAN.

Example: Set the native vlan to 100 for a Hybrid port.

Switch(config)#interface ethernet 1/0/5

Switch(Config-If-Ethernet1/0/5)#switchport mode hybrid

Switch(Config-If-Ethernet1/0/5)#switchport hybrid native vlan 100

Switch(Config-If-Ethernet1/0/5)#exit

3.13.10 switchport hybrid allowed vlan

Command: switchport hybrid allowed vlan {WORD | all | add WORD | except WORD | remove WORD | none} {tag | untag}

no switchport hybrid allowed vlan

Function: Set hybrid port which allow the VLAN to pass with tag or untag method; the "**no switchport hybrid allowed vlan**" command restores the default setting.

Parameter: WORD: Set vlan List to allowed vlan, and the late configuration will cover the previous configuration;

all: Set all VLANs to allowed vlan;

add WORD: Add vlanList to the existent allowed vlanList;

except WORD: Set all VLANs to allowed vlan except the configured vlanList;

remove WORD: Delete the specific VLAN of vlanList from the existent allow vlanList;

none: Discard all VLAN traffic;

tag: Join the specific VLAN with tag mode;

untag: Join the specific VLAN with untag mode.

Command mode: Port Mode.

Default: Deny all VLAN traffic to pass.

Usage Guide: The user can use this command to set the VLANs whose traffic allowed to pass through the Hybrid port, traffic of VLANs not included are prohibited. The difference between tag and untag mode by setting allowed vlan: set VLAN to untag mode, the frame sent via hybrid port without VLAN tag; set VLAN to tag mode, the frame sent via hybrid port with corresponding VLAN tag. The same VLAN can not be allowed with tag and untag mode by a Hybrid port at the same time. If configure the tag (or untag) allowed VLAN to untag (or tag) allowed VLAN, the last configuration will cover the previous.

Example: Set hybrid port allowed vlan 1, 3, 5-20 with untag mode and allow vlan 100; 300; 500-2000 with tag mode.

Switch(config)#interface ethernet 1/0/5

Switch(Config-If-Ethernet1/0/5)#switchport mode hybrid

Switch(Config-If-Ethernet1/0/5)#switchport hybrid allowed vlan 1;3;5-20 untag

Switch(Config-If-Ethernet1/0/5)#switchport hybrid allowed vlan 100;300;500-2000 tag

Switch(Config-If-Ethernet1/0/5)#exit

3.13.11 switchport forbidden vlan

Command: switchport forbidden vlan {WORD | all | add WORD | except WORD | remove WORD}

no switchport forbidden vlan

Function: Configure the forbidden vlan for a port. Note that this command can only be used to configure on trunk or hybrid ports and the port with GVRP not enabled. No command cancels the forbidden vlanlist for a port.

Parameters: WORD, add the vlanList as forbidden vlan and cover the previous configuration

all, set all VLANs as forbidden vlan

add WORD, add vlanList to the current forbidden vlanList

except WORD, set all VLANs as forbidden vlan except vlanList

remove WORD, remove vlan specified by vlanList from current forbidden vlanList

Command Mode: Port mode

Default: Forbidden vlanList is empty

Usage Guide: Tag the corresponding position for forbidden vlanList and clear allow vlanList flags in ports. A port leaves these VLANs if it joins them statically, and it sends message to GVRP module to enable corresponding registered machine of the port to enter forbidden mode.

Example: Port quits the corresponding VLAN and the corresponding registered machine of GVRP to enter forbidden mode.

Switch(config-if-ethernet1/0/1)#switchport forbidden vlan all

3.13.12 switchport access vlan

Command: switchport access vlan <*vlan-id*>

no switchport access vlan

Function: Add the current Access port to the specified VLAN. The "**no switchport access vlan**" command deletes the current port from the specified VLAN, and the port will be partitioned to VLAN1.

Parameter: <*vlan-id*> is the VID for the VLAN to be added the current port, valid range is 1 to 4094.

Command mode: Port Mode.

Default: All ports belong to VLAN1 by default.

Usage Guide: Only ports in Access mode can join specified VLANs, and an Access port can only join one VLAN at a time.

Example: Add some Access port to VLAN100.

Switch(config)#interface ethernet 1/0/8

Switch(Config-If-Ethernet1/0/8)#switchport mode access

Switch(Config-If-Ethernet1/0/8)#switchport access vlan 100

Switch(Config-If-Ethernet1/0/8)#exit

3.13.13 show vlan

Command: show vlan [brief | summary] [id <*vlan-id*>] [name <*vlan-name*>] [internal usage [id *<vlan-id>* | name *<vlan-name>*]] [private-vlan [id *<vlan-id>* | name *<vlan-name>*]]

Function: Display detailed information for all VLANs or specified VLAN.

Parameter: brief stands for brief information; **summary** for VLAN statistics; ***<vlan-id>*** for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094; ***<vlan-name>*** is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters. **private-vlan** displays the ID, name, relating VLAN and port of the private-vlan relative information.

Command mode: Admin Mode and Configuration Mode.

Usage Guide: If no ***<vlan-id>*** or ***<vlan-name>*** is specified, then information for all VLANs in the switch will be displayed.

Example: Display the status for the current VLAN; display statistics for the current VLAN.

```
Switch#show vlan
VLAN Name                Type         Media        Ports
---- ------------ ---------- --------- ----------------------------------------
1    default              Static       ENET       Ethernet1/0/1     Ethernet1/0/2
                                                   Ethernet1/0/3     Ethernet1/0/4
                                                   Ethernet1/0/9     Ethernet1/0/10
                                                   Ethernet1/0/11    Ethernet1/0/12
2    VLAN0002       Static       ENET      Ethernet1/0/5       Ethernet1/0/6
                                                   Ethernet1/0/7         Ethernet1/0/8

Switch#show vlan summary
The max. vlan entrys: 4094

Existing Vlans:
Universal Vlan:
1 12 13 15 16 22
Total Existing Vlans is:6
```

Displayed information	Explanation
VLAN	VLAN number
Name	VLAN name
Type	VLAN type, statically configured or dynamically learned.
Media	VLAN interface type: Ethernet
Ports	Access port within a VLAN

```
Switch(config)#show vlan private-vlan
VLAN Name        Type   Asso  VLAN   Ports
---- ------------ ---------- --------- ----------------------------------------
100  VLAN0100   Primary  101    102      Ethernet1/0/9       Ethernet1/0/10
                                          Ethernet1/0/11
```

```
      Ethernet1/0/12
                                          Ethernet1/0/13
101   VLAN0101   Community 100          Ethernet1/0/9      Ethernet1/0/10
                                          Ethernet1/0/11     Ethernet1/0/12
                                          Ethernet1/0/13
102   VLAN0102   Isolate   100          Ethernet1/0/9
```

3.13.14 private-vlan association

Command: private-vlan association <secondary-vlan-list>

no private-vlan association

Function: Set Private VLAN association; the no command cancels Private VLAN association.

Parameter: ***<secondary-vlan-list>*** Sets Secondary VLAN list which is associated to Primary VLAN. There are two types of Secondary VLAN: Isolated VLAN and Community VLAN. Users can set multiple Secondary VLANs by ';'.

Command mode: VLAN Mode.

Default: There is no Private VLAN association by default.

Usage Guide: This command can only used for Private VLAN. The ports in Secondary VLANs which are associated to Primary VLAN can communicate to the ports in Primary VLAN.

Before setting Private VLAN association, three types of Private VLANs should have no member ports; the Private VLAN with Private VLAN association can't be deleted. When users delete Private VLAN association, all the member ports in the Private VLANs whose association is deleted are removed from the Private VLANs.

Example: Associate Isolated VLAN200 and Community VLAN300 to Primary VLAN100.

```
Switch(Config-Vlan100)#private-vlan association 200;300
```

3.13.15 private-vlan

Command: private-vlan {primary | isolated | community}

no private-vlan

Function: Configure current VLAN to Private VLAN. The no command cancels the Private VLAN configuration.

Parameter: primary set current VLAN to Primary VLAN, **isolated** set current VLAN to Isolated VLAN, **community** set current VLAN to Community VLAN.

Command Mode: VLAN mode

Default: Private VLAN is not configured by default.

Usage Guide: There are three Private VLANs: **Primary** VLAN, **Isolated** VLAN and **Community** VLAN. Ports in Primary there are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN can communicate with ports of Isolated VLAN and Community VLAN related to this Primary VLAN; Ports in Isolated VLAN are isolated between each other and only communicate with ports in Primary VLAN they related to; ports in Community VLAN can communicate both with each other and with Primary VLAN ports they related to; there is no communication between ports in Community VLAN and port in Isolated VLAN.

Only VLANs containing empty Ethernet ports can be set to Private VLAN, and only the Private VLANs configured with associated private relationships can set the Access Ethernet ports their member ports. Normal VLAN will clear its Ethernet ports when set to Private VLAN.

It is to be noted Private VLAN messages will not be transmitted by GVRP.

Example: Set VLAN100, 200, 300 to private vlans, with respectively primary, Isolated, Community types.

Switch(config)#vlan 100
Switch(Config-Vlan100)#private-vlan primary
Note:This will remove all the ports from vlan 100
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
Switch(Config-Vlan200)#private-vlan isolated
Note:This will remove all the ports from vlan 200
Switch(Config-Vlan200)#exit
Switch(config)#vlan 300
Switch(Config-Vlan300)#private-vlan community
Note:This will remove all the ports from vlan 300
Switch(Config-Vlan300)#exit

3.13.16 name

Command: name *<vlan-name>*

no name

Function: Specify a name, a descriptive string, for the VLAN; the no operation of the command will delete the name of the VLAN.

Parameters: <vlan-name> is the specified name string.

Command Mode: VLAN Configuration Mode.

Default: The default VLAN name is vlanXXX, where xxx is VID.

Usage Guide: The switch can specify names for different VLANs, making it easier for users to identify and manage VLANs.

Examples: Specify the name of VLAN100 as TestVlan.

Switch(Config-Vlan100)#name TestVlan

3.13.17 Vlan-flow-statistics

Command：vlan-flow-statistics

no vlan-flow-statistics

Function：Enable the statistics of the number of messages sent and received under VLAN, 'no' means disable this feature.

Parameters：None.

Command mode：VLAN Config Mode

Default：This feature is disabled by default

Usage Guide：None

Examples： Set VLAN 1 to enable VLAN based traffic statistics

Show int vlan before configuring **vlan-flow-statistics**

```
Switch#show int vlan 1
Vlan1 is up(0), line protocol is down, dev index is 11001
   Device flag 0x1002(BROADCAST MULTICAST)
   Time since last status change:0w-0d-0h-54m-59s    (3299 seconds)
   IPv4 address is:
      (NULL)
   VRF Bind: Not Bind
   Hardware is EtherSVI, address is 00-07-0a-0a-0a-1a
   MTU is 1500 bytes , BW is 0 Kbit
   Encapsulation ARPA, loopback not set
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
   The last 5 second input rate 0 bits/sec, 0 packets/sec
   The last 5 second output rate 0 bits/sec, 0 packets/sec
```

Show int vlan after configuring **vlan-flow-statistics**

```
Switch(config)#int vlan 1
Switch(config-if-vlan1)#vlan-flow-statistics
Switch(config-if-vlan1)#end
Switch#show interface vlan 1
Vlan1 is up(0), line protocol is down, dev index is 11001
   Device flag 0x1002(BROADCAST MULTICAST)
   Time since last status change:0w-0d-0h-55m-54s    (3354 seconds)
   IPv4 address is:
      (NULL)
   VRF Bind: Not Bind
   Hardware is EtherSVI, address is 00-07-0a-0a-0a-1a
   MTU is 1500 bytes , BW is 0 Kbit
   Encapsulation ARPA, loopback not set
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
   The last 5 second input rate 0 bits/sec, 0 packets/sec
   The last 5 second output rate 0 bits/sec, 0 packets/sec
   Input packets statistics:
      Input queue 0/1200, 0 drops
      0 packets input, 0 bytes, 0 no buffer
      0 unicast packets, 0 multicast packets, 0 broadcast packets
      0 input errors, 0 CRC, 0 oversize, 0 undersize
       0 jabber, 0 fragments
   Output packets statistics:
      0 packets output, 0 bytes, 0 underruns
```

0 unicast packets, 0 multicast packets, 0 broadcast packets
0 output errors, 0 collisions

3.14 GVRP

3.14.1 garp timer join

Command: garp timer join <200-500>
Function: Set the value of garp join timer, note that the value of join timer must be less than half leave timer.
Parameters: <200-500>, the value of timer in millisecond
Command Mode: Global mode
Default: 200 ms.
Usage Guide: Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error.
Example: Set the value of garp join timer as 200ms.
Switch(config)#garp timer join 200

3.14.2 garp timer leave

Command: garp timer leave <500-1200>
Function: Set the value of garp leave timer, note that the value of leave timer must be double of join timer and less than leaveAll timer.
Parameters: <500-1200>, the value of timer in millisecond
Command Mode: Global mode
Default: 600 ms.
Usage Guide: Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error.
Example: Set the value of garp leave timer as 600ms.
Switch(config)#garp timer leave 600

3.14.3 garp timer leaveAll

Command: garp timer leaveall <5000-60000>
Function: Set the value of garp leaveAll timer, note that the value of leaveAll timer must be larger than leave timer.
Parameters: <5000-60000>, the value of timer in millisecond
Command Mode: Global mode
Default: 10000 ms.
Usage Guide: Check whether the value satisfy the range. If so, modify the value of garp leaveAll timer to the specified value, otherwise return a configuration error.
Example: Set the value of garp leaveAll as 20000ms.

Switch(config)#garp timer leaveall 20000

3.14.4 gvrp (Global)

Command: gvrp

no gvrp

Function: Enable/disable GVRP funciton globally.

Parameters: None.

Command Mode: Global mode

Default: Disabled.

Usage Guide: Enable GVRP function globally and only in this way GVRP module can work normally.

Example: Enable GVRP function globally.

Switch(config)#gvrp

3.14.5 gvrp (Port)

Command: gvrp

no gvrp

Function: Enable/disable GVRP function on port. Notice: although GVRP can be enabled on port when GVRP is not enabled globally, it will not take effect until global GVRP is enabled.

Parameters: None

Command Mode: Port mode

Default: Disabled

Usage Guide: GVRP function can only be enabled on trunk and hybrid ports, and enabling GVRP will return an error on access port. After GVRP enabled on port, this port will be added to GVRP (i.e. adding corresponding state machine to GVRP of the port).

Example: Enable GVRP of port.

Switch(config-if-ethernet1/0/1)#gvrp

3.14.6 no garp timer

Command: no garp timer (join | leave | leaveall)

Function: Restore garp join | leave | leaveAll timer to the default value.

Parameters: join, join timer

leave, leave timer

leaveAll, leaveAll timer

Command Mode: Global mode

Default: 200 | 600 | 10000 milliseconds for join | leave | leaveall timer respectively.

Usage Guide: Check whether the default value satisfy the range. If so, modify the value of garp join | leave | leaveAll timer to the default value, otherwise return a configuration error.

Example: Restore garp timer to the default value.

Switch(config)#no garp timer leaveall

3.14.7 show garp timer

Command: show garp timer (join | leave | leaveall |)

Function: Show the value of each timer. Note that the value is not the remaining time to run the timer but the initial value when enabling the timer.

Parameters: join, join timer

leave, leave timer

leaveAll, leaveAll timer

Command Mode: Admin mode

Default: 200|600|10000 milliseconds for join | leave | leaveAll timer respectively.

Usage Guide: Show the corresponding value of the timer specified in the command.

Example: Show the value of all garp timers currently.

Switch#show garp timer join

Garp join timer's value is 200(ms)

3.14.8 show gvrp fsm information

Command: show gvrp fsm information interface (ethernet | port-channel) IFNAME

Function: Show the current state of all registered machines and request state machines on specified or all ports.

Parameters: ethernet, physical port

port-channel, aggregate port

IFNAME, port name

Command Mode: Admin mode

Default: MT for registered machine and VO for request state machine.

Usage Guide: Show the corresponding state of all registered machines and request state machines.

Example: Show the state of all state machines.

Switch#show gvrp fsm information interface ethernet 1/0/1

VA：Very anxious Active member，AA：Anxious Active member，QA：Quiet Active member

VP：Very anxious Passive member，AP：Anxious Passive member，QP：Quiet Passive member

VO：Very anxious Observer，AO：Anxious Observer，QO：Quiet Observer

LA：Leaving Acitve member，LO：leaving Observer

Interface ethernet 1/0/1 gvrp fsm information:

Index	VLANID	Applicant	Registrar
1	100	VO	LV
2	300	VP	IN

3.14.9 show gvrp leaveAll fsm information

Command: show gvrp leaveall fsm information interface (ethernet | port-channel) IFNAME

Function: Show the state of leaveAll state machine on specified or all ports.

Parameters: ethernet, physical port
port-channel, aggregate port
IFNAME, port name
Command Mode: Admin mode
Default: Passive.
Usage Guide: Check the state of leaveAll state machine.
Example: Show the state of leaveAll state machine on port.
Switch#show gvrp leaveall fsm information interface ethernet 1/0/1
Interface leaveAll fsm
---------- ----------
Ethernet1/0/1 passive

3.14.10 show gvrp leavetimer running information

Command: show gvrp leavetimer running information (vlan <1-4094> |) interface (Ethernet | port-channel |) IFNAME
Function: Show running of all leavetimer on current port.
Parameters: <1-4094>, VLAN tag
Ethernet, physical port
port-channel, aggregate port
IFNAME, port name
Command Mode: Admin mode
Default: leavetimer is disabled.
Usage Guide: Show running state and expiration time of each leave timer.
Example: Show running state and expiration time of each leave timer on current port.
Switch#show gvrp leavetimer running information interface ethernet 1/0/1
VLANID running state expired time
---------- ---------- ---------
100 UP 0.2 s
300 DOWN non

3.14.11 show gvrp port-member

Command: show gvrp (active|) port-member
Function: Shows all ports with GVRP enabled. “active” means the port is in active state with GVRP enabled.
Parameters: active means the port is in active state
Command Mode: Admin mode
Default: GVRP is disabled on port.
Usage Guide: Show all ports (enable GVRP) saved in GVRP.
Example: Show all ports with GVRP enabled.
Switch#show gvrp port-member
Ports which were enabled gvrp included：

Ethernet1/0/3（T） Ethernet1/0/4（T）
Ethernet1/0/5（T） Ethernet1/0/6（T）
Ethernet1/0/7（T） Ethernet1/0/8（T）
Ethernet1/0/9（T） Ethernet1/0/10（T）

3.14.12 show gvrp port registerd vlan

Command: show gvrp port (dynamic | static |) registerd vlan interface (Ethernet | port-channel |) IFNAME

Function: Show the dynamic or static registration VLANs on current port.

Parameters: dynamic, dynamic registration
static, static registration
Ethernet, physical port
port-channel, aggregate port
IFNAME, port name

Command Mode: Admin mode

Default: No dynamic or static registration VLANs on port.

Usage Guide: Show the corresponding VLANs of the registered machines by dynamic or static registration.

Example: Show all dynamic or static registration VLANs on current port.

Switch#show gvrp port registerd vlan interface ethernet 1/0/1
Current port dynamic registerd vlan included：
Vlan10 vlan20
Vlan40 vlan60
Current port static registerd vlan included：
Vlan10 vlan30
Vlan40 vlan200

3.14.13 show gvrp timer running information

Command: show gvrp timer (join | leaveall) running information interface (ethernet | port-channel |) IFNAME

Function: Show running of all join|leaveAll timer on current port.

Parameters: join, join timer
leaveall, leaveAll timer
ethernet, physical port
port-channel, aggregate port
IFNAME, port name

Command Mode: Admin mode

Default: Join timer is disabled and leaveAll timer is enabled.

Usage Guide: Check running state of join|leaveAll timer on port.

Example: Show running state and expiration time of each timer.

Switch(config)#show gvrp timer join running information interface ethernet 1/0/1

Current port's jointimer running state is: UP
Current port's jointimer expired time is: 0.2 s

3.14.14 show gvrp vlan registerd port

Command: show gvrp vlan <1-4094> registerd port
Function: Show the ports with specified VLAN registered.
Parameters: <1-4094>: VLAN tag
Command Mode: Admin mode
Default: No ports with specified VLAN registered.
Usage Guide: None.
Example: Show all ports with current VLAN registered.
Switch#show gvrp vlan 100 registerd port
Ethernet1/0/3（T） Ethernet1/0/4（T）
Ethernet1/0/5（T） Ethernet1/0/6（T）
Ethernet1/0/7（T） Ethernet1/0/8（T）
Ethernet1/0/9（T） Ethernet1/0/10（T）

3.14.15 debug gvrp event

Command: debug gvrp event interface (ethernet | port-channel |) IFNAME
no debug gvrp event interface (ethernet | port-channel |) IFNAME
Function: Enable/disable GVRP event debugging including the transfer of state machine and the expiration of timer.
Parameters: ethernet, physical port
port-channel, aggregate port
IFNAME, port name
Command Mode: Admin mode
Default: GVRP event debugging is disabled.
Usage Guide: Use this command to enable GVRP event debugging.
Example: Show GVRP event debugging.
Switch#debug gvrp event interface ethernet 1/0/1
%Jan 16 02:25:14 2006 GVRP EVENT: LO -> VO ， interface ethernet 1/0/1, vlan 100
%Jan 16 02:35:15 2006 GVRP EVENT: join timer expire， interface ethernet 1/0/1

3.14.16 debug gvrp packet

Command: debug gvrp packet (receive | send) interface (ethernet | port-channel |) IFNAME
no debug gvrp packet (receive | send) interface (ethernet | port-channel |) IFNAME
Function: Enable/disable GVRP packet debugging.
Parameters: receive, enabling the debugging of receiving GVRP packet
send, enabling the debugging of sending GVRP packet

ethernet, physical port
port-channel, aggregate port
IFNAME, port name

Command Mode: Admin mode

Default: GVRP packet debugging is disabled.

Usage Guide: Use this command to enable the debugging of GVRP packet.

Example: Show information of sending and receiving GVRP packet.

```
Switch#debug gvrp packet receive interface ethernet 1/0/1
Receive packet, smac 00-21-27-aa-0f-46, dmac 01-80-C2-00-00-21,
    length 90, protocol ID:1,attribute type:0x01,
    Attribute Index     Length      Event       Value
    ------------------  ---------   -------     -------
        1                   10          joinIn          100
        2                   10          joinEmpty       140
        3                   10          leaveIn         150
        4                   10          leaveEmpty      180
```

3.15 Dot1q-tunnel

3.15.1 dot1q-tunnel enable

Command: dot1q-tunnel enable
no dot1q-tunnel enable

Function: Set the access port of the switch to dot1q-tunnel mode; the no command restores to default.

Parameter: None.

Command Mode: Port Mode.

Default: Dot1q-tunnel function disabled on the port by default.

Usage Guide: After enabling dot1q-tunnel on the port, data packets without VLAN tag (referred to as tag) will be packed with a tag when entering through the port; those with tag will be packed with an external tag. The TPID in the tag is 8100 and the VLAN ID is the VLAN ID that the port belongs to. Data packets with double tags will be forwarded according to MAC address and external tag, till the external tag is removed when transmitted outside from the access port. Since the length of the data packet may be over sized when packed with external tag, it is recommended to use this command associating the Jumbo function. Normally this command is used on access ports. This command and dot1q-tunnel tpid are mutually exclusive, also and vlan-translation enable.

Example: Join port1 into VLAN3, enable dot1q-tunnel function.

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/0/1
Switch(Config-Vlan3)#exit
```

Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel enable
Switch(Config-If-Ethernet1/0/1)# exit
Switch(config)#

3.15.2 dot1q-tunnel tpid

Command: dot1q-tunnel tpid {0x8100|0x9100|0x9200| *<1-65535>* }
Function: Configure the type (TPID) of the protocol of switch trunk port.
Parameter: None.
Command Mode: Port Mode.
Default: TPID on the port is defaulted at 0x8100.
Usage Guide: This function is to facilitate internetworking with equipments of other manufacturers. If the equipment connected with the switch trunk port sends data packet with a TPID of 0x9100, the port TPID will be set to 0x9100, this way switch will receive and process data packets normally. This command and dot1q-tunnel enable are mutually exclusive.
Example: Set port 10 of the switch to trunk port and sends data packet with a TPID of 0x9100.
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode trunk
Switch(Config-If-Ethernet1/0/10)#dot1q-tunnel tpid 0x9100
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#

3.15.3 show dot1q-tunnel

Command: show dot1q-tunnel
Function: Display the information of all the ports at dot1q-tunnel state.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: This command is used for displaying the information of the ports at dot1q-tunnel state.
Example: Display current dot1q-tunnel state.
Switch#show dot1q-tunnel
Interface Ethernet1/0/1:
dot1q-tunnel is enable
Interface Ethernet1/0/3:
dot1q-tunnel is enable

3.16 VLAN translation

3.16.1 vlan-translation

Command: vlan-translation <old-vlan-id> to <new-vlan-id>{in | out}

no vlan-translation <old-vlan-id>{in | out}

Function: Add VLAN translation by creating a mapping between original VLAN ID and current VLAN ID; the no form of this command deletes corresponding mapping.

Parameter: old-vlan-id is the original VLAN ID; new-vlan-id is the translated VLAN ID; in indicates ingress translation; out indicates egress translation.

Command Mode: Port Mode.

Default: There is no VLAN translation relation.

Usage Guide: The command is for configuring the in and out translation relation of the VLAN translation function. The data packets will be matched according to the configured translation relations, and its VLAN ID will be changed to the one in the configured item once matched, while the vlan-translation miss drop command will determine the next forwarding if not match.

The access ports of the switch can not support this function.

Example: Move the VLAN100 data entered from the port1 to VLAN2 after ingress translation.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#vlan-translation enable
Switch(Config-If-Ethernet1/0/1)#vlan-translation 100 to 2 in
Switch(Config-If-Ethernet1/0/1)#exit
Switch(config)#
```

3.16.2 vlan-translation enable

Command: vlan-translation enable

no vlan-translation enable

Function: Enable VLAN translation on the port; the no command restores to the default value.

Parameter: None.

Command Mode: Port Mode.

Default: VLAN translation has not been enabled on the port by default.

Usage Guide: This command and dot1q-tunnel are mutually exclusive.

The access ports of the switch can not support this function.

Example: Enable VLAN translation function on port1.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#vlan-translation enable
```

3.16.3 vlan-translation cvid

Command: vlan-translation cvid < 1-4094> svid <1-4094> {pri < 0-7>}

no vlan-translation cvid < 1-4094> svid <1-4094>

Function: Add VLAN translation by creating a mapping between client and service VLAN ID; the no form of this command deletes corresponding mapping.

Parameter:

<1-4094>: VLAN ID.

<0-7>: packet priority after vlan translation.

Command Mode: Port Mode.

Default: VLAN translation has not been enabled on the port by default.

Usage Guide: The command is for configuring the in and out translation relation of the VLAN translation function. The data packets will be matched according to the configured translation relations, and for ingress traffic, its VLAN ID will be changed to the svid in the configured item once matched the cvid, and for egress traffic, its VLAN ID will be changed to the cvid in the configured item once matched the svid, while the vlan-translation miss drop command will determine the next forwarding if not match.

The access ports of the switch can not support this function.

Example: Move the VLAN100 data entered from the port1 to VLAN200 after ingress translation; Move the VLAN200 data entered from the port1 to VLAN100 after egress translation.

Switch#config

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#vlan-translation enable

Switch(Config-If-Ethernet1/1/1)# vlan-translation cvid 100 svid 200

Switch**(**Config-If-Ethernet1/1/1)#exit

Switch(config)#

3.16.4 vlan-translation miss drop

Command: vlan-translation miss drop in

no vlan-translation miss drop in

Function: Set packet dropping when checking vlan-translation is failing; the no command restores to the default value.

Parameter: In refers to ingress.

Command Mode: Port Mode.

Default: Do not drop the packets when checking vlan-translation is failing.

Usage Guide: When performing the mapping translation between the original and the current VID, if no corresponding translation is configured, the packet will not be dropped by default, but checking failure will drop the tag message after use this command, this command is of no effect for untag message.

The access ports of the switch can not support this function.

Example: Set ingress packet dropped on port1 when translation failure.

Switch(Config-If-Ethernet1/0/1)#vlan-translation miss drop in

3.16.5 show vlan-translation

Command: show vlan-translation
Function: Show the related configuration of vlan-translation.
Parameter: None.
Command mode: Admin mode.
Usage Guide: Show the related configuration of vlan-translation.
The access ports of the switch can not support this function.
Example: Show the related configuration of vlan-translation.
Switch#show vlan-translation
Interface Ethernet1/0/1:
vlan-translation is enable, miss drop is not set
vlan-translation 5 to 10 in

3.17 Dynamic VLAN

3.17.1 dynamic-vlan mac-vlan prefer

Command: dynamic-vlan mac-vlan prefer
Function: Set the MAC-based VLAN preferred.
Parameter: None.
Command Mode: Global Mode.
Default: MAC-based VLAN is preferred by default.
Usage Guide: Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. After the IP-subnet-based VLAN is set to be preferred and the user wish to restore to preferring the MAC-based VLAN, please use this command.
Example: Set the MAC-based VLAN preferred.
Switch#config
Switch(config)#dynamic-vlan mac-vlan prefer

3.17.2 dynamic-vlan subnet-vlan prefer

Command: dynamic-vlan subnet-vlan prefer

Function: Set the IP-subnet-based VLAN preferred.
Parameter: None.
Command Mode: Global Mode.
Default: MAC-based VLAN is preferred by default.
Usage Guide: Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. This command is used to set to preferring the IP-subnet-based VLAN.
Example: Set the IP-subnet-based VLAN preferred.
Switch#config
Switch(config)#dynamic-vlan subnet-vlan prefer

3.17.3 mac-vlan

Command: mac-vlan mac <mac-addrss> <mac-mask> vlan <vlan-id> priority <priority-id>
no mac-vlan {mac <mac-addrss> <mac-mask>|all}
Function: Add the correspondence between MAC address and VLAN, it means to make the specified MAC address join the specified VLAN. The no form of this command deletes all/the correspondence.
Parameter: mac-address is the MAC address which is shown in the form of XX-XX-XX-XX-XX-XX, mac-mask is the MAC address mask which is shown in the form of 为 XX-XX-XX-XX-XX-XX, vlan-id is the ID of the VLAN with a valid range of 1~4094; priority-id is the level of priority and is used in the VLAN tag with a valid range of 0~7; all refers to all the MAC addresses.
Command Mode: Global Mode.
Default: No MAC address joins the VLAN by default.
Usage Guide: With this command user can add specified MAC address to specified VLAN. If there is a non VLAN label data packet enters from the switch port from the specified MAC address, it will be assigned with specified VLAN ID so sent enter specified VLAN. Their belonging VLAN are the same no matter which port did they enter through. The command does not have any interfere on the VLAN label data packet.
Example: Add network device of MAC address as 00-03-0f-11-22-33 to VLAN 100.
Switch#config
Switch(config)#mac-vlan mac 00-03-0f-11-22-33 ff-ff-ff-ff-ff-ff vlan 100 priority 0

3.17.4 mac-vlan vlan

Command: mac-vlan vlan *<vlan-id>*
no mac-vlan vlan *<vlan-id>*
Function: Configure the specified VLAN to MAC VLAN; the "**no mac-vlan vlan *<vlan-id>***" command cancels the MAC VLAN configuration of this VLAN.
Parameter: *<vlan-id>* is the number of the specified VLAN.
Command Mode: Global Mode.
Default: No MAC VLAN is configured by default.

Usage Guide: Set specified VLAN for MAC VLAN.
Example: Set VLAN100 to MAC VLAN.
Switch#config
Switch(config)#mac-vlan vlan 100

3.17.5 protocol-vlan

Command: protocol-vlan mode {ethernetii etype *<etype-id>* | llc {dsap *<dsap-id>* ssap *<ssap-id>*} | snap etype *<etype-id>*} vlan *<vlan-id>* priority *<priority-id>*

no protocol-vlan {mode *{ethernetii* etype *<etype-id>* | llc {dsap *<dsap-id>* ssap *<ssap-id>*} | snap etype *<etype-id>*} | all}

Function: Add the correspondence between the protocol and the VLAN namely specify the protocol to join specified VLAN. The no form of this command deletes all/the correspondence.
Parameter: mode is the encapsulate type of the configuration which is ethernetii, llc, snap; the encapsulate **type** of the ethernetii is EthernetII; **etype-id** is the type of the packet protocol, with a valid range of 1536~65535; **llc** is LLC encapsulate format; **dsap-id** is the access point of the destination service, the valid range is 0~255; **ssap-id** is the access point of the source service with a valid range of 0~255; **snap** is SNAP encapsulate format; **etype-id** is the type of the packet protocol, the valid range is 1536~65535; **vlan-id** is the ID of VLAN, the valid range is 1~4094; **priority** is the priority, the range is 0~7; **all** indicates all the encapsulate protocols.
Command Mode: Global Mode.
Default: No protocol joined the VLAN by default.
Usage Guide: The command adds specified protocol into specified VLAN. If there is any non VLAN label packet from specified protocol enters through the switch port, it will be assigned with specified VLAN ID and enter the specified VLAN. No matter which port the packets go through, their belonging VLAN is the same. The command will not interfere with VLAN labeled data packets. It is recommended to configure ARP protocol together with the IP protocol or else some application may be affected.
Example: Assign the IP protocol data packet encapsulated by the EthernetII to VLAN200.
Switch#config
Switch(config)#protocol-vlan mode ethernetii etype 2048 vlan 200

3.17.6 show dynamic-vlan prefer

Command: show dynamic-vlan prefer
Function: Display the preference of the dynamic VLAN.
Parameter: None.
Command Mode: Admin Mode and Configuration Mode.
Usage Guide: Display the dynamic VLAN preference.

Example: Display current dynamic VLAN preference.
Switch#show dynamic-vlan prefer
Mac Vlan/Voice Vlan
IP Subnet Vlan

Protocol Vlan

3.17.7 show mac-vlan

Command: show mac-vlan

Function: Display the configuration of MAC-based VLAN on the switch.

Parameter: None.

Command Mode: Admin Mode and other configuration Mode.

Usage Guide: Display the configuration of MAC-based VLAN on the switch.

Example: Display the configuration of the current MAC-based VLAN.

```
Switch#show mac-vlan
MAC-Address                    VLAN_ID    Priority
------------------              -----------   --------
00-e0-4c-77-ab-9d                 2            2
00-0a-eb-26-8d-f3                 2            2
00-03-0f-11-22-33                 5            5
```

3.17.8 show mac-vlan interface

Command: show mac-vlan interface

Function: Display the ports at MAC-based VLAN.

Parameter: None.

Command Mode: Admin Mode and other configuration Mode.

Usage Guide: Display the ports of enabling MAC-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.

Example: Display the ports of enabling MAC-based VLAN currently.

```
Switch#show mac-vlan interface
Ethernet1/0/1(A)        Ethernet1/0/2(A)
Ethernet1/0/3(A)        Ethernet1/0/4(A)
Ethernet1/0/5(H)        Ethernet1/0/6(T)
```

3.17.9 show protocol-vlan

Command: show portocol-vlan

Function: Display the configuration of Protocol-based VLAN on the switch.

Parameter: None.

Command Mode: Admin Mode and Configuration Mode

Usage Guide: Display the configuration of Protocol-based VLAN on the switch.

Example: Display the configuration of the current Protocol-based VLAN.

```
Switch#show protocol-vlan
Protocol_Type                  VLAN_ID          Priority
-------------------              -------------     ---------
mode ethernetii etype 0x800        200              4
```

mode ethernetii etype 0x860	200	4
mode snap etype 0xabc	100	5
mode llc dsap 0xac ssap 0xbd	100	5

3.17.10 show subnet-vlan

Command: show subnet-vlan

Function: Display the configuration of the IP-subnet-based VLAN on the switch.

Parameter: None.

Command Mode: Admin Mode and other Configuration Mode.

Usage Guide: Display the configuration of the IP-subnet-based VLAN on the switch.

Example: Display the configuration of the current IP-subnet-based VLAN.

```
Switch#show subnet-vlan
IP-Address          Mask            VLAN_ID
------------------  -------          -------
192.168.1.165       255.255.255.0     2
202.200.121.21      255.255.0.0       2
10.0.0.1             255.248.0.0       5
```

3.17.11 show subnet-vlan interface

Command: show subnet-vlan interface

Function: Display the port at IP-subnet-based VLAN.

Parameter: None.

Command Mode: Admin Mode and other Configuration Mode.

Usage Guide: Display the port of enabling IP-subnet-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.

Example: Display the port of enabling IP-subnet-based VLAN currently.

```
Switch#show subnet-vlan interface
Ethernet1/0/1(A)        Ethernet1/0/2(A)
Ethernet1/0/3(A)        Ethernet1/0/4(A)
Ethernet1/0/5(H)        Ethernet1/0/6(T)
```

3.17.12 subnet-vlan

Command: subnet-vlan ip-address <ipv4-addrss> mask <subnet-mask> vlan *<vlan-id>* priority *<priority-id>*

no subnet-vlan {ip-address *<ipv4-addrss>* mask *<subnet-mask>* | all}

Function: Add a correspondence between the IP subnet and the VLAN, namely add specified IP subnet into specified VLAN; the no form of this command deletes all/the correspondence.

Parameter: ipv4-address is the IPv4 address shown in dotted decimal notation; the valid range of each section is 0~255; subnet-mask is the subnet mask code shown in dotted decimal notation; the valid range of each section is 0~255; priority-id is the priority applied in the VLAN tag with a

valid range of 0~7; vlan-id is the VLAN ID with a valid range of 1~4094;all indicates all the subnets.

Command Mode: Global Mode.

Default: No IP subnet joined the VLAN by default.

Usage Guide: This command is used for adding specified IP subnet to specified VLAN. When packet without VLAN label and from the specified IP subnet enters through the switch port, it will be matched with specified VLAN id and enters specified VLAN. These packets will always come to the same VLAN no matter through which port did they enter. This command will not interfere with VLAN labeled data packets.

Example: Add the network equipment with IP subnet of 192.168.1.0/24 to VLAN 300.

Switch#config

Switch(config)#subnet-vlan ip-address 192.168.1.1 mask 255.255.255.0 vlan 300 priority 0

3.17.13 switchport mac-vlan enable

Command: switchport mac-vlan enable

no switchport mac-vlan enable

Function: Enable the MAC-based VLAN function on the port; the no form of this command will disable the MAC-based VLAN function on the port.

Parameter: None.

Command Mode: Port Mode.

Default: The MAC-base VLAN function is enabled on the port by default.

Usage Guide: After adding a MAC address to specified VLAN, the MAC-based VLAN function will be globally enabled. This command can disable the MAC-based VLAN function on specified port to meet special user applications.

Example: Disable the MAC-based VLAN function on port1.

Switch#config

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#no switchport mac-vlan enable

3.17.14 switchport subnet-vlan enable

Command: switchport subnet-vlan enable

no switchport subnet-vlan enable

Function: Enable the IP-subnet-based VLAN on the port; the no form of this command disables the IP-subnet-based VLAN function on the port.

Parameter: None.

Command Mode: Port Mode.

Default: The IP-subnet-based VLAN is enabled on the port by default.

Usage Guide: After adding the IP subnet to specified VLAN, the IP-subnet-based VLAN function will be globally enabled. This command can disable the IP-subnet-based VLAN function on specified port to meet special user applications.

Example: Disable the IP-subnet-based VLAN function on port1.

Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#no switchport subnet-vlan enable

3.18 Voice VLAN

3.18.1 show voice-vlan

Command: show voice-vlan
Function: Display the configuration status of the Voice VLAN on the switch.
Parameter: None.
Command Mode: Admin Mode and other Configuration Mode.
Usage Guide: Display Voice VLAN Configuration.
Example: Display the Current Voice VLAN Configuration.
Switch#show voice-vlan
Voice VLAN ID:2
Ports:ethernet1/0/1;ethernet1/0/3

Voice name	MAC-Address	Mask	Priority
financePhone	00-e0-4c-77-ab-9d	0xff	5
manager	00-0a-eb-26-8d-f3	0xfe	6
Mr_Lee	00-03-0f-11-22-33	0x80	5
NULL	00-03-0f-11-22-33	0x0	5

3.18.2 switchport voice-vlan enable

Command: switchport voice-vlan enable
no switchport voice-vlan enable
Function: Enable the Voice VLAN function on the port; the “no” form of this command disables Voice VLAN function on the port.
Parameter: None.
Command Mode: Port Mode.
Default: Voice VLAN is enabled by default.
Usage Guide: When voice equipment is added to the Voice VLAN, the Voice VLAN is enabled globally by default. This command disables Voice VLAN on specified port to meet specified application of the user.
Example: Disable the Voice VLAN function on port3.
Switch#config
Switch(config)#interface ethernet1/0/3
switch(Config-If-Ethernet1/0/3)#no switchport voice-vlan enable

3.18.3 voice-vlan

xx-xx-xx-xx-xx-xx

3.18.4 voice-vlan vlan

Command: voice-vlan vlan <*vlan-id*>

no voice-vlan

Function: Configure the specified VLAN to Voice VLAN; the "**no voice-vlan**" command cancels the Voice VLAN configuration of this VLAN.

Parameter: Vlan id is the number of the specified VLAN.

Command Mode: Global Mode.

Default: No Voice VLAN is configured by default.

Usage Guide: Set specified VLAN for Voice VLAN, There can be only one Voice VLAN at the same time. The voice VLAN can not be applied concurrently with MAC-based VLAN.

Example: Set VLAN100 to Voice VLAN.

Switch#config

Switch(config)#voice-vlan vlan 100

3.19 Multi-to-One VLAN Translation

3.19.1 vlan-translation n-to-1

Command: vlan-translation n-to-1 *<WORD>* to *<new-vlan-id>*

no vlan-translation n-to-1 *<WORD>*

Function: Enable/disable Multi-to-One VLAN translation of the port.

Parameters: WORD is the original VLAN ID, its range from 1 to 4094, connect them with ';' and '-'. If there are two VLANs with different range are translated into different VLAN ID in the same port, two VLAN ranges should not be superposed.

new-vlan-id is the translated VLAN ID, its range from 1 to 4094.

Command Mode: Port mode

Default: Disable

Usage Guide: Multi-to-One VLAN translation is used to network edge to map multiple VLANs to one VLAN of backbone network. When data traffic returns from backbone network to network edge, it will restore VLAN of network edge to implement Multi-to-One VLAN translation and save VLAN resource of backbone network. Note: When using this function, the device must establish the original and the translated VLAN firstly, and enabling the downlink port of this function and the uplink port for connecting backbone network, which must be join in the original and the translated VLAN with tagged mode. This function should not be used with dot1q-tunnel and VLAN translation at the same time

Note: Multi-to-One VLAN translation should be enabled after MAC learning.

The access ports of the switch can not support this function.

Example: On Ethernet 1/0/1, translate the data traffic from VLAN with the range between 1 to 5 into VLAN 100, and translate the data traffic (belongs to VLAN with the range between 1 to 5) out from VLAN100 into the corresponding VLAN ID, connect the uplink port of the backbone network as Ethernet 1/0/5.

Switch(config)#vlan 1-5;100
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# switchport mode trunk
Switch(Config-If-Ethernet1/0/1)# vlan-translation n-to-1 1-5 to 100
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)# switchport mode trunk

3.19.2 show vlan-translation n-to-1

Command: show vlan-translation n-to-1 [<*interface-name*>]
Function: Show the port configuration with Multi-to-One VLAN translation.
Parameter: interface-name: Specify the name of the port which will be shown. If there is no parameter, show all port configurations with this function.
Command Mode: Admin mode.
Default: There is no Multi-to-One VLAN translation information.
Usage Guide: show

The access ports of the switch can not support this function.**Example:** Show all port configurations with Multi-to-One VLAN translation function.

Switch# show vlan-translation n-to-1
Interface Ethernet1/0/1:
vlan-translation n-to-1 enable, vlan 1-4 to 100
vlan-translation n-to-1 enable,vlan 5-8;13 to 101
Interface Ethernet1/0/2:
vlan-translation n-to-1 enable,vlan 1-4 to 100

3.20 Super VLAN

3.20.1 supervlan

Command: supervlan
no supervlan
Function: Set VLAN as super vlan, the no command restores the default configuration.
Parameter: None.
Command Mode: VLAN Configuration Mode.
Default: No configuration.
Usage Guide: Set VLAN (except SUB VLAN) as super vlan. Super vlan will be filtered automatically when setting trunk port and any port can not belong to it.

Example: Set vlan2 as supervlan.
Swithc#config
Switch(config)#vlan 2
Switch (config-vlan2)#supervlan

3.20.2 subvlan

Command: subvlan WORD
no subvlan {WORD | all}
Function: Set VLAN as subvlan, the no command restores the default configuration.
Parameter: WORD: VLAN ID, use "-" and ";" to connect VLANs.
all: all subvlans.
Command Mode: VLAN Configuration Mode.
Default: No configuration.
Usage Guide: Set VLAN (it must exist and must be common VLAN, at the same time, it should not be sub vlan of other super vlan and should not be super vlan) as sub vlan. Each super vlan can establish mapping relation with 127 Sub VLANs, and switch can set 1024 Super VLANs at most.
Example: Set vlan3 as subvlan.
Swithc#config
Switch(config)#vlan 2-3
Switch(config)#vlan 2
Switch (config-vlan2)#supervlan
Switch (config-vlan2)#subvlan 3

3.20.3 arp-proxy subvlan

Command: arp-proxy subvlan {WORD | all}
no arp-proxy subvlan {WORD | all}
Function: Enable arp proxy function of subvlan, the flow received by this VLAN can be forwarded to other subvlan. The no command restores the default configuration.
Parameter: WORD: VLAN ID, use "-" and ";" to connect VLANs.
all: all subvlans.
Command Mode: Interface Configuration Mode.
Default: No Configuration.
Usage Guide: Interface of VLAN must be supervlan's interface, the flow received by this VLAN can be forwarded to other subvlan. When switch receives ARP REQUEST from this VLAN, it uses its MAC to reply ARP REPLY, so as to forward flows by switch.
Example: Enable arp-proxy function of all subvlans on vlan2.
Swithc#config
Switch(config)#interface vlan 2
Switch (config-if-vlan2)#arp-proxy subvlan all

3.20.4 ip-addr-range subvlan

Command: ip-addr-range subvlan *<vlan-id>* *<ipv4-address>* to *<ipv4-address>*

no ip-addr-range subvlan *<vlan-id>*

Function: Configure the specified address range for a subvlan. After switch received flows, it needs to check whether destination IP address of package is within the address range when sending ARP REQUEST. If not, switch will not send ARP REQUEST. The no command restores the default configuration.

Parameter: *<vlan-id>*: VLAN ID, its range between 1 and 4094.

***<ipv4-address>*:** IPv4 address in dotted decimal notation, the value range from 0 to 255.

Command Mode: Interface Configuration Mode.

Default: No address range.

Usage Guide: After switch received flows from sub vlan with address range, it needs to check whether destination IP address of package is within the address range when sending ARP REQUEST. If not, switch will not send ARP REQUEST.

Example: Set address range of subvlan3.

Swithc#config

Switch(config)#interface vlan 2

Switch (config-if-vlan2)#ip-addr-range subvlan 3 1.1.1.1 to 1.1.1.10

3.20.5 ip-addr-range

Command: ip-addr-range *<ipv4-address>* to *<ipv4-address>*

no ip-addr-range

Function: Configure the specified address range for an interface. After switch received flows, it needs to check whether the destination IP address of package is within the address range when sending ARP REQUEST. If not, switch will not send ARP REQUEST. The no command restores the default configuration.

Parameter: *<ipv4-address>*: IPv4 address in dotted decimal notation, the value range from 0 to 255.

Command Mode: Interface Configuration Mode.

Default: No address range.

Usage Guide: After switch received flows from the interface with the address range, it needs to check whether the destination IP address of package is within the address range when sending ARP REQUEST. If not, switch will not send ARP REQUEST. If the interface is supervlan's interface, but the requested IP address is not within the address range when this interface received ARP REQUEST, it will not forward this ARP REQUEST.

Example: Set address range for interface vlan2.

Swithc#config

Switch(config)#interface vlan 2

Switch (config-if-vlan2)#ip-addr-range 1.1.1.1 to 1.1.1.10

3.20.6 show supervlan

Command: show supervlan [<*vlan-id*>]

Function: Show super vlan configuration.

Parameter: <*vlan-id*>: VLAN ID, its range between 1 and 4094.

Command Mode: Admin Mode.

Usage Guide: Show all supervlan configurations if VLAN ID is not specified.

Example: Show the current supervlan configuration.

```
Swithc#show supervlan
VLAN Name            Type          sub VLAN    Ports
---- ------------ ---------- --------- ----------------------------------------
2      VLAN0002        Universal     3        Ethernet1/0/2
                                        4        Ethernet1/0/3
```

3.21 MAC Address Table

3.21.1 mac-address-table avoid-collision

This command is not supported by switch.

3.21.2 clear collision-mac-address-table

Command：clear collision-mac-address-table

Function： Clear the hash collision mac table.

Parameter： None.

Command mode： Admin Mode.

Usage Guide： If enable the function of the hash collision mac table that issued ffp (**mac-address-table avoid-collision**), the mac cannot be cleared.

Example： Clear the hash collision mac table.

```
Switch#clear collision-mac-address-table
```

3.21.3 clear mac-address-table dynamic

Command: clear mac-address-table dynamic [address <*mac-addr*>] [vlan <*vlan-id*>] [interface [ethernet | portchannel] <*interface-name*>]

Function: Clear the dynamic address table.

Parameter: <*mac-addr*>: MAC address will be deleted; ***<interface-name>*** the port name for forwarding the MAC packets; ***<vlan-id>*** VLAN ID.

Command mode: Admin mode.

Usage Guide: Delete all dynamic address entries which exist in MAC address table, except application, system entries. MAC address entries can be classified according to different sources, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC

address entries learned by switch, it can be aged by switch automatically.
Example: Delete all dynamic MAC.
Switch#clear mac-address-table dynamic

3.21.4 mac-address-learning cpu-control

Command: mac-address-learning cpu-control
no mac-address-learning cpu-control
Function: Enable MAC learning through CPU control, the no command restores that the chip automatically learn MAC address.
Parameter: None.
Command Mode: Global mode.
Default: Chip automatically learn MAC address.
Usage Guide: If enable port-security, private-vlan, mac-notification, mac-limit, etc., it should enable MAC learning through CPU first.
Example: Enable MAC learning through CPU.
Switch(Config)#mac-address-learning cpu-control

3.21.5 mac-address-table aging-time

Command: mac-address-table aging-time <*0 | aging-time*>
no mac-address-table aging-time
Function: Sets the aging-time for the dynamic entries of MAC address table.
Parameter: ***<aging-time>*** is the aging-time seconds, range from 10 to 1000000; **0** to disable aging.
Command Mode: Global Mode.
Default: Default aging-time is 300 seconds.
Usage Guide: If no destination address of the packets is same with the address entry in aging-time, the address entry will get aged. The user had better set the aging-time according to the network condition, it usually use the default value.
Example: Set the aging-time to 600 seconds.
Switch(config)#mac-address-table aging-time 600

3.21.6 mac-address-table static | static-multicast | blackhole

Command: mac-address-table {static | static-multicast | *blackhole}* address <*mac-addr*> vlan <vlan-id**> *[interface* [ethernet | portchannel] <interface-name>] | [source | destination | both]**
no mac-address-table {static | static-multicast | blackhole | dynamic} *[address* <mac-addr>] *[vlan* <vlan-id>] [*interface [*ethernet | portchannel] *<interface-name>*]
Function: Add or modify static address entries, static multicast *entries* and filter

address *entries.* The no command *deletes* the three entries.

Parameter*: static is the *static* entries**; **static-multicast** is the static multicast entries; blackhole is filter entries, which is for discarding frames from specific MAC address, it can filter source address, destination address or the both. When choose the filter entries, blackhole address can't based on port**,** and not configure to interface; dynamic*** is dynamic address entries; <mac-addr> MAC ***address to*** be added or deleted; <interface-name> name of the ***port transmitting*** the MAC data packet; **<vlan-id>** is the vlan number. source **is** based on source address filter; destination **is** based on destination address filter; both is based on source address and destination address filter, the default is both.**Command Mode:** Global Mode

Default: When VLAN interface is configured and is up, the system will generate a static address mapping entry of which the inherent MAC address corresponds to the VLAN number.

Usage Guide: In certain special applications or when the switch is unable to dynamically learn the MAC address, users can use this command to manually establish mapping relation between the MAC address and port and VLAN.

no mac-address-table command is for deleting all dynamic, static, filter MAC address entries existing in the switch MAC address list, except application, system entries. MAC address entries can be classified according to the different source, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically. STATIC is the static MAC address entries (including blackhole entries) added by user. APPLICATION is the static MAC address entries added by application protocol (such as dot1x, security port…). SYSTEM is the additive static MAC address entries according to VLAN interface. When adding STATIC entries, it can cover the conflictive DYNAMIC, except APPLICATION, SYSTEM entries.

After configure the static multicast MAC by this command, the multicast MAC traffic will be forwarded to the specified port of the specified VLAN.

Example: Port 1/0/1 belongs to VLAN200, and establishes address mapping with MAC address 00-03-0f-f0-00-18.

Switch(config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 1/0/1

Configure a static multicast MAC 01-00-5e-00-00-01, the egress is ehernet 1/0/1.

Switch(config)#mac-address-table static-multicast address 01-00-5e-00-00-01 vlan 1 interface ethernet1/0/1

3.21.7 l2-address-table static-multicast address

This command is not supported by the switch.

3.21.8 show collision-mac-address-table

Command：show collision-mac-address-table

Function： Show the hash collision mac table.

Parameter： None.

Command mode： Global Mode.

Usage Guide： If enable the function of the hash collision mac table that issued ffp (**mac-address-table avoid-collision**), the collision mac which issued ffp use * to sign.

Example： Show the hash collision mac table.

Switch(Config)#show collision-mac-address-table

The max number can be recorded is 200

The max number of collision is 0

The current number recorded is 0

MAC Address VLAN Collision-count

3.21.9 show mac-address-table

Command: show mac-address-table [static | blackhole | multicast | aging-time <*aging-time*> | count] [address <*mac-addr*>] [vlan <vlan-id>] [count] [interface <interface-name>]

Function: Show the current MAC table.

Parameter: static static entries; blackhole filter entries; **aging-time <*aging-time*>** address aging time; **count** entry's number, ***multicast multicast*** entries; <mac-addr> ***entry's MAC*** address; <vlan-id> ***entry's VLAN*** number; <interface-name> entry's interface name.**Command mode:** Admin and Configuration Mode.

Default: MAC address table is not displayed by default.

Usage guide: This command can display various classes of MAC address entries. Users can also use **show mac-address-table** to display all the MAC address entries.

Example: Display all the filter MAC address entries.

Switch#show mac-address-table blackhole

3.21.10 Show l2-address-table multicast

This command is not supported by the switch.

3.22 MAC Notification

3.22.1 clear mac-notification statistics

Command: clear mac-notification statistics

Function: Clear the statistics of MAC notification trap.

Parameter: None.

Default: None.

Command Mode: Admin mode

Usage Guide: When this command is used with show command, it is able to check the executive result by show command after executing this command.

Example:

Switch# clear mac-notification statistics

3.22.2 mac-address-table notification

Command: mac-address-table notification

no mac-address-table notification

Function: Enable the MAC address notification globally, the no command disables the global MAC address notification.

Parameter: None.

Default: Disable.

Command Mode: Global mode

Usage Guide: This command is used with trap switch of snmp. When disabling the MAC address notification, other configuration can be shown, but the function is invalid.

Example: Enable the MAC address notification.

Switch(Config)#mac-address-table notification

3.22.3 mac-address-table notification history-size

Command: mac-address-table notification history-size <0-500>

no mac-address-table notification history-size

Function: Configure the maximum history-size for storing MAC changing message, the no command restores the default value.

Parameter: history-size: data length of sending the notification, its range from 1 to 500.

Default: 10.

Command Mode: Global mode

Usage Guide: After the global switch is disabled, this command is also able to be configured sequentially.

Example: Change the maximum history-size to be 256.

Switch(Config)#mac-address-table notification history-size 256

3.22.4 mac-address-table notification interval

Command: mac-address-table notification interval <0-86400>

no mac-address-table notification interval

Function: Configure the interval for sending the MAC address notification, the no command restores the default interval.

Parameter: interval: interval for sending the notification, unit is second, its range from 0 to 86400.

Default: 30s.

Command Mode: Global mode

Usage Guide: After the global switch is disabled, this command is also able to be configured sequentially.

Example: Configure the interval as 30s for sending the MAC address notification.

Switch(Config)#mac-address-table notification interval 30

3.22.5 mac-notification

Command: mac-notification {added | both | removed}

no mac-notification

Function: Configure the MAC address notification for the specified port, the no command cancels the function.

Parameter: added: the added MAC address

removed: the removed MAC address

both: the added and the removed MAC addresses

Default: No MAC address notification.

Command Mode: Port mode

Usage Guide: After the global switch is disabled, this command is also able to be configured sequentially.

Example: Send the trap notification after the MAC address is added to Ethernet 1/0/5.

Switch(Config)#in ethernet 1/0/5

Switch(Config-if-ethernet 1/0/5)#mac-notification added

3.22.6 show mac-notification summary

Command: show mac-notification summary

Function: Show the configuration of MAC notification and the data of the notification packet.

Parameter: None.

Default: Do not show the summary.

Command Mode: Admin mode

Usage Guide: With this command, check the configuration of MAC address and the sending status of MAC notification trap.

Example:

Switch#show mac-notification summary

MAC address notification:enabled

MAC address snmp traps:enabled

MAC address notification interval = 10

MAC address notification history log size = 120

MAC address added = 0

MAC address removed = 0

MAC address snmp traps generated = 0

3.22.7 snmp-server enable traps mac-notification

Command: snmp-server enable traps mac-notification

no snmp-server enable traps mac-notification

Function: Enable the trap notification of MAC address globally, the no command disables the trap notification.

Parameter: None.

Default: Disable trap notification globally.
Command Mode: Global mode
Usage Guide: This command is used with MAC notification switch. When the switch is disabled, other configuration can be shown, but the function is invalid.
Example: Enable the trap notification of MAC address.
Switch(Config)#snmp-server enable traps mac-notification

3.23 Commands for CFM OAM

3.23.1 clear ethernet cfm

Command: clear ethernet cfm { statistic | traceroute-reply }
Function: Delete the MEP message receive statistic information and tracking of link result.
Parameters: statistic： MEP message receive statistic information
traceroute-reply： Result of automatic tracking of link
Default: None.
Command Mode: Admin Mode.
Usage Guide: Using this command on the switch will delete current MEP message receive statistic information and tracking of link result.
Example: Delete the local MEP message receive statistic information and tracking of link automatically：
Switch#clear ethernet cfm statistic

3.23.2 continuity-check

Command: continuity-check enable
no continuity-check enable
Function: Open the local CCM message sending and receiving functions.
Parameters: None.
Default: MEP and CCM message sending and receiving functions are closed.
Command Mode: MA Configuration Mode.
Usage Guide: Using this command to open the maintance point of CCM message sending and receiving functions.
Example: Open CCM message sending and receiving functions in the test_ma.
Switch(config)#ethernet cfm domain test_1
Switch (config-ecfm)#service test_ma
Switch (config-ecfm-srv)#continuity-check enable

3.23.3 continuity-check interval

Command: continuity-check interval *< interval-value >*

no continuity-check interval

Function: Configure the time interval value for sending message from MEP to CCM.

Parameters: ***interval-value*****：** Represent the time interval value, the range as 1-7.

Default: the time interval value for sending message from MEP to CCM as 4, it means 1s.

Command Mode: MA Configuration Mode.

Usage Guide: Using the command to amend the time interval value for sending message in all mep of MA. The range is 1-7.

Example: Configure the time interval value as 7 for sending message from MEP to CCM in the particular maintance collection test_ma:

Switch(config)#ethernet cfm domain test_1

Switch (config-ecfm)#service test_ma

Switch(config-ecfm-srv)#continuity-check interval 7

3.23.4 continuity-check receive

Command: continuity-check receive rmep <*mep-id*> [active time < *time* >]

no continuity-check receive rmep <*mep-id*>

Function: Open CCM message receiving function and build up rmep in MA.

Parameters: ***<mep-id>*****：** Represent received RMEP number, range is 1- 4094.

< time >：Represent the activate time for RMEP. The range is 0-600, units as second.

Default: MA's CCM message receiving function is closed. Active time default as 0 second, once configure the RMEP, it will open the RMEP receiving function.

Command Mode: MA Configuration Mode.

Usage Guide: Using this command can let the particular rmep CCM can receive the detection function of message in the meplist of MA. Local MEP detection can receive others CCM that is sending from others MEP in the same MA.

Example: Detect the CCM message which sent from the RMEP2 in the particular maintance collection test_ma in MA:

Switch(config)#ethernet cfm domain test_1

Switch (config-ecfm)#service test_ma

Switch(config-ecfm-srv)#continuity-check receive rmep 2

3.23.5 cos

Command: cos < *cos-value* >

no cos

Function: Configure the priority of the message that sending from mep.

Parameters: ***< cos-value >*****：** The priority of the message, the range is 0-7.

Default: cos value as 0.

Command Mode: MA Configuration Mode.

Usage Guide: using this command can let the entire message that sending by MEP fillin this cos value or inform out of order in the MA.

Example: Changing the message cos priority as 7 in the particular test_ma.

Switch(config)#ethernet cfm domain test_1

Switch (config-ecfm)#service test_ma

Switch(config-ecfm-srv)# cos 5

3.23.6 debug ethernet cfm

Command: debug ethernet cfm packet [detail] [lb|lt]

debug ethernet cfm packet [detail] cc [domain *<md_name>* [service *{ ma-name | number < ma-num > | pvlan < vlan-id > }*]]

debug ethernet cfm fsm [lb|lt]

debug ethernet cfm fsm cc [send|received] [domain *<md_name>* [service *{ ma-name | number < ma-num > | pvlan < vlan-id > }*]]

debug ethernet cfm timer [domain *< md_name >* [service *{ ma-name | number < ma-num > | pvlan < vlan-id > }*]

no debug ethernet cfm packet [detail] [lb|lt]

no debug ethernet cfm packet [detail] cc [domain *<md_name>* [service { ma-name | number *< ma-num >* | pvlan *< vlan-id >* }]]

no debug ethernet cfm fsm [lb|lt]

no debug ethernet cfm fsm cc [send|received] [domain *< md_name >* [service { ma-name | number *< ma-num >* | pvlan *< vlan-id >* }]]

no debug ethernet cfm timer [domain *<md_name >* [service { ma-name | number *< ma-num >* | pvlan *< vlan-id >* }]

Function: Open the CFM debug information.

Parameters: packet： Open the message debug information.

detail： Open the detail message debug information.

continuity-check： Open the ccmessage debug information.

send： Open the sending cc message related status debug information.

received： Open the receiving cc message related status debug information.

lb： Open lbrelated degub information.

lt： Open ltrelated debug information.

fsm： Represent open status machine debug information.

timer： Represent open timer debug information domain.

***< domain_name >*：** Represent open particular domain debug information.

***< ma-name >*：** Build up the maintance collection name; it can contain 1-43 characters. It can be letter, number, and underline. The first and the last letter cannot be the underline. The maintance collection and domain name cannot exceed than 44 characters.

number *< ma-num >*： The only MA number that mark in the maintance domain.The range is 0~65535.

***< vlan-id >*：** Configure the service primary vlan. The range is 1-4094.

Default: debug information close.

Command Mode: Admin Mode.

Usage Guide: This command use to open the CFM message, status machines, timing debug

information. It can open all maintance domain debug information.Also, it can contrapose to particular maintance collection for opening the debug function.

Example: Open local CFM debug information.

Switch#debug ethernet cfm all

3.23.7 debug ethernet cfm error

Command: debug ethernet cfm error

no debug ethernet cfm error

Function: Display CFM out of order information.

Parameters: None.

Default: Disable.

Command Mode: Admin Mode.

Usage Guide: Using this command to display CFM out of order information.

Example: Display CFM out of order information.

Switch#debug ethernet cfm error

3.23.8 debug ethernet cfm operation

Command: debug ethernet cfm operation

no debug ethernet operation

Function: Display CFM platform transfer driveport to sending information.

Parameters: None.

Default: Disable.

Command Mode: Admin Mode.

Usage Guide: Display CFM platform transfer driveport to sending information.

Example: Display local CFM platform transfer driveport to sending information.

Switch#debug ethernet cfm operation

3.23.9 ethernet cfm alarm

Command: ethernet cfm alarm {delay < *mseconds* > / notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon} | reset < *mseconds* >}

no ethernet cfm alarm { delay | notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon} | reset }

Function: Using the alarm function for error.

Parameters: delay < *mseconds* >：Represent delay the notification time, it needs to continuous to detect of error occour, then it will inform the out of order. The units as ms, the range is 2500-10000. Default value as 2500.

notification：Configure which error need to be notified.

all：Represent all the errors need to notify, the error including: DefRDI, DefMACStatus, DefRemote, DefError, and DefXcon.

error-xcon：Represent sending the notification to tell the DefError and DefXcon

defects failure occoured.

mac-remote-error-xcon：Represent only inform when DefMACStatus, DefRemote, DefError and DefXcon error occou. This value is the default value of the notification error.

none： No matter what error occoured will not have any notification.

remote-error-xcon： Represent only inform when DefRemote， DefError and DefXconerror occour.

xcon： Only DefXconerror will notify.

reset < *mseconds* >： The reset time for errorring is occour. Once detect the error and notify, this is the time slots that no error should be occoured again. The units: ms, range is 2500-10000. The default value is 10000.

Default: Delay notification is 2.5s, only inform when DefMACStatus, DefRemote, DefError and DefXcon error occour. Next error notification should not be occour within 10s.

Command Mode: Global Mode.

Usage Guide: This command is using for selecting which types of errors to be informed, the delay time for notification and reset time.

Example: configure only notify when xcon error occour.

Switch(config)#ethernet cfm alarm notification xcon

3.23.10 ethernet cfm auto-traceroute cache

Command: ethernet cfm auto-traceroute cache { size < *size-value* > | hold-time *<minutes>*}

no ethernet cfm auto-traceroute cache { size | hold-time }

Function: Configure saving the size of automatic LT detection result or over time result.

Parameters: < *size-value* >： Represent automatic LT detection buffer size, the size-value range is 1～100. The unit is the number of time for sending, the default number is 5. It means that the 5 least detection result for buffer.

***<minutes>*：** Represent automatic saving LTdetection buffer is overtime. The range is 1-65535. The unit is minutes. The default value is 100 minutes. In the other words, the overtime records of buffer will be deleted after 100 minutes.

Default: The buffer just records the 5 least automatic detection result, the overtime as 100minutes.

Command Mode: Global Mode.

Usage Guide: Using this command can configure local automatic saving LT detection result buffer size and over time.

Example: Configure automatic LT detection result over time as 500 minutes:

Switch(config)#ethernet cfm auto-traceroute cache hold-time 500

3.23.11 ethernet cfm domain

Command: ethernet cfm domain < *domain-name* > level < *level-id* >

no ethernet cfm domain < *domain-name* >

Function: Build up MD， enter into the MD configuration mode.

Parameters: < *domain-name* >： Build up the maintance domain name, 1-43 characters. It can be

letter, number, and underline. The first and the last letter cannot be the underline.

< level-id >: Build up maintance domain level. The range is 0-7.

Default: None.

Command Mode: Global Mode.

Usage Guide: Build up MD. Under the default mode, do not build up the MD. When the MD name is illegal or not exist, it will not build up the maintance domain. In the same switch, it can configure multi level of domain with different name. But in the same maintance domain it can only have one level; after build up the maintance domain, it cannot be amended.

Example: Build up the level 3 MD which name as operatorA

Switch(config)#ethernet cfm domain operatorA level 3

Switch(config-ecfm)#

3.23.12 ethernet cfm global

Command: ethernet cfm global

no ethernet cfm global

Function: Open local CFM function.

Parameters: None.

Default: Close.

Command Mode: Global Mode.

Usage Guide: Using this command to open the CFM-OAM function of this computer.

Example: open CFM-OAMfunction:

Switch(config)#ethernet cfm global

3.23.13 ethernet cfm logging

Command: ethernet cfm logging

no ethernet cfm logging

Function: Open CFM registry log function.

Parameters: None.

Default: alarm record in log.

Command Mode: Global Mode.

Usage Guide: Open the log record function. If alarm is occour, it means that has already recorded or inform out of order.

Example: Open CFM record log function:

Switch(config)#ethernet cfm logging

3.23.14 ethernet cfm mep

Command: ethernet cfm mep *< mepid >* domain *< domain-name >* service { *< ma-name >* | number *< ma-num >* | pvlan *< vlan-id >* }

no ethernet cfm mep < mepid > domain < domain-name > service { < ma-name > | number < ma-num > | pvlan < vlan-id > }

Function: Build up MEP

Parameters: ***< domain-name >:*** Domain name of maintance

< mepid >: Represent the number of the maintance point

< ma-name >: Build up the name of maintance collection

< ma-num >: The only MA number that label in the maintance domain. The range is 0-65535.

< vlan-id >: Configure service primary vlan. The range is 1-4094.

Default: MEP does not exist on the port.

Command Mode: Port Configuration Mode.

Usage Guide: MD must be exised in the command, otherwise it will occour error. If this port would like to configure be MEP for several MDs. Can through this command for build up; vlan in the command must already saved in the primary vlan of maintance collection,it means that must use this vlan to find out the corresponding MA, otherwise error occours.

Example: Build up the MA ID as 5 MEP in the ma1 of CustomerB in the e1/1.

Switch(config)#interface ethernet 1/1

Switch(config-if-ethernet1/1)#ethernet cfm mep 5 domain CustomerB service ma1

3.23.15 ethernet cfm mip

Command: ethernet cfm mip auto-create level *< level-id >* vlan *< WORD >* [lower-mep-only] [sender-id chassis]

no ethernet cfm mip auto-create level

Function: Build up the MIP configueation on the layer that does not relate to MA.

Parameters: ***< level-id >:*** Build up default maintance domain level. The range is 0-7.

<WORD>: Configure build up MIP that is not related to ma vlan list. The range is 1~4094, use ";" and "-" for connection.

lower-mep-only: It means the rules of Explicit. It represent if the particular port does not have higher level of MEP, at the lower level of maintance if there is no mid point, whether this level build up the mid point depends on the lower of maintance collection have maintance point or not. If not enter into this parameter, it means that using the default as the rules. If the particular do not have much higher MEP, and the lower maintance does not has maintance mid point, then this level will build up the maintance mid point.

sender-id chassis: Represent the message of the created mip on the default maintance domain will carry Sender ID TLV for sending. If this parameter does not enter, it means that not carry this TLV.

Default: Does not configure the maintance mid point build up rules, and also not exist the maintance mid point. Default not carries sender-id.

Command Mode: Global Mode.

Usage Guide: This build up MIP priority is lower than the manual MIP command (ethernet cfm mip level), it means that under the Port Mode, using the manual command to build up the MIP does not use the manual build up rules. 802.1ag2007standard prescribe each facilities can have one default MD. If you need to maintance the MD, please delete the original default MD, and build up the new one. The default MD level must be higher than the MEP all MD level, and the

priority is equal to the higher MD, use higher level of CCM message to pass through, build up the MIP node recover LTR message.

Example: In the vlan 500, the rule for build up the MIP level on the level 6 port.

Switch(config)#ethernet cfm mip auto-create level 6 vlan 500 lower-mep-only

3.23.16 ethernet cfm mode

Command: ethernet cfm mode {hw|sw|auto}

no ethernet cfm mode

Function: Configure the actualizemethod for the facilities.

Parameter: hw： The supporting method of facilities as hardware.

sw： The supporting method of facilities as software.

auto： The supporting method of facilities as auto depends on the automatic detection for deciding using which method. If the supporting method of all slave cards are consist, then using that method. Otherwise, use the software supporting method.

Default: Automatic.

Command Mode: Global Mode.

Usage Guide: This command is use for the machice mode switch, if the supporting method is not equal for the the slave card, then it can configure as the support mode.

Example: Under the Global Mode to configure the CFM supporting method as hardware.

Switch(config)# ethernet cfm mode hw

3.23.17 ethernet cfm pvlan

Command: ethernet cfm pvlan *<1-4094>* vlan WORD

no ethernet cfm pvlan *<1-4094>*

Function: Configure pvlan and vlan corresponding relationship.

Parameters: *< vlan-id >*： Configure primary vlan. The range is 1~4094.

***< WORD >*：** Configure the pvlan related vlans.

Default: No corresponding relationship between pvlan and vlan.

Command Mode: Global Mode

Usage Guide: This command can configure pvlan and vlan corresponding relation. And MA is relating to one pvlan. Therefore, one MA can relate to several of vlans. Please pay attention to the ma that is related to the pvlan will not be configured with the vlan corresponding relation.

Example: Configure pvlan1 and vlan10 corresponding relation.

Switch(config)#ethernet cfm pvlan 1 vlan 10

3.23.18 ethernet cfm snmp-server enable traps

Command: ethernet cfm snmp-server enable traps

no ethernet cfm snmp-server enable traps

Function: Having the snmp notification during the alarm.

Parameters: None.

Default: Open the trap notification function.
Command Mode: Global Mode.
Usage Guide: If the set up is success, it will have the snmp notification during the alarm.
Example: configure the trap notification duaring alarm.
Switch(config)# ethernet cfm snmp-server enable traps

3.23.19 ethernet cfm y1731 global

Command: ethernet cfm y1731 global
no ethernet cfm y1731 global
Function: Open the y1731 function.
Parameters: None.
Default: Close the y1731 fuction.
Command Mode: Global Mode.
Usage Guide: Open the Y1731 function. After initial this function, the switch will ente into the y1731 mode. The messages are sending and decoding in the Y1731 format.
Notice: It need to use the ethernet cfm global command before using this command, otherwise, it cannot be function.
Example: Global open the y1731 function:
Switch(config)# ethernet cfm y1731 global

3.23.20 id

Command: id {mac-address XX-XX-XX-XX-XX-XX domain-number < *domain-number* > | dns < *dns-name* > | null }
no id
Function: Configure MDID.
Parameters: mac-address XX-XX-XX-XX-XX-XX domain-number < *domain-number* >： Three corresponding format names in the name of maintance domain resolve. Domain-number is two byte integral number.
dns < *dns-name* >： The name of DNS. Two of the format names of corresponding maintance domain resolve. 1-43 characters string.
null： One of the format names of corresponding maintance domain resolve which does not configure md name, MA name is the unique name in the global.
Default: None.
Command Mode: MD Configuration Mode.
Usage Guide: Configure this command means that domain-name which is configured by the name of maintance domain will use the command of ***ethernet cfm domain*** will not be fill in the message. Fill in the MDID and ma name will create MAID; the total length of MAID is 44. The length cannot be existed; otherwise, it will have error.
Example: Configure MDID.
Switch(config)#ethernet cfm domain customerA level 5
Switch(config-ecfm)#id mac-address 00-03-0f-07-08-09 domain-number 1017

3.23.21 mep mepid

Command: mep mepid *< WORD >*

no mep mepid [*< WORD >*]

Function: Build up the MEP permit configuration table

Parameters: *<WORD>*： Represent the maintance base point table. Using "；"and "-" to connect. The range is 1-4094.

Default: None.

Command Mode: MA Configuration Mode.

Usage Guide: Using this command to build up the permit configured MEP table in the maintance collection.

Example: Build up a mepid in the vlan 5 service of operatorA in maintance domain; the range of mepid is 1-25:

Switch(config)#ethernet cfm domain operatorA level 5

Switch(config-ecfm)#service ma1 vlan 5

Switch(config-ecfm-srv)#mep mepid 1-25

3.23.22 mip auto-create

Command: mip auto-create [lower-mep-only | none]

no mip auto-create

Function: Configure the automatic MIP in the maintance collection's domain.

Parameters: lower-mep-only： Mean that Explicit rules, represent if there is no higher priority MEP in the particular port, and there is no mid point in the lower maintance collection. To consider whether build up the mid point depends on if there is a maintance base point in the lower level of maintance collection.

none： Mean that nonerules, under this mode, cannot build up MIP activitely.

Default: Cannot create the mip point.

Command Mode: MA Configuration Mode.

Usage Guide: Using to configure the build up rules for the mid point of the automatic maintance collection. The mid point of maintance is according to the rules to build up on the port of VLAN automatically. No need to enter into any parameters, just follow the default rules to build up. Default rules mean that if there is no higher level of MEP in the port, and no maintance mid point in the lower level of maintance collection. Then this level will build up the maintance mid point.

Notice: The priority of this build up MIP is lower than the MIP command (ethernet cfm mip level) which is build up manually. That is, should not use the automatic build up rules while you use manual build up command in the Port Mode.

If you want to create the the maintance mid point in all of the ports of maintance domain, then select the default rules. If you just want to create the maintance mid point in the base point of lower maintance level, then select the explicit rules.

If the rules to build up the MIP in ma are different from md, then it will follow the ma rules to undergo the establishment.

Because of the number of mip cannot exist than 384, undergo the establishment will according to

the rules to build up. If the number exists the range, then establishment is ineffective and occour error.

The default value of md is none; default value of mip under ma is defer. That means default to accede the mip build up value of md.

Example: Configure the mid point build up rules as default in the 5 maintance domain customerA.

Switch(config)#ethernet cfm domain customerA level 5

Switch(config-ecfm)#mip auto-create

3.23.23 ping ethernet

Command: ping ethernet [target-mep < *mepid* > | target-mac < *mac-address* >] {domain < *domain-name* > service { < *ma-name* > | number < *ma-num* > | pvlan < *vlan-id* > }} [number < *number* >] [packetsize < *size* >] [timeout < *timeout* >]

Function: Open the circulate function.

Parameters: < *mepid* >： Represent the maintance base point number of the LBM message destation.

< *mac-address* >： Represent the destation MAC address, the format of mac-address is H-H-H.

< *domain-name* >： It is the maintance domain name of the destation MP.

< *ma-name* >： It is the name of build up maintance collection. 1～43 characters straing.It can be formed by letter, number, underline and the first and the last character cannot be underline.

***number* < *ma-num* >：** The only number which label the MA in the maintance domain. The range is 0~65535.

< *vlan-id* >： Configure service primary vlan. The range is 1~4094.

< *number* >： The number of the LMB messages that has already sent. The range of the number is 1～10, default value is 5.

< *size* >： It is the size of the LBM data package. The range is 46~1500byte, the default value is 46.

< *timeout* >： Represent the LBM messages which have already sent timeout. If it cannot receive the LBR within the time, then it will leave the LB processes. The range is 3-10, default time is 5s.

Default: The circulate function close. After open the function, the number of LBM message is 5, the size is within 46 character strings, timeout is 5s.

Command Mode: Admin Mode.

Usage Guide: Send LBM messages and receiving LBR message from a particular maintance point to the other points. Under the default stage, this function is closed. If enter into target-mep-id, it cannot searching the corresponding mac address. If it cannot find, it will display error. If you enter the mac address, then will according to this address for the circulation. If it is a domain-name, then it require opening the y1731function, then sending the group broadcast LBM message.

Example: Open the circulation function; check the maintance base point 2 linkage statuses of

test_ma.

Swtich#ping ethernet target-mep 2 domain test_ma service 4

Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=0

Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=1

Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=2

Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=3

Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=4

Packets statistics for 00-03-0f-00-00-03:

Sent = 5, Received = 5, Lost = 0 (0% loss).

Approximate round trip times in milli-seconds:

Minimum < 16 ms, Maximum = 16 ms, Average < 16 ms.

Field	Description
Reply from 00-03-0f-00-00-03	MAC as 00-03-0f-00-00-03 facility recover toLBR
bytes = 46	Recover the LBR messages size to 32bytes
sequence number	Recover the LBR sequence number
Packets statistics for 00-03-0f-00-00-03	MAC as 00-03-0f-00-00-03 facility receive the LBR
Send	The number of current LBM
Received	Receive the number of replay recover LBR
Lost	The number of drop LBM or LBR
Minimum	The shorest time that ping sending to LBM and receive from LBR
Maximum	The longest time that ping sending to LBM and receive from LBR
Average	The average time that ping sending to LBM and receive from LBR

3.23.24 sender-id

Command: sender-id { chassis | none}

Function: Configure the sending messages if there is sender id information.

Parameters: chassis： The sending message contains of chassis idinformation.

none： The sending message does not contain of Sender ID TLV.

Default: The sending messages do not contain Sender ID TLV.

Command Mode: MA Configuration Mode.

Usage Guide: Using this command to decide whether the message contains of sender-id information.

Example: Configurate the message to carry chassis id information in the particular ma.

Switch(config-ecfm-srv)#sender-id chassis

3.23.25 service

Command: service { < ma-name > | number < ma-num > | pvlan < vlan-id > }{ port | pvlan < vlan-id > } [direction down]

no service { < ma-name > | number < ma-num > | pvlan < vlan-id > }

Function: Build up MA.

Parameters: *< ma-name >*： Build up the name of maintance ,1～43 characters. It can be formed by letter, number, underline and the first and the last character cannot be underline. The total number of the collection and the domain name cannot exist than 44 characters.

number *< ma-num >*： The only number which label the MA in the maintance domain. The range is 0~65535.

***< vlan-id >*：** Configure the service primary vlan. The range is 1~4094.

port： This is not related to any vlan.

direction down： The direction of maintance collection, the default value as up, entering this command means down.

Default: Do not build up maintance collection.

Command Mode: MD configuration mode.

Usage Guide: In the same domain, the maintance collection is the unquie one. If thedomain name is null, then the collection represent is unquie one in the global.

If it is not include Maintenance Domain Name, the name of collection cannot exist than 45 characters. If it includes the Maintenance Domain Name, then the domain name cannot exist than 43 characters.Also the sum of collection name and the domain name should not bigger than 44 characters.

Before build up the collection, it must build up the domain. One switch can configure maximum 512 MA.

One service can related to one or more vlan. If the configured service direction as down, then several levels' service can relate to same vlans. If the direction is up service, then it cannot relate to same vlans.

One primary vlan cannot relate by different level of domain md, primary vlan and level can confirm the ma.

If configure one service as port, then not relate to vlan, service is only link to these two point. And the mep contains in service should be down mep, will only sending between these two point, and cannot be transmit.

Example: In the maintance collection customerA to build up ID as 10, the related VLAN 17 direction as down collection.

```
Switch(config)#ethernet cfm domain customerA level 5
Switch(config-ecfm)#service 10 pvlan 17 direction down
Switch(config-ecfm-srv)#
```

3.23.26 show ethernet cfm domain

Command: show ethernet cfm domain { < domain_name > | brief }

Function: Display the configured information of maintance domain.

Parameters: *< domain-name >*： Build up the domain name, 1～43 characters. .It can be formed by letter, number, underline and the first and the last character cannot be underline.If it cannot

be appointed, then it will display all the domains in the facilities.

brief：Display the brief maintance domain information.

Default: None.

Command Mode: Admin Mode.

Usage Guide: To display the configured information in MD.

Example: Display all the configured information that is in the local maintance domain.

Switch#show ethernet cfm domain brief

Domain Name	Level	Services Number
test_ma	Lv4	2

Field	Description
Domain Name	The domain name of maintance, it is the only label in the domain
Level	The level of maintance domain
Services Number	The number of maintance collection contains in the domain name

Display the configured information that is in the local maintance domain in test_ma.

Switch#show ethernet cfm domain test_ma

Domain Name: test_ma

Level: 4

Total Services: 2

Service Name	Primary Vlan	Dir	CC Send	CC Received	CC Interval
4	Vlan1	Down	Enable	Enable	1(s)
1	Vlan2	Up	Disable	Disable	1(s)

Field	Description
Domain Name	The domain name of maintance, it is the only label in the domain
Level	The level of maintance domain
Total Services	The number of maintance collection contains in the domain name
Service Name	The name of maintance collection
Primary Vlan	Maintance collection that is related to Vlan
Dir	The direction of maintance collection
CC Send	The sending function of CC in maintance collection
CC Received	The received function of CC in maintance collection
CC Interval	The interval of CC sending in maintance collection

3.23.27 show ethernet cfm errors

Command: show ethernet cfm errors

Function: Display the errors that are detected on the facility.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Display the errors that are detected on the facility.

Example: Display the errors that are detected on the facility.

Switch(config))#show ethernet cfm errors

Code：X – xconCCDomainefect, E – errorCCDomainefect, O - someRMEPCCDomainefect，M – someMACstatusDefect, R - someRDIdefect

Mepid	Error type	Domain name	Service name	Level
1	X E	kk	ma	lv7
1	X E	kk	ma	lv7
1	X E	kk	ma	lv7
1	X E	kk	ma	lv7

Field	Description
MEPID	Detected errors in the Local MEPID
DOMAIN id	The DOMAIN name of MEP that is the detected errors located
MAName	MA name of the detected errors MEP
error-type	Types of error, including：xconCCDomainefect, errorCCDomainefect, someRMEPCCDomainefect, someMACstatusDefect, someRDIdefect
Level	The level that MEP belongs to

3.23.28 show ethernet cfm maintenance-points local

Command: show ethernet cfm maintenance-points local [detail] [mep | mip] [domain < ***domain-name*** **> | interface { ethernet | } <*IFNAME*>]**

Function: Display the attribute and the operation information of the maintance basepoint.

Parameters: detail： Display the detail information.

mep： Display the MEP information.

mip： Display the MIP information.

< *domain-name* >: The domain name of the maintance domain.

interface { ethernet | } <*IFNAME*>： The port that is maintance point located.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Display the local maintance base point information. Please pay attention to the following: if there are no selectable parameters, then display all the mp basic information on the switch. Can undergo the following screening range to display the MP: appointed maintance

domain or particular port.

Example: Display all the local MP information on the switch.

Switch#show ethernet cfm maintenance-points local mep

```
-----------------------------------------------------------------------------------------------------
Mepid     Domain Name     Level                Vlan-id          CC Send
          Service Name    Direction            Port
-----------------------------------------------------------------------------------------------------
1         test_ma         Lv4                  Vlan1            Enable
          4               Down                 Ethernet1/4
```

Field	Description
Mepid	MP label.If it is mip, then None.
Domain Id	The domain id label
MA Name	The name of MA
Lvl	The level which MP belongs to
Dir	MP direction
Port	MP located port
Type	Types of MEP（VLAN or port）
Vlan-id	MEP related vlan id list
CC	Whether CC function is open

```
Switch#show ethernet cfm maintenance-points local detail mep
Mepid:11
Port:Ethernet1/1                    Active:0
Domain Name:kk
Service Name:mb
Level:2                  Vlan:None                  Direction:Down
-----------------------------------------------------------------------------------------------------
CCM:
CC      Send:Enable              CC      Received:Enable              Interval:1(s)
-----------------------------------------------------------------------------------------------------
No CCM from some remote MEPs is received.
-----------------------------------------------------------------------------------------------------
One or more error CCM is received. The last-received CCM:
Domain Name: kk
Service Name: ma
Mepid:2
Received Time:Jan 01 00:17:25 2006
-----------------------------------------------------------------------------------------------------
One or more cross-connect CCM is received. The last-received CCM:
Domain Name: kk
Service Name: ma
Mepid:2
Received Time:Jan 01 00:17:25 2006
```

Some other MEPs are transmitting the RDI bit.

Field	Description
Interface	The port that is maintance base point located
DOMAIN	The domain that is maintance base point located
SERVICE	The maintance collection that is maintance base point located
Level	The level of domain
VLAN	The VLAN that is maintance collection point located
Direction	The maintance base point direction
CCM	CCM related information
CCM send	Whether base point sending CCM message
CCM received	Whether base point receiving CCM message
Interval	The interval to sending CCM
Crosscheck	Whether the base point is checking cross error
Start-delay	The delay time for cross check
No CCM from some remote MEPs is received	To tell not receiving outlying MEP sending CCM message （occour the time out error）
One or more streams of error CCMs is received. The last-received CCM	To tell receiving error CCM message and display the last error message information
DOMAIN	The domain of last error CCM message
SERVICE	The service of last error CCM message
MEP	The MEP of last error CCM message
Received Time	The received time of last error CCM message
One or more cross-connect CCMs is received. The last-received CCM	The network may have the cross connection, this message means that to tell receiving cross connection message and display the last message information
Some other MEPs are transmitting the RDI bi	Receiving others maintance base point sending RDI （reverse error）that is configure by the CCM message （this will only display when receive the CCM message）

3.23.29 show ethernet cfm maintenance-points remote

Command: show ethernet cfm maintenance-points remote (domain WORD (service (WORD|number *<0-65535>*|pvlan *<1-4094>*) (mepid *<1-4094>*|)|)|)

Function: Display the attribute and operation information of outlaying maintance base point.

Parameters: *< domain-name >*： The maintance domain name.

***< mepid >*：** Represent the maintance base point number.

***< ma-name >*：** It is the name of build up maintance collection. 1～43 characters straing.It can be formed by letter, number, underline and the first and the last character cannot

be underline.

number < *ma-num* >: The only number which label the MA in the maintance domain. The range is 0~65535.

***< vlan-id >*:** Configure service primary vlan. The range is 1~4094.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Display the outlying base point information. Please pay attention: if there are no selectable parameters, then it will display all the outlying mep basic information on the switch.

Example: Display all the MP information of the switch.

Switch#show ethernet cfm maintenance-points remote

```
-----------------------------------------------------------------------------------------------------
Mepid        Domain Name    Level          Mac Address              RDI
             Service Name   Vlanid         Ingress                  Status
-----------------------------------------------------------------------------------------------------
2            test_ma        Lv4            00-03-0f-00-00-03        Y
             4              Vlan1          Ethernet1/4              Linkup
```

Field	Description
Mepid	MEP label
Domain Name	The domain name
Level	The level of maintance domain
Mac Address	MEP mac address
RDI	Whether the RDI of CCM message which is sending from outlying MEP location is 1
Service Name	The name of maintance collection
Vlanid	The related Vlan of maintance collection
Ingress	Outlaying MEP message enter port
Status	Outlaying MEP status

3.23.30 show ethernet cfm maintenance-points remote detail

Command: show ethernet cfm maintenance-points remote detail (mac XX-XX-XX-XX-XX-XX | domain WORD (service ((WORD)|(number *<0-65535>*)|(pvlan *<1-4094>*))) mepid *<1-4094>*)

Function: Display the attribute and the operation information for the outlaying maintance base point.

Parameters: mac *< mac-address >*: MEP mac address.

***< mepid >*:** Represent the maintance base point number.

***< domain-name >*:** The maintance domain name.

***< ma-name >*:** It is the name of build up maintance collection. 1～43 characters straing.It can be formed by letter, number, underline and the first and the last character cannot be underline.

number < *ma-num* >： The only number which label the MA in the maintance domain. The range is 0~65535.

< *vlan-id* >： Configure service primary vlan. The range is 1~4094.

Default: None.

Command Mode: Admin Mode.

Usage Guide: If the parameter is mac address, it will display all the outlying mep detail information which is using this mac address. If the parameter is mepid, then need to appoint the domain and the collection that is located.

Example: Display the appoint outlying MEP message on the switch, this MEP belongs to Domain_L5, maintance collection primary vlan as 5:

Switch#show ethernet cfm maintenance-points remote detail mepid 401 domain Domain_L5 vlan 5

Mac Address:00-03-0f-07-04-01

Domain Name:kk

Service Name:ma

Level:2

Vlan:1

Mepid:1

Incoming Port:Ethernet1/2

CC Send Interval:1(s)

Mep Port Status:Up

Receive Rdi:N

Field	Description
MAC Address	Outlying MEP mac address
Domain Name	Domain name
MA Name	The name of MA
Level	The level of the maintance collection
VLAN	The primary vlan of the maintance collection
MPID	Outlying MEPID
Sender Chassis ID	Sender id tlv fill in content
Incoming Port(s)	The local port which is receiving the messages from the outlying MEP
Cc send interval(ms)	The interval that sending cc from the outlying MEP
MEP interface status	The status of outlying MEP
Receive RDI	Whether RDI is sending

3.23.31 show ethernet cfm mpdb

Command: show ethernet cfm mpdb

Function: Display the content of MIP datebase.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Display the content of MIP datebase.

Example: Display the content of MIP datebase.

Switch#show ethernet cfm mpdb

Mac Address Ingress Vlan Age

00-03-0f-00-00-03 Ethernet1/4 Vlan1 0 (s)

Field	Description
MacAddress	The source mac addressIn CCM
Ingress	Entery port of CCM
Type Id	Fid and its value
Age	The upload and renewal time of Mip database distance

3.23.32 show ethernet cfm service

Command: show ethernet cfm service [domain < *domain-name* > [service { ma-name | number < *ma-num* > | pvlan < *vlan-id* > }]]

Function: Display the configured information of the maintance collection.

Parameters: < *domain-name* >： The maintance domain name.

< *ma-name* >： It is the name of build up maintance collection. 1～43 characters straing. It can be formed by letter, number, underline and the first and the last character cannot be underline.

number < *ma-num* >： The only number which label the MA in the maintance domain. The range is 0~65535.

< *vlan-id* >： Configure service primary vlan. The range is 1~4094.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Display the configuration information in the maintance collection.

Notice: If the is no appoint domain, will display all the configured information in all maintance collections and domains.

If it is only appointed the domain but not maintance collection, then just display all the maintance collection in the the appointed domain.

Example: Display all the configured information of maintance collection in all domains.

Switch#show ethernet cfm service

Domain Name: test_ma

Level: 4

Service Name: 4

Active: 1

Primary Vlan: 1

Vlanlist: 1
Direction: Down
CC Send: Enable
CC Received: Enable
CC Interval: 1(s)
Meplist: 1-4094
Remote Mep: 2

Domain Name: test_ma
Level: 4
Service Name: 1
Active: 1
Primary Vlan: 2
Vlanlist: 2
Direction: Up
CC Send: Disable
CC Received: Disable
CC Interval: 1(s)

Field	Description
Domain Name	The domain name
Level	The level of maintance domain
Service Name	The name of maintance collection
Active	Whether the maintance collection is working
Primary Vlan	The related primary Vlan of maintance collection
Vlanlist	The related Vlan of maintance collection
Direction	The direction of maintance collection
CC Send	The sending function of CC in maintance collection
CC Received	The received function of CC in maintance collection
CC Interval	The interval of CC sending in maintance collection
Meplist: 1-4094	MEP table
Remote Mep	Outlying MEP

3.23.33 show ethernet cfm statistic

Command: show ethernet cfm statistic [domain < *domain-name* > [service { ma-name | number < *ma-num* > | pvlan < *vlan-id* > }]]

Function: Display the message sending statistics information in the CFM of the facility.

Parameters: ***< domain-name >***：The maintance domain name.

< ma-name >：It is the name of build up maintance collection. 1～43 characters straing.It can be formed by letter, number, underline and the first and the last character cannot be underline.

number ***< ma-num >***：The only number which label the MA in the maintance domain. The range is 0~65535.

< vlan-id >：Configure service primary vlan. The range is 1~4094.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Display the message sending statistics information in the CFM of the facility.

Example: Display the message sending statistics information in the CFM of the facility.

```
Switch#show ethernet cfm statistic
LB:
    SendLBM: 5                    ReceiveLBM: 0
    SendLBR: 0                    ReceiveLBR: 5
    ReceiveInOrderLBR: 5          ReceiveOutOrderLBR: 0          ErrorLBR: 0

LT:
    SendLTM: 0                    ReceiveLTM: 0
    SendLTR: 0                    ReceiveLTR: 0                  ErrorLTR: 0

Domain Name: test_ma
Service Name: 4
Mepid: 1
CCM:
    SendCCM: 0                    ReceivedCCM: 18162
    OutOfOrder: 0                 Xcon: 24
    ErrorCCM: 0                   MacStatusCCM: 0                RdiCCM: 18138
```

Field	Description
SendLBM	The number of sending LBM
ReceiveLBM	The number of receiving LBM
SendLBR	The number of sending BR
ReceiveLBR	The number of receiving BR
ReceiveInOrderLBR	The number of receive in order LBR
ReceiveOutOrderLBR	The number of receive out of order LBR
ErrorLBR	The number of receiving illegal LBR
SendLTM	The number of sending LTM
ReceiveLTM	The number of receiving LTM
SendLTR	The number of sending LRT
ReceiveLTR	The number of receiving LRT
ErrorLTR	The number of receiving illegal LTR
Domain Name	Domain name

Service Name	Maintance collection Name
Mepid	MEP Name
SendCCM	The number of sending CCM
ReceivedCCM	The number of receiving CCM
OutOfOrder	The number of out of order CCM
Xcon	The number of receiving cross CCM
ErrorCCM	The number of receiving illegal CCM
MacStatusCCM	The number of receiving mac status error CCM
RdiCCM	The number of CCM that is receiving RDI position 1

3.23.34 show ethernet cfm status

Command: show ethernet cfm status

Function: Display the status of CFM of the facility.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Display the status of CFM of the facility.

Example: Display the status of CFM of the facility.

Switch#show ethernet cfm status

Ethernet cfm is enabled.

Y1731 global is enabled.

Field	Description
CFM is enabled.	Open the CFM function
CFM is disabled.	Do not open the CFM function
Y1731 global is enabled	Y1731 function has opened

3.23.35 show ethernet cfm traceroute-reply auto

Command: show ethernet cfm traceroute-reply auto [domain < *domain_name* > [service { ma-name | number < *ma-num* > | pvlan < *vlan-id* > }]]

Function: Display the result of the automatic LT.

Parameters: < *domain-name* >： The maintance domain name.

< *ma-name* >： It is the name of build up maintance collection. 1～43 characters straing.It can be formed by letter, number, underline and the first and the last character cannot be underline.

number < *ma-num* >： The only number which label the MA in the maintance domain. The range is 0~65535.

< *vlan-id* >： Configure service primary vlan. The range is 1~4094.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Display the received LTR content that is automatic saving LTM message.

Notice: If there is no appointed domain, then it will display all the automatic LT result in the facilities.

If there is no appointed ma, then it will display particular domain's automatic LT result in the facilities.

Example: Display all the result of the automatic LT.

Switch#show ethernet cfm traceroute-reply auto

Traceroute to MEP 606 with the sequence number 0,TTL 255.

Timeout is 5 seconds.Tracing the route to 00-03-0f-aa-22-23 on DOMAIN test_4 ,Level 4, Service:4

Traceroute sent via Ethernet1/1, path found via MPDB

I-----Intermedian Bridge

D----Target Destination

*-----Per hop Timeout

	MAC Address	TTL	Last MAC	Ingress/Egress Action	Relay Action
I	00-03-0f-00-00-03	254	00-03-0f-00-00-03	IngOK/EgrOK	FDB
D	00-03-0f-aa-22-23	253	00-03-0f-00-00-03	/EgrDown	Hit

Filed	Explanation
MAC Address	Source MAC address in LTR.
TTL	The number of hops that LTM passed by the device.
Last MAC	The MAC of the last hop of device that LTM packet passed by.
Ingress/Egress Action	The analyzed port status with Reply Ingress TLV and Reply Egress TLV.
Relay Action	It means whether the forwarding device found the target表示MAC address in MAC address. Hit: this device is the target MAC address. FDB: have found the target MAC address in forwarding table.

3.23.36 show ethernet cfm vlan table

Command: show ethernet cfm vlan table

Function: Show the corresponding relationship of the configured pvlan and vlan on this device.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Use **ethernet cfm pvlan *<1-4094>* vlan WORD** command to configure pvlan to associate with vlan, and then use this command to show the corresponding relationship of the

configured pvlan and vlan on this device.

Example: Show the corresponding relationship of the configured pvlan and vlan on this device.

Switch(config))# show ethernet cfm vlan table

ethernet cfm vlan table:

pvlan 2 vlan 3-6

pvlan 7 vlan 8-10

3.23.37 switchport ulpp group <group-id> track cfm cc level <level-value>

Command: switchport ulpp group *<group-id>* track cfm cc level *<level-value>*

Function: Configure ulpp group member port to associate with cfm cc detection.

Parameters: *<group-id>*： ID information of ulpp group.

***<level-value>*：** Associate with that the configured down mep of this level on the port detecting the cc error.

Default: Do not associate.

Command Mode: Port Mode.

Usage Guide: Configure the level information of the association of ulpp group member port and cfm cc detection. When ulpp group member port received the matching cfm information (timeout or recover), conduct the association.

Example: Configure the port of ulpp group1 to associate with the cc detection of down mep on level 1.

Switch(config-if-ethernet1/1)#switchport ulpp group 1 track cfm level 1

3.23.38 traceroute ethernet

Command: traceroute ethernet { target-mep *< target-mep-id >* | target-mac *< mac-address >* } {domain *< domain-name >* service { *< ma-name >* | number *< ma-num >* | pvlan *< vlan-id >* }} [fdb-only | source *< mepid >*]] [ttl *< ttl-value >*]

Function: Check the path from the appointed maintaining point to the target point.

Parameters: *< target-mep-id >*： The number of the target maintaining point of LTM packet;

***< mac-address >*：** The target MAC address, the format if H-H-H;

***< domain-name >*：** The maintaining domain name that the target MP belongs to.

***< ma-name >*：** The name of the created maintaining set, with 1 to 43 characters.it ismade up by letters, numbers and underscores, the first and last character cannot be the underscore.

number *< ma-num >*： It is the number which is only used to mark the MA,range is 0 to 65535.

***< vlan-id >*：** Primary vlan of the configured service, range is 1 to 4094.

fdb-only： When finding the egress port, whether to inquiry the FDB table. If this value is not configured, it means that not only inquiry the FDB, and inquiry the MIP database.

source *< source-mepid >*： It is he id of MEP which is used to issue the LTM.

***< ttl-value >*:** It is he number of hops that LTM can pass by, range is 1 to 255 and the default value is 64.

Default: ttl=64 and inquiry FDB and MIP database.

Command Mode: Admin Mode.

Usage Guide: CFM traceroute command is used to inquiry the the path from the appointed maintaining point to the target point. Through sending LTM packet to the target maintaining point and detecting the responsed LTR packet, ensure the path among the devices.

Example: Inquiry the path with mac of 00-03-0f-aa-22-23 in test_4.

Switch#traceroute ethernet target-mac 00-03-0f-aa-22-23 domain test_4 service 4

Traceroute with the sequence number 4,TTL 64.

Timeout is 5 seconds.Tracing the route to 00-03-0f-aa-22-23 on MD test_4, Level 4, Service:4

Traceroute sent via Ethernet1/4, path found via MPDB

I-----Intermedian Bridge

D----Target Destination

*-----Per hop Timeout

	MAC Address	TTL	Last MAC	Ingress/Egress Action	Relay Action
D	00-03-0f-aa-22-23	63	00-03-0f-00-00-03	IngOK/	Hit

Field	Explanation
MAC Address	Source MAC address in LTR.
TTL	The number of hops that LTM passed by the device.
Last MAC	The MAC of the last hop of device that LTM packet passed by.
Ingress/Egress Action	The analyzed port status with Reply Ingress TLV and Reply Egress TLV.
Relay Action	It means whether the forwarding device found the target表示 MAC address in MAC address. Hit: this device is the target MAC address. FDB: have found the target MAC address in forwarding table.

3.23.39 traceroute ethernet auto

Command: traceroute ethernet auto

no traceroute ethernet auto

Function: Enable the function of sending the link track packets automatically.

Parameters: None.

Default: Disable.

Command Mode: MA Configuration Mode.

Usage Guide: Enable the function of sending the link track packets automatically. As default, this function is disabled.

Notice: After enabled this function, when the maintaining point does not receive the CCM packets from the distant point in 3.5 sending cycles of CCM packets, judge that the connection to

the distant point is wrong, then send LTM packet (the target of this LTM packet is the distant maintaining point, the TTL field in LTM packet is the maximum value of 255) to locate the error through detecting the responsed LTR packet.

Example: Enable the function of sending the link track packets automatically.

Switch(config-ecfm-srv)#traceroute ethernet auto

Chapter 4 Commands for IP services

4.1 Layer 3 Interface

4.1.1 Bandwidth

Command: bandwidth <bandwidth>
no bandwidth
Function: Configure the bandwidth for Interface vlan. The 'no bandwidth' command recovery the default value. The bandwidth of interface vlan is used to protocol account but not control the bandwidth of port. For instance, it is use the interface bandwidth（cost=10^8/bandwidth）when OSPF account the link cost, so change the bandwidth can result in OSPF link cost changed.
Parameters: <*bandwidth*> is the bandwidth for interface vlan. Range from 1bits to 10000000000 bits. It is can use unit 'k, m, g'. There are no decimal numbers after conversion.
Command mode: VLAN Interface Mode
Default: The default bandwidth for interface VLAN is 100,000,000bit.
Usage Guide: This command only can be used at interface VLAN mode. The conversion of unit: 1g=1,000m=1,000,000k=1,000,000,000bit.
Example: Configure the bandwidth for vlan1 is 50,000,000bit.
Switch(Config-if-Vlan1)#bandwidth 50m

4.1.2 description

Command: description <*text*>
no description
Function: Configure the description information of VLAN interface. The no command will cancel the description information of VLAN interface.
Parameter: <*text*> is the description information of VLAN interface, the length should not exceed 256 characters.
Default: Do not configure.
Command Mode: VLAN interface mode
Usage Guide: The description information of VLAN interface behind description and shown under the configured VLAN.
Example: Configure the description information of VLAN interface as test vlan.
Switch(config)#interface vlan 2
Switch(config-if-vlan2)#description test vlan

4.1.3 description (VRF mode)

Command: description <text>
no description
Function: Configure the VRF description information to record the relation of VPN instance and any. The no operation of the command will cancel the VPN description information.
Parameter: <*text*>: Description text, the ranging from 1 to 256 characters.
Default: Not configured.
Command Mode: VRF mode.
Usage Guide: VRF description information behind description and shown under the configured VRF to supply the relative information.
Example: Configure VRF description information as

4.1.4 interface loopback

Command: interface loopback <loopback-id>
no interface loopback ***<loopback-id>***
Function: Create a Loopback interface; the no operation of this command will delete the specified Loopback interface.
Parameters: <*loopback-id*> is the ID of the new created Loopback interface.
Default: There is no Loopback interface in factory defaults.
Command Mode: Global Configuration Mode.
Usage Guide: IDs of the VLANs taken up by a Loopback interfaces start from 1006. If Loopback take up a VLAN whose ID is larger than or equal with1006, users are forbidden to configure the corresponding VLAN. If a VLAN after VLAN 1006 is already configured, such as VLAN 1006, then the Loopback interface will take up the first available VLAN after that VLAN, such as VLAN 1007.
Examples: Enter the interface configuration mode of Loopback 1.
Switch(config)#interface loopback 1
Switch(Config-if-Loopback1)#

4.1.5 mac-address

Command: interface loopback <loopback-id**>**
no interface loopback <loopback-id**>**
Function: Create a Loopback interface; the no operation of this command will delete the specified Loopback interface.
Parameters: <loopback-id> is the ID of the new created Loopback interface.
Default: There is no Loopback interface in factory defaults.
Command Mode: Global Configuration Mode.
Usage Guide: IDs of the VLANs taken up by a Loopback interfaces start from 1006. If Loopback take up a VLAN whose ID is larger than or equal with1006, users are forbidden to configure the corresponding VLAN. If a VLAN after VLAN 1006 is already configured, such as VLAN 1006, then the Loopback interface will take up the first available VLAN after that VLAN, such as VLAN 1007.
Examples: Enter the interface configuration mode of Loopback 1.
Switch(config)#interface loopback 1

Switch(Config-if-Loopback1)#witch(config)#interface vlan 1
switch(Config-if-Vlan1)# mac-address 00-11-22-33-44-55

4.1.6 interface vlan

Command: interface vlan *<vlan-id>*
no interface vlan *<vlan-id>*
Function: Create a VLAN interface (a Layer 3 interface); the "**no interface vlan *<vlan-id>***" command deletes the Layer 3 interface specified.
Parameters: *<vlan-id>* is the VLAN ID of the established VLAN, ranging from 1 to 4094.
Default: No Layer 3 interface is configured upon switch shipment.
Command mode: Global Mode
Usage Guide: When creating a VLAN interface (Layer 3 interface), VLANs should be configured first, for details, see the VLAN chapters. When VLAN interface (Layer 3 interface) is created with this command, the VLAN interface (Layer 3 interface) configuration mode will be entered. After the creation of the VLAN interface (Layer 3 interface), interface vlan command can still be used to enter Layer 3 Port Mode.
Example: Create a VLAN interface (layer 3 interface).
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#

4.1.7 ip vrf

Command: ip vrf <vrf-name>
no ip vrf ***<vrf-name>***
Function: Configure the corresponding VPN instance, the no command cancel this VPN instance.
Parameter: *<vrf-name>*: Configure the name of VPN instance, the ranging from 1 to 64.
Default: Not configured.
Command Mode: Global configuration mode.
Usage Guide: Configure the corresponding VPN instance. There is no default VPN instance on PE, a PE can create multiple VPN instances and the name distinguishes the **capital letter and small letter. Please pay attention: VPN instance takes effect after configure RD.**
Example:
Switch(config)#ip vrf VRF-A
Switch(config-vrf)#

4.1.8 ip vrf forwarding vrfName

Command: ip vrf forwarding <vrfName>
no ip **vrf forwarding *<vrfName>***

Function: Relate the interface to the specific VRF.

Parameter: <*vrf-name*>: Configure the name of VPN instance, the length is less than 32 characters.

Default: Bind the interface to the master VRF.

Command Mode: Interface configuration mode.

Usage Guide: If the interface needs to access internet, this command can be configured and an interface bind a VRF only, but a VRF can bind multiple interfaces.

Example:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ip vrf forwarding vpn1

4.1.9 no interface IFNAME

Command: no interface IFNAME

Function: Delete the interface, deal with the interface vlan and interface loopback only.

Parameters: IFNAME: interface name.

Command Mode: Global mode.

Usage Guide: This command is used to delete the layer 3 interface. It can deal with the situation that the interface name is spelt in special way. IFNAME can match multiple ways, such as vlan1, Vlan1, v1, V1 and etc.

Example: Delete interface vlan1.

(config)# no interface vlan1

4.1.10 rd

Command: rd <ASN:nn_or_IP-address:nn>

Function: Configure RD(Route Distinguish) of VRF.

Parameter: ASN:nn_or_IP-address:nn is the IP address format of the route identification label.

Default: Not configured.

Command Mode: VRF mode

Usage Guide: The configured RD is for identifying different VPN each of which shall have a unique RD, VPN instance implement the space independence and address repeat through RD. But attention should be paid on that this setting is made up by AS number and a arbitrary number and RD can not be deleted directly.

Example:

Switch (config)#ip vrf VRF-A

Switch (config-vrf)# rd 300:3

Switch (config-vrf)#

4.1.11 route-target

命令：route-target {import | export | both} <rt-value>
no **route-target {import | export | both} <*rt-value*>**
功能： 配置指定 VRF 的 Route-Target；no 命令删除配置。
参数： import：表示对路由进行入口过滤，即判断 VPN 路由是否可以加入本 VRF；
export：表示当将本 VRF 的路由作为 VPNv4 路由向外发送时需附加的 Route-Target，用于对端口进行入口过滤；
both：表示 import、export 使用相同的 Route-Target 值；
<rt-value>：表示路由目标值。
缺省情况： 默认不配置。
命令模式： VRF 配置模式。
使用指南： 一个 RT 是一个 BGP 扩展团体，用于对 VPN 路由进行过滤，实现对直连 site 的 VPN 成员关系和路由规则的控制。对于配置的 import 规则，遍历所有 BGP 进程收到的路由，对符合条件的路由（路由的 export route-target 与本 VRF 的 import route-target 有交集），添加到该 VRF 下的 BGP 进程中，并向该 VRF 下的 BGP 私网邻居发布路由更新消息。对于配置的 export 规则，遍历该 VRF 关联的 BGP 进程中存储的所有 BGP 路由，对这些路由增加一个 export route-target，之后向所有公网邻居发布路由更新消息，同时，如果有其它 VRF 的 import route-target 与该 export route-target 相匹配，则复制一份路由到匹配 VRF 中，并向这个 VRF 下的 BGP 私网邻居发布路由更新。
举例：
Switch (config)#ip vrf VRF-A
Switch (config-vrf)# route-target both 100:1
Switch (config-vrf)#

4.1.12 show ip route

Command: show ip route [database]
Function: Display routing table.
Parameters:< Database>represents database information.
Command mode: privileged user configuration mode.
Usage guide: Display the contents of the core routing table, including routing type, destination network, mask, next hop address, interface, etc.
give an example:
Switch#show ip route
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
A - OSPF ASE, B - BGP derived
Destination Mask Nexthop Interface Pref
C 2.2.2.0 255.255.255.0 0.0.0.0 vlan2 0
C 4.4.4.0 255.255.255.0 0.0.0.0 vlan4 0
S 6.6.6.0 255.255.255.0 9.9.9.9 vlan9 1

display information	explain
C - connected	Direct routing refers to the network segment directly connected to the layer 3 switch
S – static	Direct routing refers to static routing of network segments directly connected to layer 3 switches, which is manually configured by users
R - RIP derived	RIP routing, obtained by layer 3 switches through RIP protocol
O - OSPF derived	OSPF routing, obtained by layer 3 switches through the OSPF protocol
A- OSPF ASE	OSPF introduces routing
B- BGP derived	BGP routing, obtained through the BGP protocol
Destination	target network
Mask	Mask of the target network
Nexthop	Next hop IP address
Interface	The interface of the three-layer switch that the next hop passes through
Preference	The priority of the route, if there are other types of routes to reach the target network, only the routing information with higher priority will be displayed in the core routing table

4.1.13 show ip route vrf

Command: show ip route vrf <vrf-name> **[bgp | datebase]**

Parameter: <*vrf-name*>: VRF name is created by if vrf <vrf-name>.

bgp: Import the route through BGP.

database: The database of IP route table.

Default: None.

Command Mode: Any modes.

Usage Guide: Show the specific route protocol.

Example:

Switch#show ip route vrf vrf-a bgp

Network Next Hop Metric LocPrf Weight Path

Route Distinguisher: 100:10 (Default for VRF test)

*> 11.1.1.0/24 11.1.1.64 0 0 200 ?
*> 20.1.1.0/24 11.1.1.64 0 0 200 ?

4.1.14 show ip vrf

Command: show ip vrf [<vrf-name>]
Function**:** Show the related RIP instance information with VPN route/forwarding instance, it can show fallback global option.
Parameter: <*vrf-name*>: Specify the name of VPN route/forwarding instance.
Default: Not display.
Command Mode: Any modes.
Usage Guide: This command exists in other route protocol. When using this command, the information of other related route protocol will be shown.
Example: Show the related RIP instance information with VRF route/forwarding instance of IPI.

```
Switch# show ip vrf IPI
  VRF IPI, FIB ID 1
  Router ID: 11.1.1.1 (automatic)
  Interfaces:
  Vlan1
  !
  VRF IPI; (id=1); RIP enabled Interfaces:
  Ethernet1/0/8

  Name                Interfaces
  IPI                   Vlan1

  Name                      Default RD          Interfaces
  IPI                                             Vlan1
```

4.1.15 shutdown

Command: shutdown
no shutdown
Function: Shut down the specified VLAN interface of the switch. The no operation of the command will enable the VLAN interface.
Command Mode: VLAN Interface Configuration Mode.
Default: The VLAN interface is enabled by default.
Usage Guide: While shutting down the VLAN interface of the switch, it will not send data frames.

If this interface needs to obtain an IP address via BOOTP/DHCP protocol, it should be enabled.
Example: Enable the VLAN1 interface of the switch.
Switch(Config-if-Vlan1)#no shutdown

4.2 Network management port

4.2.1 duplex

Command: bandwidth <bandwidth>
no bandwidth
Function: Configure the bandwidth for Interface vlan. The 'no bandwidth' command recovery the default value. The bandwidth of interface vlan is used to protocol account but not control the bandwidth of port. For instance, it is use the interface bandwidth（cost=10^8/bandwidth）when OSPF account the link cost, so change the bandwidth can result in OSPF link cost changed.
Parameters: <*bandwidth*> is the bandwidth for interface vlan. Range from 1bits to 10000000000 bits. It is can use unit 'k, m, g'. There are no decimal numbers after conversion.
Command mode: VLAN Interface Mode
Default: The default bandwidth for interface VLAN is 100,000,000bit.
Usage Guide: This command only can be used at interface VLAN mode. The conversion of unit: 1g=1,000m=1,000,000k=1,000,000,000bit.
Example: Configure the bandwidth for vlan1 is 50,000,000bit.
Switch(Config-if-Vlan1)#bandwidth 50m

4.2.2 interface ethernet

Command: interface ethernet <interface-name>
Function: Enter network management port configuration mode from global configuration mode.
Parameters:< Interface name>is the port number, set to 0.
Command mode: Global configuration mode.
Usage guide: Use the command 'exit' to return from network management port configuration mode to global configuration mode.
Example: Enter the network management port.
Switch(config)#interface ethernet 0
Switch(Config-If-Ethernet0)#

4.2.3 ip address

Command: ip address <ip-address> <mask>
no ip address [<ip-address> <mask>]
Function: Set the IP address and mask of the switch; The 'no' operation of this command is to delete the IP address configuration.

Parameters:< Ip address>is the IP address, in dotted decimal format< Mask>is a subnet mask in dotted decimal format.
Command mode: Network management port configuration mode.
Default situation: The system does not have an IP address configuration by default.
Usage guide: This command is used to configure the IP address on the network management port.
For example, the IP address of the network management port is set to 192.168.1.10/24.
Switch(Config-If-Ethernet0)#ip address 192.168.1.10 255.255.255.0

4.2.4 shutdown

Command: shutdown
no shutdown
Function: Close the network management port; The 'no' operation of this command is to open the port.
Command mode: Network management port configuration mode.
Default situation: The network management port is set to open by default.
Usage guide: When the network management port is closed, it will not send data frames and the port status will be displayed as down when the user inputs the show interface command.
Example: Open the network management port.
Switch(config)#interface ethernet 0
Switch(Config-If-Ethernet0)#no shutdown

4.2.5 speed

Command: bandwidth <bandwidth>
no bandwidth
Function: Configure the bandwidth for Interface vlan. The 'no bandwidth' command recovery the default value. The bandwidth of interface vlan is used to protocol account but not control the bandwidth of port. For instance, it is use the interface bandwidth（cost=10^8/bandwidth）when OSPF account the link cost, so change the bandwidth can result in OSPF link cost changed.
Parameters: <*bandwidth*> is the bandwidth for interface vlan. Range from 1bits to 10000000000 bits. It is can use unit 'k, m, g'. There are no decimal numbers after conversion.
Command mode: VLAN Interface Mode
Default: The default bandwidth for interface VLAN is 100,000,000bit.
Usage Guide: This command only can be used at interface VLAN mode. The conversion of unit: 1g=1,000m=1,000,000k=1,000,000,000bit.
Example: Configure the bandwidth for vlan1 is 50,000,000bit.
Switch(Config-if-Vlan1)#bandwidth 50m

4.3 IP Configuration

4.3.1 clear ip traffic

Command: clear ip traffic

Function: Clear the statistic information of IP protocol.

Parameter: None.

Command mode: Admin Mode.

Default: None.

Usage guide: Clear the statistic information of receiving and sending packets for IP kernel protocol, including the statistic of receiving packets, sending packets and dropping packets and the error information of receiving and sending packets for IP protocol, ICMP protocol, TCP protocol and UDP protocol.

Example: Clear statistic information of IP protocol.

Switch#clear ip traffic

4.3.2 clear ipv6 neighbor

Command: clear ipv6 neighbors

Function: Clear the neighbor cache of IPv6.

Parameter: None

Command Mode: Admin Mode

Default: None

Usage Guide: This command can not clear static neighbor.

Example: Clear neighbor list.

Switch#clear ipv6 neighbors

4.3.3 debug ip icmp

Command: debug ip icmp

no debug ip icmp

Function: The debugging for receiving and sending ICMP packets.

Parameter: None.

Default: None.

Command mode: Admin Mode

Usage Guide: None.

Example:

Switch#debug ip icmp

IP ICMP: sent, type 8, src 0.0.0.0, dst 20.1.1.1

Display	Description
IP ICMP: sent	Send ICMP packets
type 8	Type is 8（PING request）

src 0.0.0.0	Source IPv4 address
dst 20.1.1.1	Destination IPv4 address

4.3.4 debug ip packet

Command: debug ip packet

no debug ip packet

Function: Enable the IP packet debug function: the "**no debug IP packet**" command disables this debug function.

Parameter: None

Default: IP packet debugging information is disabled by default.

Command mode: Admin Mode

Usage Guide: Displays statistics for IP packets received/sent, including source/destination address and bytes, etc.

Example: Enable IP packet debug.

Switch #debug ip packet

IP PACKET: sent, src 200.1.1.35, dst 224.0.0.9, size 312, proto 17, vrf 0

IP PACKET: rcvd, src 101.1.1.1, dst 224.0.0.9, size 312, proto 17, from Vlan200, vrf 0

4.3.5 debug ipv6 packet

Command: debug ipv6 packet

no debug ipv6 packet

Function: IPv6 data packets receive/send debug message.

Parameter: None

Default: None

Command Mode: Admin Mode

Usage Guide:

Example:

Switch#debug ipv6 packet

IPv6 PACKET: rcvd, src <fe80::203:fff:fe01:2786>, dst <fe80::1>, size <64>, proto <58>, from Vlan1

Displayed information	Explanation
IPv6 PACKET: rcvd	Receive IPv6 data report
Src <fe80::203:fff:fe01:2786>	Source IPv6 address
Dst <fe80::1>	Destination IPv6 address
size <64>	Size of data report
proto <58>	Protocol field in IPv6 header
from Vlan1	IPv6 data report is collected from Layer 3 port vlan1

4.3.6 debug ipv6 icmp

Command: debug ipv6 icmp

no debug ipv6 icmp

Function: ICMP data packets receive/send debug message.

Parameter: None

Default: None

Command Mode: Admin Mode

Usage Guide: None

Example:

Switch#debug ipv6 icmp

IPv6 ICMP: sent, type <129>, src <2003::1>, dst <2003::20a:ebff:fe26:8a49> from Vlan1

Displayed information	Explanation
IPv6 ICMP: sent	Send IPv6 data report
type <129>	Ping protocol No.
Src <2003::1>	Source IPv6 address
Dst <2003::20a:ebff:fe26:8a49>	Destination IPv6 address
from Vlan1	Layer 3 port being sent

4.3.7 debug ipv6 nd

Command: debug ipv6 nd [ns | na | rs | ra | redirect]

no debug ipv6 nd [ns | na | rs | ra | redirect]

Function: Enable the debug of receiving and sending operations for specified types of IPv6 ND messages. The ns, na, rs, ra and redirect parameters represent neighbor solicitation, neighbor advertisement, route solicitation, route advertisement and route redirect. No specification means to enable the debug for all five types of ND message. The no operation of this command will disable debug of receiving and sending operations for specified types of IPv6 ND messages, while no specification means to disable that for all five types of ND message.

Parameter: None.

Default: The debug of receiving and sending operations for all five types of IPv6 ND messages is disabled by default.

Command Mode: Admin Mode

Usage Guide: The ND protocol is an essential part of IPv6. This command can display the ND message of a specified type for troubleshooting.

Example:

Switch#debug ipv6 nd

IPv6 ND: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

Displayed information	Explanation
IPv6 ND: rcvd	Receive ND data report

type <136>	ND Type
src <fe80::203:fff:fe01:2786>	Source IPv6 address
dst <fe80::203:fff:fe01:59ba>	Destination IPv6 address

4.3.8 debug ipv6 tunnel packet

Command: debug ipv6 tunnel packet

no debug ipv6 tunnel packet

Function: tunnel data packets receive/send debug message.

Parameter: None

Default: None

Command Mode: Admin Mode

Usage Guide: None

Example:

Switch#debug ipv6 tunnel packet

IPv6 tunnel: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

IPv6 tunnel packet : rcvd src 178.1.1.1 dst 179.2.2.2 size 128 from tunnel1

Displayed information	Explanation
IPv6 tunnel packet : rcvd	Receive tunnel data report
type <136>	ND type
src 178.1.1.1 dst	Tunnel source IPv4 address
dst 179.2.2.2	Tunnel destination IPv4 address

4.3.9 description

Command: description <*desc*>

no description

Function: Configure the tunnel description. The no operation of this command will delete the tunnel description.

Parameters: <*desc*> is the tunnel description, its length can not exceed 256 characters.

Command Mode: Tunnel Configuration Mode.

Default: There is no tunnel description by default.

Usage Guide: When there is more than one tunnel in the system, configuring description will help user with identifying the purposes of different tunnels.

Examples: Set the tunnel description as toCernet2.

Switch(Config-if-Tunnel1)#description toCernet2

4.3.10 ip address

Command: ip address <*ip-address*> <*mask*> [secondary]

no ip address [*<ip-address> <mask>*] [secondary]

Function: Set IP address and net mask of switch; the "**no ip address [*<ip-address> <mask>*] [secondary]**" command deletes the IP address configuration.

Parameter: ***<ip-address>*** is IP address, dotted decimal notation; ***<mask>*** is subnet mask, dotted decimal notation; **[secondary]** indicates that the IP address is configured as secondary IP address.

Command Mode: VLAN interface configuration mode

Default: The system default is no IP address configuration.

Usage Guide: This command configures IP address on VLAN interface manually. If optional parameter **secondary** is not configured, then it is configured as the primary IP address of VLAN interface; if optional parameter **secondary** is configured, then that means the IP address is the secondary IP address of VLAN. One VLAN interface can only have one primary IP address and more than one secondary IP addresses. Primary IP and Secondary IP all can be used on SNMP/Web/Telnet management. Furthermore, the switch also provides BOOTP/DHCP manner to get IP address.

Example: The IP address of switch VLAN1 interface is set to 192.168.1.10/24.

Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0

4.3.11 ip default-gateway

This command is not supported by the switch.

4.3.12 ip route

This command is not supported by the switch.

4.3.13 ipv6 address

Command: ipv6 address *<ipv6-address|prefix-length>* [eui-64]

no ipv6 address *<ipv6-address|prefix-length>* [eui-64]

Function: Configure aggregately global unicast address, site-local address and link-local address for the interface.

Parameter: Parameter ***<ipv6-address>*** is the prefix of IPv6 address, parameter ***<prefix-length>*** is the prefix length of IPv6 address, which is between 3-128, **eui-64** means IPv6 address is generated automatically based on eui64 interface identifier of the interface.

Command Mode: Interface Configuration Mode.

Default: None.

Usage Guide: IPv6 address prefix can not be multicast address or any other specific IPv6 address, and different layer 3 interfaces can not configure the same address prefix. For global unicast address, the length of the prefix must be greater than or equal to 3. For site-local address and link-local address, the length of the prefix must be greater than or equal to 10. For interface loopback port, the length of the prefix must be equaled to 128.

Example: Configure an IPv6 address on VLAN1 Layer 3 interface: the prefix is 2001:3f:ed8::99 and the length of the prefix is 64.

Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64

4.3.14 ipv6 default-gateway

This command is not supported by the switch.

4.3.15 ipv6 route

Command: ipv6 route <*ipv6-prefix | prefix-length*> **{<*ipv6address*> | <*interface-type interface-number*> | {<*ipv6address*> <*interface-type interface-number*>} | tunnel <*tunnel no*> } [<*precedence*>]**

no ipv6 route <*ipv6-prefix | prefix-length*> {<*ipv6address*> | <*interface-type interface-number*> | {<*ipv6address*> <*interface-type interface-number*>} | tunnel <*tunnel no*> } [<*precedence*>]

Function: Set IPv6 static route.

Parameters: Parameter ***<ipv6-prefix>*** is the destination prefix of IPv6 static route, parameter ***<prefix-length>*** is the length of IPv6 prefix, parameter ***<ipv6-address>*** is the next hop IPv6 address of the reachable network, parameter ***<interface-type interface-number>*** is the name of interface from which to reach the destination, ***<tunnel no>*** is the output tunnel number of the tunnel route, parameter ***<precedence>*** is the weight of this route, the range is 1-255, the default is 1

Default: There is not any IPv6 static route which is configured by default.

Command Mode: Global Mode

Usage Guide: When the next hop IPv6 address is link-local address, the interface name must be specified. When the next hop IPv6 address is global aggregatable unicast address and site-local address, if no interface name of the exit is specified, it must be assured that the IP address of the next hop and the address of some interface of the switch must be in the same network segment. As for tunnel route, interface name can be directly specified.

Example: Configure static route 1 with destination address 3ffe:589:dfc::88, prefix length 64 and next hop 2001:8fd:c32::99 (the router has been configured IPv6 address of 2001:8fd:c32::34/64).

Switch(config)#ipv6 route 3ffe:589:dfc::88/64 2001:8fd:c32::99

Configure static route 2 with destination 3ffe:ff7:123::55, prefix length 64, next hop fe80::203:ff:89fd:46ac and exit interface name Vlan1.

Switch(config)#ipv6 route 3ffe:ff7:123::55/64 fe80::203:ff:89fd:46ac Vlan1

4.3.16 ipv6 redirect

Command: ipv6 redirect

no ipv6 redirect

Function: Enable IPv6 router redirect function. The no operation of this command will disable the function.

Parameters: None.

Command Mode: Global Configuration Mode.

Default Settings: IPv6 router redirect function is disabled by default.

Usage Guide: If router A, router B, and node C are on the same network link, and router A forwards IPv6 packets from node C to router B, expecting router B to continue the forwarding, then router A will send an IPv6 ICMPv6 redirect message to node C-source of the packet, notifying it that the best next hop of this destination address is router B. By doing so, the forwarding overhead of router A will be decreased, so is the network transmission delay of node C.

Examples: Enable IPv6 router redirect function.

Switch(config)# ipv6 redirect

4.3.17 ipv6 nd dad attempts

Command: ipv6 nd dad attempts *<value>*

no ipv6 nd dad attempts

Function: Set Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection.

Parameter: <*value*> is the Neighbor Solicitation Message number sent in succession by Duplicate Address Detection, and the value of **<*value*>** must be in 0-10, NO command restores to default value 1.

Command Mode: Interface Configuration Mode

Default: The default request message number is 1.

Usage Guide: When configuring an IPv6 address, it is required to process IPv6 Duplicate Address Detection, this command is used to configure the ND message number of Duplicate Address Detection to be sent, *value* being 0 means no Duplicate Address Detection is executed.

Example: The Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection is 3.

Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3

4.3.18 ipv6 nd ns-interval

Command: ipv6 nd ns-interval *<seconds>*

no ipv6 nd ns-interval

Function: Set the time interval of Neighbor Solicitation Message sent by the interface.

Parameter: parameter **<*seconds*>** is the time interval of sending Neighbor Solicitation Message, **<*seconds*>** value must be between 1-3600 seconds, **no** command restores the default value 1 second.

Command Mode: Interface Configuration Mode

Default: The default Request Message time interval is 1 second.

Usage Guide: The value to be set will include the situation in all routing announcement on the interface. Generally, very short time interval is not recommended.

Example: Set Vlan1 interface to send out Neighbor Solicitation Message time interval to be 8 seconds.

Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8

4.3.19 ipv6 nd suppress-ra

Command: ipv6 nd suppress-ra
no ipv6 nd suppress-ra
Function: Prohibit router announcement.
Parameter: None
Command Mode: Interface Configuration Mode
Default: Router Announcement function is disabled.
Usage Guide: no ipv6 nd suppress-ra command enable router announcement function.
Example: Enable router announcement function.
Switch(Config-if-Vlan1)#no ipv6 nd suppress-ra

4.3.20 ipv6 nd ra-lifetime

Command: ipv6 nd ra-lifetime <*seconds*>
no ipv6 **nd ra-lifetime**
Function: Configure the lifetime of router announcement.
Parameter: parameter ***<seconds>*** stands for the number of seconds of router announcement lifetime, ***<seconds>*** value must be between 0-9000.
Command Mode: Interface Configuration Mode
Default: The number of seconds of router default announcement lifetime is 1800.
Usage Guide: This command is used to configure the lifetime of the router on Layer 3 interface, seconds being 0 means this interface can not be used for default router, otherwise the value should not be smaller than the maximum time interval of sending router announcement. If no configuration is made, this value is equal to 3 times of the maximum time interval of sending routing announcement.
Example: Set the lifetime of routing announcement is 100 seconds.
Switch(Config-if-Vlan1)#ipv6 nd ra-lifetime 100

4.3.21 ipv6 nd min-ra-interval

Command: ipv6 nd min-ra-interval <*seconds*>
no ipv6 **nd min-ra-interval**
Function: Set the minimum time interval of sending routing message.
Parameter: Parameter ***<seconds>*** is number of seconds of the minimum time interval of sending routing announcement, ***<seconds>*** must be between 3-1350 seconds.
Command Mode: Interface Configuration Mode
Default: The default minimum time interval of sending routing announcement is 200 seconds.
Usage Guide: The minimum time interval of routing announcement should not exceed 3/4 of the maximum time interval.
Example: Set the minimum time interval of sending routing announcement is 10 seconds.

Switch(Config-if-Vlan1)#ipv6 nd min-ra-interval 10

4.3.22 ipv6 nd max-ra-interval

Command: ipv6 nd max-ra-interval <*seconds*>
no ipv6 **nd max-ra-interval**
Function: Set the maximum time interval of sending routing message.
Parameter: Parameter ***<seconds>*** is number of seconds of the time interval of sending routing announcement, ***<seconds>*** must be between 4-1800 seconds.
Command Mode: Interface Configuration Mode
Default: The default maximum time interval of sending routing announcement is 600 seconds.
Usage Guide: The maximum time interval of routing announcement should be smaller than the lifetime value routing announcement.
Example: Set the maximum time interval of sending routing announcement is 20 seconds.
Switch(Config-if-Vlan1)#ipv6 nd max-ra-interval 20

4.3.23 ipv6 nd prefix

Command: ipv6 nd prefix <ipv6-prefix | prefix-length>{ [<valid-lifetime> <preferred-lifetime>] [no-autoconfig | off-link[no-autoconfig]]}
no ipv6 nd prefix <ipv6-prefix | prefix-length>
Function: Configure the address prefix and relative parameters for router announcement.
Parameter: Parameter <ipv6-prefix> is the address prefix of the specified announcement, parameter <prefix-length> is the length of the address prefix of the specified announcement, parameter <valid-lifetime> is the valid lifetime of the prefix, parameter <preferred-lifetime> is the preferred lifetime of the prefix, and the valid lifetime must be no smaller than preferred lifetime. Parameter no-autoconfig says this prefix can not be used to automatically configure IPv6 address on the host in link-local. Parameter off-link says the prefix specified by router announcement message is not assigned to link-local, the node which sends data to the address including this prefix consider link-local as unreachable.
Command Mode: Interface Configuration Mode
Default: The default value of valid-lifetime is 2592000 seconds (30 days), the default value of preferred-lifetime is 604800 seconds (7 days). off-link is off by default, no-autoconfig is off by default.
Usage Guide: This command allows controlling the router announcement parameters of every IPv6 prefix. Note that valid lifetime and preferred lifetime must be configured simultaneously.
Example: Configure IPv6 announcement prefix as 2001:410:0:1::/64 on Vlan1, the valid lifetime of this prefix is 8640 seconds, and its preferred lifetime is 4320 seconds.
Switch(Config-if-Vlan1)#ipv6 nd prefix 2001:410:0:1::/64 8640 4320

4.3.24 ipv6 nd ra-hoplimit

Command: ipv6 nd ra-hoplimit <value>
Function: Set the hoplimit of sending router advertisement.
Parameters: <value> is the hoplimit of sending router advertisement, ranging from 0 to 255.
Command Mode：Interface Configuration Mode.
Default: The default hoplimit of sending router advertisement is 64.
Example: Set the hoplimit of sending router advertisement in interface vlan 1 as 128.
Switch#(Config-if-Vlan1)#ipv6 nd ra-hoplimit 128

4.3.25 ipv6 nd ra-mtu

Command: ipv6 nd ra-mtu <value>
Function: Set the mtu of sending router advertisement.
Parameters: <value> is the mtu of sending router advertisement, ranging from 0 to 1500.
Command Mode：Interface Configuration Mode.
Default: The default mtu of sending router advertisement is 1500.
Example: Set the mtu of sending router advertisement in interface vlan 1 as 500.
Switch#(Config-if-Vlan1)#ipv6 nd ra-mtu 500

4.3.26 ipv6 nd reachable-time

Command: ipv6 nd reachable-time <seconds>
Function: Set the reachable-time of sending router advertisement.
Parameters: <value> is the reachable-time of sending router advertisement, ranging from 0 to 3600000 milliseconds.
Command Mode: Interface Configuration Mode.
Default Settings: The default reachable-time of sending router advertisement is 30000 milliseconds.
Example: Set the reachable-time of sending router advertisement in interface vlan 1 as 100000 milliseconds.
Switch(Config-if-Vlan1)#ipv6 nd reachable-time 100000

4.3.27 ipv6 nd retrans-timer

Command: ipv6 nd retrans-timer <seconds>
Function**:** Set the retrans-timer of sending router advertisement.
Parameters: <value> is the retrans-timer of sending router advertisement, ranging from 0 to 4294967295 milliseconds.
Command Mode: Interface Configuration Mode.
Default: The default retrans-timer of sending router advertisement is 1000 milliseconds.
Example: Set the reachable-time of sending router advertisement in interface vlan 1 as 10000

milliseconds.
Switch(Config-if-Vlan1)#ipv6 nd retrans-timer 10000

4.3.28 ipv6 nd other-config-flag

Command: ipv6 nd other-config-flag
Function: Set the flag representing whether information other than the address information will be obtained via DHCPv6.
Parameters: None.
Command Mode: Interface Configuration Mode.
Default: Information other than the address information won't be obtained via DHCPv6.
Examples: Set IPv6 information other than the address information in interface vlan 1 will be obtained via DHCPv6.
Switch(Config-if-Vlan1)#ipv6 nd other-config-flag

4.3.29 ipv6 nd managed-config-flag

Command: ipv6 nd managed-config-flag
Function: Set the flag representing whether the address information will be obtained via DHCPv6.
Parameters: None.
Command Mode: Interface Configuration Mode.
Default: The address information won't be obtained via DHCPv6.
Examples: Set IPv6 address information in interface vlan 1 will be obtained via DHCPv6.
Switch(Config-if-Vlan1)#ipv6 nd managed-config-flag

4.3.30 ipv6 neighbor

Command: ipv6 neighbor *<ipv6-address>* *<hardware-address>* interface *<interface-type interface-name>*

no ipv6 neighbor *<ipv6-address>*

Function: Set static neighbor table entry.
Parameters: Parameter ***ipv6-address*** is static neighbor IPv6 address, same to interface prefix parameter, parameter ***hardware-address*** is static neighbor hardware address, ***interface-type*** is Ethernet type, ***interface-name*** is Layer 2 interface name.
Command Mode: Interface Configuration Mode
Default Situation: There is not static neighbor table entry.
Usage Guide: IPv6 address and multicast address for specific purpose and local address can not be set as neighbor.
Example: Set static neighbor 2001:1:2::4 on port E1/0/1, and the hardware MAC address is 00-03-0f-89-44-bc.
Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet 1/0/1

4.3.31 interface tunnel

Command: interface tunnel *<tnl-id>*
no interface **tunnel *<tnl-id>***
Function: Create/Delete tunnel.
Parameter: Parameter <tnl-id> is tunnel No.
Command Mode: Global Mode.
Default: None.
Usage Guide: This command creates a virtual tunnel interface. Since there is not information such as specific tunnel mode and tunnel source, ***show ipv6 tunnel*** does not show the tunnel, enter tunnel mode after creating, under that model information such as tunnel source and destination can be specified. No command deletes a tunnel.
Example: Create tunnel 1.
Switch(Config)#interface tunnel 1

4.3.32 show ip interface

Command: show ip interface [*<ifname>* | vlan *<vlan-id>*] brief
Function: Show the brief information of the configured layer 3 interface.
Parameters: ***<ifname>*** Interface name; ***<vlan-id>*** VLAN ID.
Default: Show all brief information of the configured layer 3 interface when no parameter is specified.
Command mode: All modes.
Usage Guide: None.
Example:
Restarter#show ip interface vlan1 brief

Index	Interface	IP-Address	Protocol
3001	Vlan1	192.168.2.11	up

4.3.33 show ip traffic

Command: show ip traffic
Function: Display statistics for IP packets.
Command mode: Admin Mode
Usage Guide: Display statistics for IP, ICMP, TCP, UDP packets received/sent.
Example:
Switch#show ip traffic
IP statistics:
Rcvd: 3249810 total, 3180 local destination
0 header errors, 0 address errors
0 unknownnnnn protocol, 0 discards
Frags: 0 reassembled, 0 timeouts

```
        0 fragment rcvd, 0 fragment dropped
        0 fragmented, 0 couldn't fragment, 0 fragment sent
Sent:   0 generated, 3230439 forwarded
         0 dropped, 0 no route
ICMP statistics:
Rcvd:  0 total 0 errors 0 time exceeded
        0 redirects, 0 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
Sent:   0 total 0 errors 0 time exceeded
        0 redirects, 0 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
TcpActiveOpens          0, TcpAttemptFails      0
TcpCurrEstab            0, TcpEstabResets       0
TcpInErrs               0, TcpInSegs            3180
TcpMaxConn              0, TcpOutRsts           3
TcpOutSegs              0, TcpPassiveOpens      8
TcpRetransSegs          0, TcpRtoAlgorithm      0
TcpRtoMax               0, TcpRtoMin            0
UDP statics:
UdpInDatagrams          0, UdpInErrors          0
UdpNoPorts              0, UdpOutDatagrams      0
```

Displayed information	Explanation
IP statistics：	IP packet statistics.
Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknownnnnn protocol, 0 discards	Statistics of total packets received, number of packets reached local destination, number of packets have header errors, number of erroneous addresses, number of packets of unknownnnnn protocols; number of packets dropped.
Frags： 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Fragmentation statistics: number of packets reassembled, timeouts, fragments received, fragments discarded, packets that cannot be fragmented, number of fragments sent, etc.
Sent： 0 generated, 0 forwarded 0 dropped, 0 no route	Statistics for total packets sent, including number of local packets, forwarded packets, dropped packets and packets without route.

ICMP statistics：	ICMP packet statistics.
Rcvd： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets received and classified information
Sent： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets sent and classified information
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.

4.3.34 show ipv6 interface

Command: show ipv6 interface {brief|*<interface-name>*}

Function: Show interface IPv6 parameters.

Parameter: Parameter brief is the brief summarization of IPv6 status and configuration, and parameter interface-name is Layer 3 interface name.

Default: None

Command Mode: Admin and Configuration Mode

Usage Guide: If only brief is specified, then information of all L3 is displayed, and you can also specify a specific Layer 3 interface.

Example:

Switch#show ipv6 interface Vlan1
Vlan1 is up, line protocol is up, dev index is 2004
Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST)
IPv6 is enabled
Link-local address(es):
fe80::203:fff:fe00:10 PERMANENT
Global unicast address(es):
3001::1 subnet is 3001::1/64 PERMANENT
Joined group address(es):
ff02::1
ff02::16
ff02::2
ff02::5
ff02::6
ff02::9

ff02::d
ff02::1:ff00:10
ff02::1:ff00:1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts is 1
ND managed_config_flag is unset
ND other_config_flag is unset
ND NS interval is 1 second(s)
ND router advertisements is disabled
ND RA min-interval is 200 second(s)
ND RA max-interval is 600 second(s)
ND RA hoplimit is 64
ND RA lifetime is 1800 second(s)
ND RA MTU is 0
ND advertised reachable time is 0 millisecond(s)
ND advertised retransmit time is 0 millisecond(s)

Displayed information	Explanation
Vlan1	Layer 3 interface name
[up/up]	Layer 3 interface status
dev index	Internal index No.
fe80::203:fff:fe00:10	Automatically configured IPv6 address of Layer 3 interface
3001::1	Configured IPv6 address of Layer 3 interface

4.3.35 show ipv6 route

Command: show ipv6 route [<destination>|<*destination* >|<*length*>/ database| fib [local]| nsm [connected | static | rip| ospf | bgp | isis| kernel| database]|statistics]
Function: Display IPv6 routing table.
Parameter: <destination> is destination network address; **<*destination*>|<*length*>** is destination network address plus prefix length; **connected** is directly connected router; **static** is static router; **rip** is RIP router; **ospf** is OSPF router; **bgp** is BGP router; **isis** is ISIS router; **kernel** is kernel router; **statistics** shows router number; **database** is router database.
Default Situation: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: show ipv6 route only shows IPv6 kernal routing table (routing table in tcpip), database shows all routers except the local router, fib local shows the local router, statistics shows router statistics information.
Example:
Switch#show ipv6 route
Codes: C - connected, L - Local, S - static, R - RIP, O - OSPF,

```
I - IS-IS, B - BGP
C       ::/0        via ::,     tunnel3     256
S       2001:2::/32         via fe80::789,      Vlan2       1024
S       2001:2:3:4::/64         via fe80::123,      Vlan2       1024
O       2002:ca60:c801:1::/64       via ::,     Vlan1       1024
C       2002:ca60:c802:1::/64       via ::,     tunnel49        256
C       2003:1::/64         via ::,     Vlan4       256
C       2003:1::5efe:0:0/96         via ::,     tunnel26        256
S       2004:1:2:3::/64         via fe80:1::88,     Vlan2       1024
O       2006:1::/64         via ::,     Vlan1       1024
S       2008:1:2:3::/64         via fe80::250:baff:fef2:a4f4,       Vlan1       1024
C       2008:2005:5:8::/64          via ::,     Ethernet0       256
S       2009:1::/64         via fe80::250:baff:fef2:a4f4,       Vlan1       1024
C       2022:1::/64         via ::,     Ethernet0       256
O       3333:1:2:3::/64         via fe80::20c:ceff:fe13:eac1,       Vlan12      1024
C       3ffe:501:ffff:1::/64        via ::,     Vlan4       256
O       3ffe:501:ffff:100::/64          via ::,     Vlan5       1024
O       3ffe:3240:800d:1::/64           via ::,     Vlan1       1024
O       3ffe:3240:800d:2::/64           via ::,     Vlan2       1024
O       3ffe:3240:800d:10::/64          via ::,     Vlan12      1024
O       3ffe:3240:800d:20::/64          via fe80::20c:ceff:fe13:eac1,       Vlan12      1024
C       fe80::/64       via ::,     Vlan1       256
C       fe80::5efe:0:0/96           via ::,     tunnel26        256
C       ff00::/8        via ::,     Vlan1       256
```

Displayed information	Explanation
IPv6 Routing Table	IPv6 routing table status
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,I - IS-IS, B - BGP > - selected route, * - FIB route, p - stale info	Abbreviation display sign of every entry
S 2009:1::/64 via fe80::250:baff:fef2:a4f4, Vlan1 1024	The static router in FIB table, of which the destination network segment is 2002::/64, via means passing fe80::250:baff:fef2:a4f4 is the next hop, VLAN1 is the exit interface name, 1024 is router weight.

4.3.36 show ipv6 neighbors

Command: show ipv6 neighbors [{vlan|ethernet|tunnel } interface-number | interface-name | address *<ipv6address>*]

Function: Display neighbor table entry information.

Parameter: Parameter {vlan|ethernet|tunnel} interface-number**/**interface-name specify the lookup based on interface. **Parameter** ipv6-address specifies the lookup based on IPv6 address. It displays the whole neighbor table entry if without **parameter**.

Default Situation: None

Command Mode: Admin and Configuration Mode

Usage Guide:

Example:

Switch#show ipv6 neighbors

IPv6 neighbour unicast items: 14, valid: 11, matched: 11, incomplete: 0, delayed: 0, manage items 5

IPv6 Address Hardware Addr Interface Port State

2002:ca60:c801:1:250:baff:fef2:a4f4 00-50-ba-f2-a4-f4 Vlan1 Ethernet1/0/2 reachable

3ffe:3240:800d:1::100 00-03-0f-01-27-86 Vlan1 Ethernet1/0/3 reachable

3ffe:3240:800d:1::8888 00-02-01-00-00-00 Vlan1 Ethernet1/0/1 permanent

3ffe:3240:800d:1:250:baff:fef2:a4f4 00-50-ba-f2-a4-f4 Vlan1 Ethernet1/0/4 reachable

3ffe:3240:800d:2::8888 00-02-01-00-01-01 Vlan2 Ethernet1/0/16 permanent

3ffe:3240:800d:2:203:fff:fefe:3045 00-03-0f-fe-30-45 Vlan2 Ethernet1/0/15 reachable

fe80::203:fff:fe01:2786 00-03-0f-01-27-86 Vlan1 Ethernet1/0/5 reachable

fe80::203:fff:fefe:3045 00-03-0f-fe-30-45 Vlan2 Ethernet1/0/17 reachable

fe80::20c:ceff:fe13:eac1 00-0c-ce-13-ea-c1 Vlan12 Ethernet1/0/20 reachable

fe80::250:baff:fef2:a4f4 00-50-ba-f2-a4-f4 Vlan1 Ethernet1/0/6 reachable

IPv6 neighbour table: 11 entries

Displayed information	Explanation
IPv6 Addres	Neighbor IPv6 address
Hardware Addr	Neighbor MAC address
Interface	Exit interface name
Port	Exit interface name
State	Neighbor status (reachable、statle、delay、probe、permanent、incomplete、unknownnnn)

4.3.37 show ipv6 traffic

Command: show ipv6 traffic

Function: Display IPv6 transmission data packets statistics information.

Parameter: None

Default: None

Command Mode: Admin and Configuration Mode

Example:

Switch#show ipv6 traffic

IP statistics:

Rcvd: 90 total, 17 local destination

0 header errors, 0 address errors

0 unknownnnnn protocol, 13 discards

Frags: 0 reassembled, 0 timeouts

0 fragment rcvd, 0 fragment dropped

0 fragmented, 0 couldn't fragment, 0 fragment sent

Sent: 110 generated, 0 forwarded

0 dropped, 0 no route

ICMP statistics:

Rcvd: 0 total 0 errors 0 time exceeded

0 redirects, 0 unreachable, 0 echo, 0 echo replies

Displayed information	Explanation
IP statistics	IPv6 data report statistics
Rcvd: 90 total, 17 local destination0 header errors, 0 address errors0 unknownnnnn protocol, 13 discards	IPv6 received packets statistics
Frags: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped0 fragmented, 0 couldn't fragment, 0 fragment sent	IPv6 fragmenting statistics
Sent: 110 generated, 0 forwarded 0 dropped, 0 no route	IPv6 sent packets statistics

4.3.38 show ipv6 redirect

Command: show ipv6 redirect

Function: Display the state IPv6 redirect switch.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: This command can be used to check whether the IPv6 redirect function in the

system is enabled.

Examples:

Switch show ipv6 redirect

ipv6 redirect is disabled

4.3.39 show ipv6 tunnel

Command: show ipv6 tunnel [<*tnl-id*>]

Function: Display tunnel information.

Parameter: Parameter ***<tnl-id>*** is tunnel No.

Default Situation: None.

Command Mode: Admin Mode.

Usage Guide: If there is not tunnel number, then information of all tunnels are shown. If there is tunnel number, then the detailed information of specified tunnel is shown.

Example:

Switch#show ipv6 tunnel

name	mode	source	destination	nexthop
tunnel3	6to4	178.1.1.1		

Displayed information	Explanation
Name	Tunnel name
Mode	Tunnel type
Source	Tunnel source ipv4 address
Destination	Tunnel destination ipv4 address
Nexthop	Tunnel next hop (only applies to ISATAP tunnel)

4.3.40 tunnel source

Command: tunnel source {<ipaddress> | <ipv6address> **| *<interface-name>*}**

no tunnel source

Function: Configure the IPv4/IPv6 address of the tunnel source.

Parameter: ***<ipaddress>*** is the IPv4 address of tunnel source, must be the unicast address; ***<ipv6address>*** is the IPv6 address of tunnel source; ***<interface-name>*** means the tunnel source address is the IPv4 address of the interface ***<interface-name>***.

Command Mode: Tunnel Configuration Mode.

Default Situation: There is no IPv4/IPv6 address and interface name of tunnel source.

Usage Guide: Set the source IPv4/IPv6 address or specify an interface name of the tunnel source address to configure the tunnel.

Example: Configure tunnel source IPv4 address 202.89.176.6.

Switch(Config-if-Tunnel1)#tunnel source 202.89.176.6

4.3.41 tunnel destination

Command: tunnel destination <*ipaddress* | *ipv6address*>
no **tunnel destination**
Function: Configure the IPv4/IPv6 address of the tunnel destination.
Parameter: ***<ipaddress>*** is the IPv4 address of tunnel destination, ***<ipv6address>*** is the IPv6 address of tunnel destination.
Command Mode: Tunnel Configuration Mode.
Default Situation: There is no IPv4/IPv6 address of tunnel destination.
Usage Guide: This command is used to configure the IPv4/IPv6 address of tunnel destination.
Example: Configure tunnel destination 203.78.120.5.
Switch(Config-if-Tunnel1)#tunnel destination 203.78.120.5

4.3.42 tunnel nexthop

Command: tunnel nexthop <*ipaddress*>
no tunnel **nexthop**
Function: Configure tunnel nexthop.
Parameter: ***<ipaddress>*** is the IPv4 address of tunnel nexthop.
Command Mode: Tunnel Configuration Mode.
Default Situation: There is no IPv4 address of tunnel nexthop.
Usage Guide: This command is for ISATAP tunnel, other tunnels won't check the configuration of nexthop. Notice: IPv4 address of ISATAP tunnel nexthop and IPv4 address of tunnel source should be in same segment.
Example: Configure tunnel next hop 178.99.156.8.
Switch(Config-if-Tunnel1)#tunnel source 178.99.156.7
Switch(Config-if-Tunnel1)#tunnel nexthop 178.99.156.8
Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap

4.3.43 tunnel 6to4-relay

This command is not supported by the switch.

4.3.44 tunnel mode

Command: tunnel mode [[gre] | ipv6ip [6to4 | isatap]]
no tunnel mode
Function: Configure Tunnel Mode.
Parameter: gre is GRE tunnel.

Command Mode: Tunnel Configuration Mode.
Default: None.
Usage Guide: In configuring tunnel mode, only specifying ipv6ip indicates configuring tunnel. Ipv6ip 6to4 indicates it is 6to4 tunnel, ipv6ip isatap indicates it is ISATAP tunnel.
Example: Configure tunnel mode.
1、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip
2、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip 6to4
3、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap

4.4 IP Forwarding

4.4.1 ip fib optimize

Command: ip fib optimize
no ip fib optimize
Function: Enables the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.
Default: Optimized IP route aggregation algorithm is disabled by default.
Command mode: Global Mode.
Usage Guide: This command is used to optimize the aggregation algorithm: if the route table contains no default route, the next hop most frequently referred to will be used to construct a virtual default route to simplify the aggregation result. This method has the benefit of more effectively simplifying the aggregation result. However, while adding a virtual default route to the chip segment route table reduces CPU load, it may introduce unnecessary data stream to switches of the next hop. In fact, part of local switch CPU load is transferred to switches of the next hop.
Example: Disabling optimized IP route aggregation algorithm.
Switch(config)# no ip fib optimize

4.5 URPF

4.5.1 debug urpf

Command: debug urlf
No debug URPF function: Enable URPF debugging function and prompt an error when URPF rule installation fails.
Command mode: privileged mode.
Parameter: None.

Usage guide: None available.
give an example:
Switch#debug urpf

4.5.2 ip urpf enable

This command is not supported by the switch.

4.5.3 show urpf rule ipv4 num

This command is not supported by the switch.

4.5.4 show urpf rule ipv6 num

This command is not supported by the switch.

4.5.5 show urpf rule ipv4

This command is not supported by the switch.

4.5.6 show urpf rule ipv6

This command is not supported by the switch.

4.5.7 show urpf

Command: show urpf
Function: Display which interfaces have been enabled with URPF function.
Command Mode: Admin and Configuration Mode
Parameters: None
Usage Guide: None
Example:
Switch#show urpf

4.5.8 urpf enable

Command: urpf enable
no urpf enable
Function: Enable the global URPF function.
Parameters: None
Command mode: Global Mode
Default: The URPF protocol module is disabled by default.

Usage Guide: None
Example:
Switch(config)#urpf enable

4.6 ARP

4.6.1 arp

Command: arp <*ip_address*> <*mac_address*> {interface [ethernet] <*portName*>}
no arp <*ip_address*>
Function: Configures a static ARP entry; the "**no arp <*ip_address*>**" command deletes a ARP entry of the specified IP address.
Parameters: ***<ip_address>*** is the IP address, at the same field with interface address; ***<mac_address>*** is the MAC address; **ethernet** stands for Ethernet port; ***<portName>*** for the name of layer2 port.
Default: No static ARP entry is set by default.
Command mode: VLAN Interface Mode
Usage Guide: Static ARP entries can be configured in the switch.
Example: Configuring static ARP for interface VLAN1.
Switch(Config-if-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 interface eth 1/0/2

4.6.2 clear arp-cache

Command: clear arp-cache
Function: Clears ARP table.
Command mode: Admin Mode
Example:
Switch#clear arp-cache

4.6.3 clear arp traffic

Command: clear arp traffic
Function: Clear the statistic information of ARP messages of the switch. For box switches, this command will only clear statistics of APP messages received and sent from the current boardcard.
Command mode: Admin Mode
Example:
Switch#clear arp traffic

4.6.4 debug arp

Command: debug arp {receive|send|state}

no debug arp {receive|send|state}

Function: Enables the ARP debugging function; the "**no debug arp {receive|send|state}**" command disables this debugging function.

Parameter: receive the debugging-switch of receiving ARP packets of the switch; **send** the debugging-switch of sending ARP packets of the switch; **state** the debugging-switch of APR state changing of the switch.

Default: ARP debug is disabled by default.

Command mode: Admin Mode.

Usage Guide: Display contents for ARP packets received/sent, including type, source and destination address, etc.

Example: Enable ARP debugging.

Switch#debug arp receive

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

e%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

4.6.5 clear ip arp dynamic

Command: clear ip arp dynamic

Function: Clear all of dynamic ARP on interface.

Parameter: None

Command Mode: Interface Configuration

Usage Guide: This command will clear dynamic entries before binding ARP. Once implemented, this command will lose its effect.

Example:

Switch(Config-if-Vlan1)#clear ip arp dynamic

4.6.6 clear ipv6 nd dynamic

Command: clear ipv6 nd dynamic

Function: Clear all dynamic ND on interface.

Parameter: None

Command mode: Interface Configuration

Usage Guide: This command will clear dynamic entries before binding ND. Once implemented, this command will lose its effect.

Example:
Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

4.6.7 ip proxy-arp

Command: ip proxy-arp
no ip proxy-arp
Function: Enables proxy ARP for VLAN interface; the no command disables proxy ARP.
Default: Proxy ARP is disabled by default.
Command mode: VLAN Interface Mode
Usage Guide: When an ARP request is received on the layer 3 interface, requesting an IP address in the same IP segment of the interface but not the same physical network, and the proxy ARP interface has been enabled, the interface will reply to the ARP with its own MAC address and forward the actual packets received. Enabling this function allows machines to physically be separated but in the same IP segment and communicate via the proxy ARP interface as if in the same physical network. Proxy ARP will check the route table to determine whether the destination network is reachable before responding to the ARP request; ARP request will only be responded if the destination is reachable.
Note: the ARP request matching default route will not use proxy.
Example: Enable proxy ARP for VLAN 1.
Switch(Config-if-Vlan1)#ip proxy-arp

4.6.8 l3 hashselect

This command is not supported by the switch.

4.6.9 show arp

Command: show arp [<*ipaddress*>] [<*vlan-id*>] [<*hw-addr*>] [type {static | dynamic}] [count] [vrf word]
Function: Displays the ARP table.
Parameters: <*ipaddress*> is a specified IP address; **<*vlan-id*>** stands for the entry for the identifier of specified VLAN; **<*hw-addr*>** for entry of specified MAC address; **static** for static ARP entry; **dynamic** for dynamic ARP entry; **count** displays number of ARP entries; **word** is the specified vrf name.
Command mode: Admin Mode
Usage Guide: Displays the content of current ARP table such as IP address, MAC address, hardware type, interface name, etc.
Example:
Switch#show arp

ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed: 0, None: 0

Address	Hardware Addr	Interface	Port	Flag
50.1.1.6	00-0a-eb-51-51-38	Vlan50	Ethernet1/0/11	Dynamic
50.1.1.9	00-00-00-00-00-09	Vlan50	Ethernet1/0/1	Static
150.1.1.2	00-00-58-fc-48-9f	Vlan150	Ethernet1/0/4	Dynamic

Displayed information	Explanation
Total arp items	Total number of ARP entries.
Valid	ARP entry number matching the filter conditions and attributing the legality states.
Matched	ARP entry number matching the filter conditions.
Verifying	ARP entry number at verifying again validity for ARP.
InCompleted	ARP entry number have ARP request sent without ARP reply.
Failed	ARP entry number at failed state.
None	ARP entry number at begin-found state.
Address	IP address of ARP entries.
Hardware Address	MAC address of ARP entries.
Interface	Layer 3 interface corresponding to the ARP entry.
Port	Physical (Layer2) port corresponding to the ARP entry.
Flag	Describes whether ARP entry is dynamic or static.

4.6.10 show arp traffic

Command: show arp traffic

Function: Display the statistic information of ARP messages of the switch. For box switches, this command will only show statistics of APP messages received and sent from the current boardcard.

Command mode: Admin and Config Mode

Usage Guide: Display statistics information of received and sent APP messages.

Example:

Switch#show arp traffic

ARP statistics:

Rcvd: 10 request, 5 response

Sent: 5 request, 10 response

4.7 station movement

4.7.1 l3-station-move

This command is not supported on this model of switch.

4.8 Hardware Tunnel Capacity

4.8.1 hardware tunnel-capacity

Command: hardware tunnel-capacity *<size>*

no hardware tunnel-capacity

Function: Configure the maximum value of hardware tunnel-capacity, the no command restores the default value.

Parameter: <*size*> is the value of hardware tunnel-capacity, its range from 0 to 1024.

Default: 64.

Command Mode: Global mode

Usage Guide: This command is used to configured the maximum number of tunnel and MPLS forwarded by hardware. Increasing capacity will reduce hardware routing number supported by switch, vice versa.

Note: It needs to reset switch to enable the valid configuration.

Example: Configure that hardware tunnel-capacity supports the maximum value of 200.

Switch(config)#hardware tunnel-capacity 200

Set successfully！ Write and reload to take effect.

Switch(config)#exit

Switch#write

Switch#reload

4.9 ARP Scanning Prevention

4.9.1 anti-arpscan enable [ip|port]

Command: anti-arpscan enable [ip|port]

no anti-arpscan enable [ip|port]

Function: Globally enable ARP scanning prevention function; "**no anti-arpscan enable**" command globally disables ARP scanning prevention function.

Parameters: None.

Default Settings: Enable or disable ARP scanning prevention function based on ip or port in the

same time.

Command Mode: Global configuration mode

User Guide: When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.

Example: Enable the ARP scanning prevention function of the switch.

Switch(config)#anti-arpscan enable ip

4.9.2 anti-arpscan port-based threshold

Command: anti-arpscan port-based threshold *<threshold-value>*

no anti-arpscan port-based threshold

Function: Set the threshold of received messages of the port-based ARP scanning prevention. If the rate of received ARP messages exceeds the threshold, the port will be closed. The unit is packet/second. The “no anti-arpscan port-based threshold” command will reset the default value, 10 packets/second.

Parameters: rate threshold, ranging from 2 to 200.

Default Settings: 10 packets /second.

Command Mode: Global Configuration Mode.

User Guide: the threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.

Example: Set the threshold of port-based ARP scanning prevention as 10 packets /second.

Switch(config)#anti-arpscan port-based threshold 10

4.9.3 anti-arpscan ip-based threshold

Command: anti-arpscan ip-based threshold <threshold-value>

no anti-arpscan ip-based level1|level2 threshold

Function: Set the threshold of received messages of the IP-based ARP scanning prevention. By default the level-1 threshold is 4p/s.

Parameters: rate threshold, ranging from 1 to 200.

Default Settings: By default the level-1 threshold is 4p/s.

Command Mode: Global configuration mode

User Guide: The threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.

Example: Set the threshold of IP-based ARP scanning prevention as 6 packets/second.

Switch(Config)# anti-arpscan ip-based threshold 6

4.9.4 anti-arpscan trust

Command: anti-arpscan trust { port | supertrust-port | iptrust-port }

no anti-arpscan trust {port | supertrust-port | iptrust-port}

Function: Configure a port as a trusted port or a super trusted port;" **no anti-arpscan trust <port | supertrust-port>**"command will reset the port as an untrusted port.
Parameters: None.
Default Settings: By default all the ports are non- trustful.
Command Mode: Port configuration mode
User Guide: If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed, but the non- trustful IP of this port will still be checked. If a port is set as a super trusted port, then neither the port nor the IP of the port will be dealt with. If the port is already closed by ARP scanning prevention, it will be opened right after being set as a trusted port. If a port is set as a trusted IP port, then the IP will not be dealt with, but the port will be dealt with. If the IP is already closed by ARP scanning prevention, it will be opened right after being set as a trusted IP port.
When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.
Example: Set port ethernet 1/0/5 of the switch as a trusted port.
Switch(config)#in e1/0/5
Switch(Config-If-Ethernet1/0/5)# anti-arpscan trust port

4.9.5 anti-arpscan trust ip

Command: anti-arpscan trust ip *<ip-address>* [*<netmask>*]
no anti-arpscan trust ip *<ip-address>* [*<netmask>*]
Function: Configure trusted IP;" **no anti-arpscan trust ip *<ip-address>* [*<netmask>*]**"command reset the IP to non-trustful IP.
Parameters: *<ip-address>*: Configure trusted IP address; ***<netmask>*:** Net mask of the IP.
Default Settings: By default all the IP are non-trustful. Default mask is 255.255.255.255
Command Mode: Global configuration mode
User Guide: If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed. If the port is already closed by ARP scanning prevention, its traffic will be recovered right immediately.
Example: Set 192.168.1.0/24 as trusted IP.
Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0

4.9.6 anti-arpscan recovery enable

Command: anti-arpscan recovery enable
no anti-arpscan recovery enable
Function: Enable the automatic recovery function, "**no anti-arpscan recovery enable**" command will disable the function.

Parameters: None
Default Settings: Disable the automatic recovery function
Command Mode: Global configuration mode
User Guide: If the users want the normal state to be recovered after a while the port is closed, they can configure this function.
Example: Enable the automatic recovery function of the switch.
Switch(config)#anti-arpscan recovery enable

4.9.7 anti-arpscan recovery time

Command: anti-arpscan recovery time *<seconds>*
no anti-arpscan recovery time
Function: Configure automatic recovery time; "**no anti-arpscan recovery time**" command resets the automatic recovery time to default value.
Parameters: Automatic recovery time, in second ranging from 5 to 86400.
Default Settings: 300 seconds.
Command Mode: Global configuration mode
User Guide: Automatic recovery function should be enabled first.
Example: Set the automatic recovery time as 3600 seconds.
Switch(config)#anti-arpscan recovery time 3600

4.9.8 anti-arpscan log enable

Command: anti-arpscan log enable
no anti-arpscan log enable
Function: Enable ARP scanning prevention log function; "**no anti-arpscan log enable**" command will disable this function.
Parameters: None.
Default Settings: Disable ARP scanning prevention log function.
Command Mode: Global configuration mode
User Guide: After enabling ARP scanning prevention log function, users can check the detailed information of ports being closed or automatically recovered by ARP scanning prevention or IP being disabled and recovered by ARP scanning prevention. The level of the log is "Warning".
Example: Enable ARP scanning prevention log function of the switch.
Switch(config)#anti-arpscan log enable

4.9.9 anti-arpscan trap enable

Command: anti-arpscan trap enable
no anti-arpscan trap enable
Function: Enable ARP scanning prevention SNMP Trap function; "**no anti-arpscan trap enable** " command disable ARP scanning prevention SNMP Trap function.
Parameters: None.

Default Settings: By default disable or enable level-1 limited speed and level-2 insulate trap function.

Command Mode: Global configuration mode

User Guide: After enabling ARP scanning prevention SNMP Trap function, users will receive Trap message whenever a port is closed or recovered by ARP scanning prevention, and whenever IP t is closed or recovered by ARP scanning prevention.

Example: Enable ARP scanning prevention SNMP Trap function of the switch.

Switch(config)#anti-arpscan trap enable

4.9.10 anti-arpscan FFP max-num <num>

Command: anti-arpscan FFP max-num <num>

Function: The maximum quantity of ARP scanning prevention function occupied FFP item.

Parameters: <1-1024>, the default is 200 available resources.

Command Mode: Global configuration mode

User Guide: When port received a arp packets whose source above max-num and arp rate of every source ip above level-1 or level-2 threshold, users can set a higher value for ffp item after ffp resource exhausted.

Example: Switch(config)#anti-arpscan ffp max-num 1024

4.9.11 debug anti-arpscan

Command: debug anti-arpscan [port | ip]

no debug anti-arpscan [port | ip]

Function: Enable the debug switch of ARP scanning prevention; ”**no debug anti-arpscan [port | ip]**” command disables the switch.

Parameters: None.

Default Settings: Disable the debug switch of ARP scanning prevention

Command Mode: Admin Mode

User Guide: After enabling debug switch of ARP scanning prevention users can check corresponding debug information or enable the port-based or IP-based debug switch separately whenever a port is closed by ARP scanning prevention or recovered automatically, and whenever IP t is closed or recovered .

Example: Enable the debug function for ARP scanning prevention of the switch.

Switch#debug anti-arpscan

4.9.12 show anti-arpscan

Command: show anti-arpscan [trust {ip | port | supertrust-port | iptrust-port} |prohibited {ip | port}]

Function: Display the operation information of ARP scanning prevention function.

Parameters: None.

Default Settings: Display every port to tell whether it is a trusted port and whether it is closed. If

the port is closed, then display how long it has been closed. Display all the trusted IP and disabled IP.

Command Mode: Admin Mode

User Guide: Use "**show anti-arpscan trust port**" if users only want to check trusted ports. The reset follow the same rule.

Example: Check the operating state of ARP scanning prevention function after enabling it.

Switch(config)#show anti-arpscan

Total port: 28

Name	Port-property	beShut	shutTime(seconds)
Ethernet1/0/1	untrust	N	0
Ethernet1/0/2	untrust	N	0
Ethernet1/0/3	untrust	N	0
Ethernet1/0/4	untrust	N	0
Ethernet1/0/5	untrust	N	0
Ethernet1/0/6	untrust	N	0
Ethernet1/0/7	untrust	N	0
Ethernet1/0/8	untrust	N	0
Ethernet1/0/9	untrust	N	0
Ethernet1/0/10	untrust	N	0
Ethernet1/0/11	untrust	N	0
Ethernet1/0/12	untrust	N	0
Ethernet4/1	untrust	N	0
Ethernet4/2	untrust	N	0
Ethernet4/3	untrust	N	0
Ethernet4/4	trust	N	0
Ethernet4/5	untrust	N	0
Ethernet4/6	supertrust	N	0
Ethernet4/7	untrust	Y	30
Ethernet4/8	trust	N	0
Ethernet4/9	untrust	N	0
Ethernet4/10	untrust	N	0
Ethernet4/11	untrust	N	0
Ethernet4/12	untrust	N	0
Ethernet4/13	untrust	N	0
Ethernet4/14	untrust	N	0
Ethernet4/15	untrust	N	0
Ethernet4/16	untrust	N	0
Ethernet4/17	untrust	N	0
Ethernet4/18	untrust	N	0
Ethernet4/19	untrust	N	0
Ethernet4/20	untrust	N	0
Ethernet4/21	untrust	N	0
Ethernet4/22	untrust	N	0

Ethernet4/23	untrust	N	0
Ethernet4/24	untrust	N	0

Prohibited IP:

IP	shutTime(seconds)
1.1.1.2	132

Trust IP:

192.168.99.5	255.255.255.255
192.168.99.6	255.255.255.255

4.9.13 show anti-arpscan ip-based attack-list [history]

Command: show anti-arpscan ip-based attack-list [history]

Function: Display source information or history source information of ARP scanning attacks prevention.

Parameters: None.

Default: Display the source information of ARP scanning attacks prevention.

Command Mode: Admin Mode, Config Mode.

User Guide: (1) Display ARP scanning attacks prevention source information which includes source ip, corresponding port, vlan, rate and state. When it aboves level-1 threshold, state is Speed-Limit; if above level-2, action is discard-arp and state is Discard-Arp, but state is Isolate when action is isolate.

(2) Display the history source information of ARP scanning attacks prevention, including source IP, port, vlan, times of attacks, state of last attack and internal if attacking. When it aboves level-1 threshold, state is Speed-Limit; if above level-2, action is discard-arp and state is Discard-Arp, but state is Isolate when action is isolate.

Example:

Switch#show anti-arpscan ip-based attack-list

SIP-Addr	Port	VLAN	Speed	ARP-Count	State
30.1.1.6	Ethernet2/48	26	4	57	Speed-Limit
30.1.1.4	Ethernet2/48	26	4	56	Speed-Limit

Switch#show anti-arpscan ip-based attack-list history

SIP-Addr	Port	VLAN	Attack-Times	State	Keep-Time
30.1.1.6	Ethernet2/48	26	6	Speed-Limit	0 weeks,0 days,0 hours,8 minutes,46 seconds
30.1.1.4	Ethernet2/48	26	3	Speed-Limit	0 weeks,0 days,0 hours,0 minutes,28 seconds

4.9.14 show anti-arpscan ip-based running-config

Command: show anti-arpscan ip-based running-config
Function: Display the current configuration of arp scanning prevention.
Parameters: None.
Command Mode: Admin Mode, Config Mode.
User Guide: Display the current configuration of arp scanning prevention, the action after level-1 threshold and level-2 threshold above level-2 threshold, cpu rate and the size of ffp items and so on after arp above level-1 threshold.
Example:

```
Switch(config)#show anti-arpscan ip-based running-config
level1 thrshould:     4
level2 thrshould:     8
level2 action:          Discard-Arp
arp-to-cpu speed:     2
actIp-num:              0
ffp-max:                1024
ffp-used:               0
```

4.10 Preventing ARP Spoofing

4.10.1 ip arp-security updateprotect

Command: ip arp-security updateprotect
no ip arp-security updateprotect
Function: Forbid ARP table automatic update. The "**no ip arp-security updateprotect**" command re-enables ARP table automatic update.
Parameter: None.
Default: ARP table automatic update.
Command Mode: Global Mode/ Interface configuration.
User Guide: Forbid ARP table automatic update, the ARP packets conflicting with current ARP item (e.g. with same IP but different MAC or port) will be dropped, the others will be received to update aging timer or create a new item; so, the current ARP item keep unchanged and the new item can still be learned.
Example:

```
Switch(Config-if-Vlan1)#ip arp-security updateprotect.
Switch(config)#ip arp-security updateprotect
```

4.10.2 ip arp-security learnprotect

Command: ip arp-security learnprotect
no ip arp-security learnprotect

Function: Forbid ARP learning function of IPv4 Version, the "**no ip arp-security learnprotect**" command re-enables ARP learning function.
Parameter: None.
Default: ARP learning enabled.
Command Mode: Global Mode/ Interface Configuration.
Usage Guide: This command is for preventing the automatic learning and updating of ARP. Unlike ip arp-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.
Example:
Switch(Config-if-Vlan1)# ip arp-security learnprotect
Switch(config)# ip arp-security learnprotect

4.10.3 ip arp-security convert

Command: ip arp-security convert
Function: Change all of dynamic ARP to static ARP.
Parameter: None
Command Mode: Global Mode/ Interface configuration
Usage Guide: This command will convert the dynamic ARP entries to static ones, which, in combination with disabling automatic learning, can prevent ARP binding. Once implemented, this command will lose its effect.
Example:
Switch(Config-if-Vlan1)#ip arp -security convert
Switch(config)#ip arp -security convert

4.11 ARP GUARD

4.11.1 arp-guard ip

Command: arp-guard ip <addr>
no arp-guard ip <addr>
Function: Add an ARP GUARD address, the no command deletes ARP GUARD address.
Parameters: <addr> is the protected IP address, in dotted decimal notation.
Default: There is no ARP GUARD address by default.
Command Mode: Port configuration mode
Usage Guide: After configuring the ARP GUARD address, the ARP messages received from the ports configured ARP GUARD will be filtered. If the source IP addresses of the ARP messagse match the ARP GUARD address configured on this port, these messages will be judged as ARP cheating messages, which will be directly dropped instead of sending to the CPU of the switch or forwarding. 16 ARP GUARD addresses can be configured on each port.
Example:

Configure the ARP GUARD address on port ethernet1/0/1 as 100.1.1.1.
switch(config)#interface ethernet1/0/1
switch(Config-If-Ethernet 1/0/1)#arp-guard ip 100.1.1.1
Delete the ARP GUARD address on port ethernet1/0/1 as 100.1.1.1.
switch(config)#interface ethernet1/0/1
switch(Config-If-Ethernet 1/0/1)#no arp-guard ip 100.1.1.1

4.12 ARP Local Proxy

4.12.1 ip local proxy-arp

Command: ip local proxy-arp
no ip local proxy-arp
Function: Enable/disable the local ARP Proxy function of a specified interface.
Parameters: None.
Default Settings: This function is disabled on all interfaces by default.
Command Mode: Interface VLAN Mode.
User Guide: This function is disabled on all interfaces by default, and differs from the original proxy-arp in that this function acts as an ARP Proxy inside the same layer-3 interface and thus directs the layer-3 forwarding of the switch.
Example: Enable the local ARP Proxy function of interface VLAN1.
Switch(Config-if-Vlan1)# ip local proxy-arp

4.13 Gratuitous ARP

4.13.1 ip gratuitous-arp

Command: ip gratuitous-arp [<*interval-time*>]
no ip gratuitous-arp
Function: To enabled gratuitous ARP, and specify update interval for gratuitous ARP. The no form of this command will disable the gratuitous ARP configuration.
Parameters: ***<interval-time>*** is the update interval for gratuitous ARP with its value limited between 5 and 1200 seconds and with default value as 300 seconds.
Command Mode: Global Configuration Mode and Interface Configuration Mode.
Default: Gratuitous ARP is disabled by default.
Usage Guide: When configuring gratuitous ARP in global configuration mode, all the Layer 3

interfaces in the switch will be enabled to send gratuitous ARP request. If gratuitous ARP is configured in interface configuration mode, then only the specified interface is able to send gratuitous ARP requests. When configuring the gratuitous ARP, the update interval configuration from interface configuration mode has higher preference than that from the global configuration mode.

Example:

1) To enable gratuitous ARP in global configuration mode, and set the update interval to be 400 seconds.

```
Switch>enable
Switch#config
Switch(config)#ip gratuitous-arp 400
```

2) To enable gratuitous ARP for interface VLAN 10 and set the update interval to be 350 seconds.

```
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 350
```

4.13.2 show ip gratuitous-arp

Command: show ip gratuitous-arp [interface vlan *<vlan-id>*]

Function: To display configuration information about gratuitous ARP.

Parameters: *<vlan-id>* is the VLAN ID. The valid range for <*vlan-id*> is between 1 and 4094.

Command Mode: All the Configuration Modes.

Usage Guide: In all the configuration modes, the command **show ip gratuitous arp** will display information about the gratuitous ARP configuration in global and interface configuration mode. The command **show ip gratuitous-arp interface vlan *<vlan-id>*** will display information about the gratuitous ARP configuration about the specified VLAN interface.

Example:

1) To display information about gratuitous ARP configuration in both global and interface configuration modes.

```
Switch#show ip gratuitous-arp
Gratuitous ARP send is Global enabled, Interval-Time is 300(s)

Gratuitous ARP send enabled interface vlan information:
Name                Interval-Time(seconds)
Vlan1               400
Vlan10              350
```

2) To display gratuitous ARP configuration information about interface VLAN 10.

```
Switch#show ip gratuitous-arp interface vlan 10
Gratuitous ARP send interface Vlan10 information:
Name                Interval-Time(seconds)
Vlan10              350
```

4.14 Keepalive Gateway

4.14.1 keepalive gateway

Command: keepalive gateway *<ip-address>* [{*<interval-seconds>* | msec *<interval-millisecond>*} [retry-count]]

no keepalive gateway

Function: Enable keepalive gateway, configure the interval that ARP request packet is sent and the retry-count after detection is failing, the no command disables the function.

Parameters: ip-address: IP address of the gateway

interval-seconds: The interval (unit is second) that ARP request packet is sent, ranging between 1 and 32767. If there is no configuration, the default is 10 seconds.

interval-millisecond: The interval (unit is millisecond) that ARP request packet is sent, ranging between 160 and 999.

retry-count: Determine the retry-count after detection is failing. If there is no configuration, the default is 5 times.

Default: Disable keepalive gateway.

Command Mode: Interface mode.

Usage Guide: This command is supported by layer 3 switch and the detection method is used to point-to-point topology mode only.

Example:

Switch(config)#interface vlan 1

Switch(config-if-vlan1)#keealive gateway 1.1.1.1 3 10

4.14.2 show ip interface

Command: show ip interface [interface-name]

Function: Show IPv4 running status of the specified interface.

Parameters: interface-name is the specified interface name. If there is no parameter, show IPv4 running status of all interfaces.

Default: None.

Command Mode: Admin and configuration mode.

Usage Guide: Show IPv4 running status of the interface.

Example:

Switch(config)#show ip interface brief

Index	Interface	IP-Address	Protocol
3001	Vlan1	1.1.1.2	up
9000	Loopback	127.0.0.1	up

4.14.3 show keepalive gateway

Command: show keepalive gateway [interface-name]
Function: Show keepalive running status of the specified interface.
Parameters: interface-name is the specified interface name. If there is no parameter, show keepalive running status of all interfaces.
Default: None.
Command Mode: Admin and configuration mode.
Usage Guide: Show keepalive running status of the interface.
Example:
Switch(config)#show keepalive gateway
interface Vlan1 gateway 1.1.1.1 time 10s retry 1 remain 4 now UP

4.15 Dynamic ARP Inspection

4.15.1 ip arp inspection

Command: ip arp inspection vlan <vlan-id>
no ip arp inspection vlan <vlan-id>
Function: Enable the dynamic ARP inspection function based on vlan.
Parameters: <vlan-id> is the vlan which is enabled the dynamic ARP inspection function.
Command Mode: Global Mode.
Default: Disable.
Usage Guide: After configured the dynamic ARP inspection function in global mode, the administrator can intercept, record and drop the ARP data packets which have the invalid MAC address/IP address, This command is generally used in combination with ip dhcp snooping.
Example: Enable the dynamic ARP inspection function of vlan10.
Switch(config)#
Switch(config)#ip arp inspection vlan 10
Switch(config)#exit

4.15.2 ip arp inspection port

Command: ip arp inspection port recovery-time <1-3600>
no ip arp inspection port recovery-time
Function: Change the recovery time after changing the port speed limit of the dynamic ARP detection function.
Parameter:<1-3600>is the recovery time after port speed limit for dynamic ARP detection function
Command mode: Global configuration mode.

Default situation: The default recovery time is 60 seconds.
Usage guide: You can change the recovery time after the port speed limit of the dynamic ARP detection function. This command is generally used in conjunction with IP DHCP snooping.
Example: Recovery time after changing the port speed limit of dynamic ARP detection function in global mode:
Switch(config)#
Switch(config)#ip arp inspection port recovery-time 100
Switch(config)#exit

4.15.3 ip arp inspection trust

Command: ip arp inspection trust
no ip arp inspection trust
Function: Configure the port as the trusted port of the dynamic ARP inspection.
Parameters: None.
Command Mode: Port Mode.
Default: All the ports are the untrusted ports as default.
Usage Guide: After configured this command under the port mode, the configured port will not inspect the received ARP packet and it will forward it directly. If the ARP data packet is received from the untrusted port, the switch will only forward the lawful data packet. For the illegal data, it will drop the data directly and record this action, This command is generally used in combination with ip dhcp snooping.
Example: Configure the port 1/0/1 as the trusted port.
Switch(config)#
Switch(config)#in e 1/0/1
Switch(config-if-ethernet1/0/1)#ip arp inspection trust
Switch(config-if-ethernet1/0/1)#exit

4.15.4 ip arp inspection limit-rate

Command: ip arp inspection limit-rate <rate>
no ip arp inspection limit-rate
Function: Limit the ARP packet rate of the untrusted port.
Parameters: <rate> is the configured limited rate of the ARP packet of the untrusted port, the unit is pps.
Command Mode: Port Mode.
Default: Do not limit the rate for the ARP packets of the trusted or untrusted ports.
Usage Guide: This command can limit the ARP packet rate of the untrusted port. The rate of the lawful ARP data packets forwarding is in the limited range, This command is generally used in combination with ip dhcp snooping.
Example: Configure the rate of the ARP packet of the untrusted port 1/0/1 as 100pps.
Switch(config)#

```
Switch(config)#in e 1/0/1
Switch(config-if-ethernet1/0/1)# ip arp inspection limit-rate 100
Switch(config-if-ethernet1/0/1)#exit
```

4.16 DHCP

4.16.1 DHCP Server

4.16.1.1 bootfile

Command: bootfile *<filename>*

no bootfile

Function: Sets the file name for DHCP client to import on boot up; the "**no bootfile**" command deletes this setting.

Parameters: *<filename>* is the name of the file to be imported, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Specify the name of the file to be imported for the client. This is usually used for diskless workstations that need to download a configuration file from the server on boot up. This command is together with the "next sever".

Example: The path and filename for the file to be imported is "c:\temp\nos.img"

```
Switch(dhcp-1-config)#bootfile c:\temp\nos.img
```

Related Command: next-server

4.16.1.2 clear ip dhcp binding

Command: clear ip dhcp binding {*<address>* | all}

Function: Deletes the specified IP address-hardware address binding record or all IP address-hardware address binding records.

Parameters: *<address>* is the IP address that has a binding record in decimal format. **all** refers to all IP addresses that have a binding record.

Command mode: Admin Mode.

Usage Guide: "**show ip dhcp binding**" command can be used to view binding information for IP addresses and corresponding DHCP client hardware addresses. If the DHCP server is informed that a DHCP client is not using the assigned IP address for some reason before the lease period expires, the DHCP server would not remove the binding information automatically. The system administrator can use this command to delete that IP address-client hardware address binding manually, if "all" is specified, then all auto binding records will be deleted, thus all addresses in the DHCP address pool will be reallocated.

Example: Removing all IP-hardware address binding records.
Switch#clear ip dhcp binding all
Related Command: show ip dhcp binding

4.16.1.3 clear ip dhcp conflict

Command: clear ip dhcp conflict {*<address>* | all }
Function: Deletes an address present in the address conflict log.
Parameters: ***<address>*** is the IP address that has a conflict record; **all** stands for all addresses that have conflict records.
Command mode: Admin Mode.
Usage Guide: "**show ip dhcp conflict**" command can be used to check which IP addresses are conflicting for use. The "**clear ip dhcp conflict**" command can be used to delete the conflict record for an address. If "all" is specified, then all conflict records in the log will be removed. When records are removed from the log, the addresses are available for allocation by the DHCP server.
Example: The network administrator finds 10.1.128.160 that has a conflict record in the log and is no longer used by anyone, so he deletes the record from the address conflict log.
Switch#clear ip dhcp conflict 10.1.128.160
Related Command: ip dhcp conflict logging, show ip dhcp conflict

4.16.1.4 clear ip dhcp server statistics

Command: clear ip dhcp server statistics
Function: Deletes the statistics for DHCP server, clears the DHCP server count.
Parameters: None
Command mode: Admin Mode.
Usage Guide: DHCP count statistics can be viewed with "**show ip dhcp server statistics**" command, all information is accumulated. You can use the "**clear ip dhcp server statistics**" command to clear the count for easier statistics checking.
Example: Clearing the count for DHCP server.
Switch#clear ip dhcp server statistics
Related Command: show ip dhcp server statistics

4.16.1.5 client-identifier

Command: client-identifier *<unique-identifier>*
no client-identifier
Function: Specifies the unique ID of the user when binding an address manually; the "**no client-identifier**" command deletes the identifier.
Parameters: ***<unique-identifier>*** is the user identifier, in dotted Hex format.
Command Mode: DHCP Address Pool Mode
Usage Guide: This command is used with "host" when binding an address manually. If the

requesting client identifier matches the specified identifier, DHCP server assigns the IP address defined in "host" command to the client.

Example: Specifying the IP address 10.1.128.160 to be bound to user with the unique id of 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

Related Command: host

4.16.1.6 debug ip dhcp client

Command: debug ip dhcp client {event | packet}

no debug ip dhcp server {event | packet}

Function: Enable the debugging of DHCP client, no command disables the debugging of DHCP client.

Command mode: Admin Mode

Default: Disable the debugging.

4.16.1.7 debug ip dhcp relay

Command: debug ip dhcp server packet

no debug ip dhcp server packet

Function: Enable the debugging of DHCP relay, no command disables the debugging of DHCP relay.

Command mode: Admin Mode

Default: Disable the debugging.

4.16.1.8 debug ip dhcp server

Command: debug ip dhcp server { events | linkage | packets |history|lookup}

no debug ip dhcp server { events | linkage | packets|history|lookup }

Function: Enables DHCP server debug information: the "**no debug ip dhcp server {events | linkage | packets|history|lookup}**" command disables the debug information for DHCP server**.**

Default: Debug information is disabled by default.

Command mode: Admin Mode.

4.16.1.9 default-router

Command: default-router <*address1*>[<*address2*>[…<*address8*>]]

no default-router

Function: Configures default gateway(s) for DHCP clients; the "**no default-router**" command deletes the default gateway.

Parameters: <*address1*>…<*address8*> are IP addresses, in decimal format.

Default: No default gateway is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: The IP address of default gateway(s) should be in the same subnet as the DHCP client IP, the switch supports up to 8 gateway addresses. The gateway address assigned first has the highest priority, and therefore address1 has the highest priority, and address2 has the second, and so on.

Example: Configuring the default gateway for DHCP clients to be 10.1.128.2 and 10.1.128.100.

Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100

4.16.1.10 dns-server

Command: dns-server <*address1*>[<*address2*>[…<*address8*>]]

no dns-server

Function: Configure DNS servers for DHCP clients; the "**no dns-server**" command deletes the default gateway.

Parameters: <*address1*>…<*address8*> are IP addresses, in decimal format.

Default: No DNS server is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: Up to 8 DNS server addresses can be configured. The DNS server address assigned first has the highest priority, therefore address 1 has the highest priority, and address 2 has the second, and so on.

Example: Set 10.1.128.3 as the DNS server address for DHCP clients.

Switch(dhcp-1-config)#dns-server 10.1.128.3

4.16.1.11 domain-name

Command: domain-name *<domain>*

no domain-name

Function: Configures the Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.

Parameters: *<domain>* is the domain name, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Default: None

Usage Guide: Specifies a domain name for the client.

Example: Specifying 'digitalchina.com.cn' as the DHCP clients' domain name.

Switch(dhcp-1-config)#domain_x001F_-name digitalchina.com.cnwww.google.com

4.16.1.12 hardware-address

Command: hardware-address *<hardware-address>* [{Ethernet | IEEE802|*<type-number>*}]

no hardware-address

Function: Specifies the hardware address of the user when binding address manually; the "**no hardware-address**" command deletes the setting.

Parameters: *<hardware-address>* is the hardware address in Hex; **Ethernet | IEEE802** is the

Ethernet protocol type, ***<type-number>*** should be the RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.

Default: The default protocol type is Ethernet,

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used with the "host" when binding address manually. If the requesting client hardware address matches the specified hardware address, the DHCP server assigns the IP address defined in "host" command to the client.

Example: Specify IP address 10.1.128.160 to be bound to the user with hardware address 00-00-e2-3a-26-04 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04

Switch(dhcp-1-config)#host 10.1.128.160 24

Related Command: host

4.16.1.13 host

Command: host <*address*> [<*mask*> | <*prefix-length*>]

no host

Function: Specifies the IP address to be assigned to the user when binding addresses manually; the "**no host**" command deletes the IP address.

Parameters: ***<address>*** is the IP address in decimal format; ***<mask>*** is the subnet mask in decimal format; ***<prefix-length>*** means mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30".

Command Mode: DHCP Address Pool Mode

Default: None

Usage Guide: If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the system will assign a mask automatically according to the IP address class.

This command is used with "hardware address" command or "client identifier" command when binding addresses manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in "host" command to the client.

Example: Specifying IP address 10.1.128.160 to be bound to user with hardware address 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

Related command: hardware-address, client-identifier

4.16.1.14 ip dhcp conflict logging

Command: ip dhcp conflict logging

no ip dhcp conflict logging

Function: Enables logging for address conflicts detected by the DHCP server; the "**no ip dhcp conflict logging"** command disables the logging.

Default: Logging for address conflict is enabled by default.
Command mode: Global Mode
Usage Guide: When logging is enabled, once the address conflict is detected by the DHCP server, the conflicting address will be logged. Addresses present in the log for conflicts will not be assigned dynamically by the DHCP server until the conflicting records are deleted.
Example: Disable logging for DHCP server.
Switch(config)#no ip dhcp conflict logging
Related Command: clear ip dhcp conflict

4.16.1.15 ip dhcp disable

This command is not supported by the switch.

4.16.1.16 ip dhcp excluded-address

Command: ip dhcp excluded-address *<low-address>* [*<high-address>*]
no ip dhcp excluded-address *<low-address>* [*<high-address>*]
Function: Specifies addresses excluding from dynamic assignment; the "**no ip dhcp excluded-address *<low-address>* [*<high-address>*]**" command cancels the setting.
Parameters: *<low-address>* is the starting IP address, **[*<high-address>*]** is the ending IP address.
Default: Only individual address is excluded by default.
Command mode: Global Mode
Usage Guide: This command can be used to exclude one or several consecutive addresses in the pool from being assigned dynamically so that those addresses can be used by the administrator for other purposes.
Example: Reserving addresses from 10.1.128.1 to 10.1.128.10 from dynamic assignment.
Switch(config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10

4.16.1.17 ip dhcp pool

Command: ip dhcp pool *<name>*
no ip dhcp pool *<name>*
Function: Configures a DHCP address pool and enter the pool mode; the "**no ip dhcp pool *<name>***" command deletes the specified address pool.
Parameters: *<name>* is the address pool name, up to 32 characters are allowed.
Command mode: Global Mode
Usage Guide: This command is used to configure a DHCP address pool under Global Mode and enter the DHCP address configuration mode.
Example: Defining an address pool named "1".
Switch(config)#ip dhcp pool 1
Switch(dhcp-1-config)#

4.16.1.18 ip dhcp conflict ping-detection enable

Command: ip dhcp conflict ping-detection enable

no ip dhcp conflict ping-detection enable

Function: Enable Ping-detection of conflict on DHCP server; the no operation of this command will disable the function.

Parameters: None.

Default Settings: By default, Ping-detection of conflict is disabled.

Command Mode: Global Configuration Mode.

Usage Guide: To enable Ping-detection of conflict, one should enable the log of conflict addresses, when which is disabled, so will the ping-detection of conflict. When a client is unable to receive Ping request messages (when blocked by firewall, for example), this function will check local ARP according to allocated IP: if a designated IP has a corresponding ARP, then an address conflict exists; otherwise, allocate it to the client.

Examples: Enable Ping-detection of conflict.

Switch(config)#ip dhcp conflict ping-detection enable

Related Command: ip dhcp conflict logging, ip dhcp ping packets, ip dhcp ping timeout

4.16.1.19 ip dhcp ping packets

Command: ip dhcp ping packets *<request-num>*

no ip dhcp ping packets

Function: Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server, whose default value is 2; the no operation of this command will restore the default value.

Parameters: *<request-num>* is the number of Ping request message to be sent in Ping-detection of conflict.

Default Settings: No more than 2 Ping request messages will be sent by default.

Command Mode: Global Configuration Mode.

Examples: Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server as 3.

Switch(config)#ip dhcp ping packets 3

Related Command: ip dhcp conflict ping-detection enable, ip dhcp ping timeout

4.16.1.20 ip dhcp ping timeout

Command: ip dhcp ping timeout *<timeout-value>*

no ip dhcp ping timeout

Function: Set the timeout period (in ms) of waiting for a reply message (Echo Request) after each Ping request message (Echo Request) in Ping-detection of conflict on DHCP server, whose default value is 500ms. The no operation of this command will restore the default value.

Parameters: *<timeout-value>* is the timeout period of waiting for a reply message after each Ping request message in Ping-detection of conflict.

Default Settings: The timeout period is 500ms by default.

Command Mode: Global Configuration Mode.

Examples: Set the timeout period (in ms) of waiting for each reply message (Echo Request) in Ping-detection of conflict on DHCP server as 600ms.

Switch(config)# ip dhcp ping timeout 600

Related Command: ip dhcp conflict ping-detection enable, ip dhcp ping packets

4.16.1.21 lease

Command: lease { [*<days>*] [*<hours>*][*<minutes>*] | infinite }

no lease

Function: Sets the lease time for addresses in the address pool; the "**no lease**" command restores the default setting.

Parameters: ***<days>*** is number of days from 0 to 365; ***<hours>*** is number of hours from 0 to 23; ***<minutes>*** is number of minutes from 0 to 59; **infinite** means perpetual use.

Default: The default lease duration is 1 day.

Command Mode: DHCP Address Pool Mode

Usage Guide: DHCP is the protocol to assign network addresses dynamically instead of permanently, hence the introduction of ease duration. Lease settings should be decided based on network conditions: too long lease duration offsets the flexibility of DHCP, while too short duration results in increased network traffic and overhead. The default lease duration of switch is 1 day.

Example: Setting the lease of DHCP pool "1" to 3 days 12 hours and 30 minutes.

Switch(dhcp-1-config)#lease 3 12 30

4.16.1.22 max-lease-time

Command: max-lease-time {[<*days*>] [<*hours*>] [<*minutes*>] | infinite}

no max-lease-time

Function: Set the maximum lease time for the addresses in the address pool; the no command restores the default setting.

Parameters: ***<days>*** is number of days from 0 to 365; ***<hours>*** is number of hours from 0 to 23; ***<minutes>*** is number of minutes from 0 to 59; **infinite** means perpetual use.

Default: The default lease time is 1 day.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used to DHCP request packets with option51. If the lease time (user requests the address) exceeds the maximum lease time configured, the lease that DHCP server assigns the address is the maximum lease time configured. If the lease time requested by the user is less than the maximum lease time configured, the lease that DHCP server assigns the address is the lease time requested by the user. The maximum lease time is able to be set by the administrator according to the actual network condition, and the maximum lease time is 1 day by default.

Example: Set the maximum lease time of DHCP address pool1 to 3 days 12 hours and 30 minutes.

Switch(dhcp-1-config)#max-lease-time 3 12 30

4.16.1.23 netbios-name-server

Command: netbios-name-server <*address1*>[<*address2*>[…<*address8*>]]

no netbios-name-server

Function: Configures WINS servers' address; the "**no netbios-name-server**" command deletes the WINS server.

Parameters: <*address1*>…<*address8*> are IP addresses, in decimal format.

Default: No WINS server is configured by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used to specify WINS server for the client, up to 8 WINS server addresses can be configured. The WINS server address assigned first has the highest priority. Therefore, address 1 has the highest priority, and address 2 the second, and so on.

Example: Setting the server address of DHCP pool "1" to 192.168.1.1.

Switch(dhcp-1-config)#netbios-name-server 192.168.1.1

4.16.1.24 netbios-node-type

Command: netbios-node-type {b-node | h-node | m-node | p-node | <*type-number*>}

no netbios-node-type

Function: Sets the node type for the specified port; the "**no netbios-node-type**" command cancels the setting.

Parameters: b-node stands for broadcasting node, **h-node** for hybrid node that broadcasts after point-to-point communication; **m-node** for hybrid node to communicate in point-to-point after broadcast; **p-node** for point-to-point node; ***<type-number>*** is the node type in Hex from 0 to FF.

Default: No client node type is specified by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: If client node type is to be specified, it is recommended to set the client node type to **h-node** that broadcasts after point-to-point communication.

Example: Setting the node type for client of pool 1 to broadcasting node.

Switch(dhcp-1-config)#netbios-node-type b-node

4.16.1.25 network-address

Command: network-address <*network-number*> [<*mask*> | <*prefix-length*>]

no network-address

Function: Sets the scope for assignment for addresses in the pool; the "**no network-address**" command cancels the setting.

Parameters: *<network-number>* is the network number; ***<mask>*** is the subnet mask in the decimal format; ***<prefix-length>*** stands for mask in prefix form. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30". Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.

Default: If no mask is specified, default mask will be assigned according to the address class.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command sets the scope of addresses that can be used for dynamic assignment by the DHCP server; one address pool can only have one corresponding segment. This command is exclusive with the manual address binding command “hardware address” and “host”.

Example: Configuring the assignable address in pool 1 to be 10.1.128.0/24.

Switch(dhcp-1-config)#network-address 10.1.128.0 24

4.16.1.26 next-server

Command: next-server <address1>[<address2>[…<address8>]]

no next-server

Function: Sets the server address for storing the client import file; the “**no next-server**” command cancels the setting.

Parameters: <*address1*>…<*address8*> are IP addresses, in the decimal format.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command configures the address for the server hosting client import file. This is usually used for diskless workstations that need to download configuration files from the server on boot up. This command is used together with “bootfile”.

Example: Setting the hosting server address as 10.1.128.4.

Switch(dhcp-1-config)#next-server 10.1.128.4

4.16.1.27 option

Command: option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>}

no option <*code*>

Function: Sets the network parameter specified by the option code; the “**no option <*code*>**” command cancels the setting for option.

Parameters: <*code*> is the code for network parameters; **<*string*>** is the ASCII string up to 255 characters; **<*hex*>** is a value in Hex that is no greater than 510 and must be of even length; **<*ipaddress*>** is the IP address in decimal format, up to 63 IP addresses can be configured.

Command Mode: DHCP Address Pool Mode

Default: None

Usage Guide: The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.

Example: Setting the WWW server address as 10.1.128.240.

Switch(dhcp-1-config)#option 72 ip 10.1.128.240

4.16.1.28 service dhcp

Command: service dhcp

no service dhcp

Function: Enables DHCP server; the "**no service dhcp**" command disables the DHCP service.
Parameters: None
Default: DHCP service is disabled by default.
Command mode: Global Mode
Usage Guide: Both DHCP server and DHCP relay are included in the DHCP service. When DHCP services are enabled, both DHCP server and DHCP relay are enabled. Switch can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.
Example: Enabling DHCP server.
Switch(config)#service dhcp

4.16.1.29 show ip dhcp binding

Command: show ip dhcp binding [[*<ip-addr>*] [type {all | manual | dynamic}] [count]]
Function: Displays IP-MAC binding information.
Parameters: ***<ip-addr>*** is a specified IP address in decimal format; **all** stands for all binding types (manual binding and dynamic assignment); **manual** for manual binding; **dynamic** for dynamic assignment; **count** displays statistics for DHCP address binding entries.
Command mode: Admin and Configuration Mode.
Example:
Switch# show ip dhcp binding

IP address	Hardware address	Lease expiration	Type
10.1.1.233	00-00-E2-3A-26-04	Infinite	Manual
10.1.1.254	00-00-E2-3A-5C-D3	60	Automatic

Displayed information	Explanation
IP address	IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Valid time for the DHCP client to hold the IP address
Type	Type of assignment: manual binding or dynamic assignment.

4.16.1.30 show ip dhcp conflict

Command: show ip dhcp conflict
Function: Displays log information for addresses that have a conflict record.
Command mode: Admin and Configuration Mode.
Example:
Switch# show ip dhcp conflict

IP Address	Detection method	Detection Time
10.1.1.1	Ping	FRI JAN 02 00:07:01 2002

Displayed information	Explanation
IP Address	Conflicting IP address
Detection method	Method in which the conflict is detected.
Detection Time	Time when the conflict is detected.

4.16.1.31 show ip dhcp relay information option

Command: show ip dhcp relay information option
Function: Show the relative configuration for DHCP relay option82.
Parameters: None.
Command mode: Admin and configuration mode
Default: None.
Usage guide: None.
Example: Set the admin mode timeout value to 6 minutes.
Switch#show ip dhcp relay information option
ip dhcp server relay information option(i.e. option 82) is enabled
ip dhcp relay information option(i.e. option 82) is enabled

4.16.1.32 show ip dhcp server statistics

Command: show ip dhcp server statistics
Function: Displays statistics of all DHCP packets for a DHCP server.
Command mode: Admin and Configuration Mode.
Example:
Switch# show ip dhcp server statistics

Address pools	3
Database agents	0
Automatic bindings	2
Manual bindings	0
Conflict bindings	0
Expired bindings	0
Malformed message	0

Message	Received
BOOTREQUEST	3814
DHCPDISCOVER	1899
DHCPREQUEST	6
DHCPDECLINE	0
DHCPRELEASE	1
DHCPINFORM	1

Message	Send
BOOTREPLY	1911
DHCPOFFER	6
DHCPACK	6
DHCPNAK	0
DHCPRELAY	1907
DHCPFORWARD	0

Switch#

Displayed information	Explanation
Address pools	Number of DHCP address pools configured.
Database agents	Number of database agents.
Automatic bindings	Number of addresses assigned automatically
Manual bindings	Number of addresses bound manually
Conflict bindings	Number of conflicting addresses
Expired bindings	Number of addresses whose leases are expired
Malformed message	Number of error messages.
Message Received	Statistics for DHCP packets received
BOOTREQUEST	Total packets received
DHCPDISCOVER	Number of DHCPDISCOVER packets
DHCPREQUEST	Number of DHCPREQUEST packets
DHCPDECLINE	Number of DHCPDECLINE packets
DHCPRELEASE	Number of DHCPRELEASE packets
DHCPINFORM	Number of DHCPINFORM packets
Message Send	Statistics for DHCP packets sent
BOOTREPLY	Total packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCPNAK	Number of DHCPNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

4.16.2 DHCP Relay

4.16.2.1 ip dhcp broadcast suppress

Command: ip dhcp broadcast suppress

no ip dhcp broadcast suppress

Function: Enable DHCP broadcast suppress function, the no command disables the function.

Parameter: None.

Default: Disable.

Command Mode: Global mode

Usage Guide: Suppress the forwarding about DHCP broadcast packets, namely, drop or copy DHCP broadcast packets to CPU.

Example: Enable DHCP broadcast suppress function.

Switch(config)#ip dhcp broadcast suppress

4.16.2.2 ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>

Command: ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>
no ip dhcp relay share-vlan
Function: Specify a sub VLAN of a share VLAN; The no operation of this command is to cancel the sub vlan of share vlan.
Parameters:< Vlanid>is the vlan number of share vlan< Vlanlist>is a list of sub VLANs.
Default situation: None.
Command mode: Global configuration mode.
Usage guide: There can be many sub VLANs in a share VLAN, but one sub VLAN can only correspond to one share VLAN. When a DHCP Relay layer 2 device receives a DHCP Request, it first checks whether the VLAN in the received packet has a layer 3 interface. If so, it uses this layer 3 interface for DHCP Relay. If the VLAN in the received packet does not have a layer 3 interface, but this VLAN is a sub VLAN of a share VLAN, then use the layer 3 interface of the share VLAN for DHCP Relay.

4.16.2.3 ip forward-protocol udp bootps

Command: ip forward-protocol udp bootps
no ip forward-protocol udp bootps
Function: Sets DHCP relay to forward UPD broadcast packets on the port; the "**no ip forward-protocol udp bootps**" command cancels the service.
Parameter: bootps forwarding UDP port as 67 DHCP broadcast packets.
Default: Not forward UPD broadcast packets by default.
Command mode: Global Mode
Usage Guide: The forwarding destination address is set in the "**ip helper-address**" command and described later.
Example: Setting DHCP packets to be forwarded to 192.168.1.5.
Switch(config)#ip forward-protocol udp boots
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip helper-address 192.168.1.5

4.16.2.4 ip helper-address

Command: ip helper-address *<ip-address>*
no ip helper-address *<ip-address>*
Function: Specifies the destination address for the DHCP relay to forward UDP packets. The "**no ip helper-address *<ip-address>***" command cancels the setting.
Default: None.
Command mode: Interface Configuration Mode
Usage Guide: The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e. DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. When this command is run after "**ip forward-protocol udp *<port>***" command, the forwarding address configured by this command receives the UDP packets from ***<port>***. The combination of "**ip forward-protocol udp *<port>***" command and this command

should be used for configuration.

4.16.2.5 show ip forward-protocol

Command: show ip forward-protocol
Function: Show the configured port ID of the protocol which support the forwarding of broadcast packets, it means the port ID for forwarding DHCP packets.
Command mode: Admin and configuration mode
Example:
Switch#show ip forward-protocol
Forward protocol(UDP port): 67(active)

4.16.2.6 show ip helper-address

Command: show ip helper-address
Function: Show the configuration relation for the port ID of the protocol (It can forward broadcast packets), the interface (It supports forwarding function) and the forwarded destination IP.
Command mode: Admin and configuration mode
Example:
Switch#show ip helper-address

Forward protocol	Interface	Forward server
67(active)	Vlan1	192.168.1.1

4.17 DHCP Option 82

4.17.1 debug ip dhcp relay packet

Command: debug ip dhcp relay packet
Function: This command is used to display the information of data packets processing in DHCP Relay Agent, including the “add” and “peel” action of option 82.
Parameters: None
Command Mode: Admin Mode.
User Guide: Use this command during the operation to display the procedure of data packets processing of the server and to display the corresponding option82 operation information. Identified option 82 information of the request message and the option 82 information returned by the reply message.
Example: Display the information of data packets processing in DHCP Relay Agent.
Switch(config)# debug ip dhcp relay packet

4.17.2 ip dhcp relay information option

Command: ip dhcp relay information option

no ip dhcp relay information option

Function: Set this command to enable the option82 function of the switch Relay Agent. The "**no ip dhcp relay information option**" command is used to disable the option82 function of the switch Relay Agent.

Parameters: None.

Default Settings: The system disables the option82 function by default.

Command Mode: Global configuration mode

Usage Guide: Only the DHCP Relay Agents configuring with this command can add option82 to the DHCP request message, and let the server to process it. Before enabling this function, users should make sure that the DHCP service is enabled and the Relay Agent will transmit the udp broadcast messages whose destination port is 67.

Example: Enable the option82 function of the Relay Agent.

Switch(config)#service dhcp

Switch(config)# ip forward-protocol udp bootps

Switch(config)# ip dhcp relay information option

4.17.3 ip dhcp relay information option delimiter

Command: ip dhcp relay information option delimiter [colon | dot | slash | space]

no ip dhcp relay information option delimiter

Function: Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash.

Parameters: None.

Default Settings: slash ("/").

Command Mode: Global mode

Usage Guide: Divide the parameters with the configured delimiters after users have defined them which are used to create suboption (remot-de, circuit-id) of option82 in global mode.

Example: Set the parameter delimiters as dot (".") for suboption of option82.

Switch(config)#ip dhcp relay information option delimiter dot

4.17.4 ip dhcp relay information option remote-id

Command: ip dhcp relay information option remote-id {standard | *<remote-id>*}

no ip dhcp relay information option remote-id

Function: Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (They are received by the interface). The no command sets the additive suboption2 (remote ID option) format of option 82 as standard.

Parameters: standard means the default VLAN MAC format. ***<remote-id>*** means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.

Command Mode: Global Mode

Default: Use standard format to set remote-id of option 82.

Usage Guide: The additive option 82 information needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format can not satisfy server's request.

Example: Set the suboption remote-id of DHCP option82 as street-1-1.

Switch(config)#ip dhcp relay information option remote-id street-1-1

4.17.5 ip dhcp relay information option remote-id format

Command: ip dhcp relay information option remote-id format {default | vs-hp}

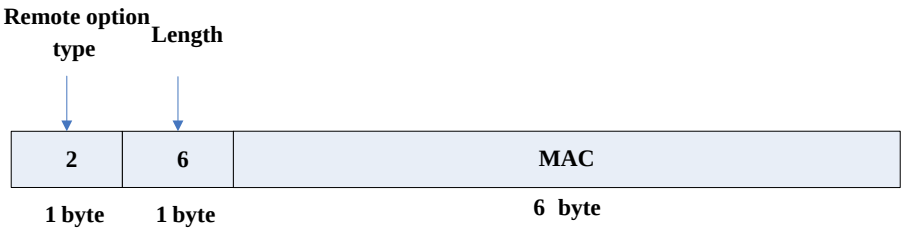
Function: Set remote-id format of Relay Agent option82.

Parameters: default means that remote-id is the VLAN MAC address with hexadecimal format, vs-hp means that remote-id is compatible with the remote-id format of HP manufacturer.

Default: default.

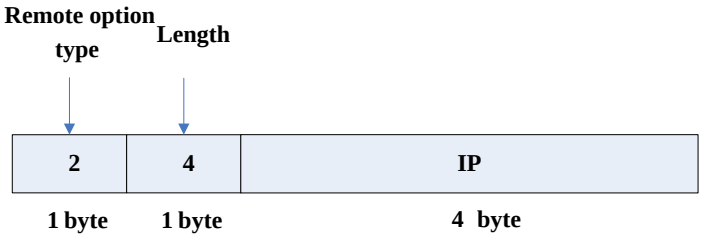
Command Mode: Global mode

Usage Guide: The default remote-id format defined as below:



MAC means VLAN MAC address.

The compatible remote-id format with HP manufacturer defined as below:



IP means the primary IP address of layer 3 interface where DHCP packets from.

Example: Set remote-id of Relay Agent option82 as the compatible format with HP manufacturer.

Switch(config)#ip dhcp relay information option remote-id format vs-hp

4.17.6 ip dhcp relay information option self-defined remote-id

Command: ip dhcp relay information option self-defined remote-id {hostname | mac | string WORD}

no ip dhcp relay information option self-defined remote-id

Function: Set creation method for option82, users can define the parameters of remote-id suboption by themselves.

Parameters: WORD the defined character string of remote-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure remote-id on interface, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occupies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp relay information option delimiter** configuration).

Example: Set self-defined method and character string of remote-id suboption are hostname and abc respectively for option82.

Switch(config)#ip dhcp relay information option self-defined remote-id hostname string abc

4.17.7 ip dhcp relay information option self-defined remote-id format

Command: ip dhcp relay information option self-defined remote-id format [ascii | hex]

Function: Set self-defined format of remote-id for relay option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format use ip dhcp relay information option type self-defined remote-id to create remote-id format.

Example: Set self-defined method of remote-id as hex for relay option82.

Switch(config)# ip dhcp relay information option self-defined remote-id format hex

4.17.8 ip dhcp relay information option self-defined subscriber-id

Command: ip dhcp relay information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD }

no ip dhcp relay information option self-defined subscriber-id

Function: Set creation method for option82, users can define the parameters of circute-id suboption by themselves.

Parameters: WORD the defined character string of circuit-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure circuit-id on interface, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined format is ascii, the filled format of vlan such as “Vlan2”, the format of port such as “Ethernet1/0/1”, the format of mac and remote-mac such as “00-02-d1-2e-3a-0d”. If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp relay information option delimiter** configuration).

Example: Set self-defined method of circuit-id suboption as port, mac for option82.

Switch(config)# ip dhcp relay information option self-defined subscriber-id port id switch-id mac

4.17.9 ip dhcp relay information option self-defined subscriber-id format

Command: ip dhcp relay information option self-defined subscriber-id format [ascii | hex]

Function: Set self-defined format of circuit-id for relay option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format use ip dhcp relay information option type self-defined subscriber-id to create circuit-id format.

Example: Set self-defined format of circuit-id as hex for relay option82.

Switch(config)# ip dhcp relay information option self-defined subscriber-id format hex

4.17.10 ip dhcp relay information option subscriber-id

Command: ip dhcp relay information option subscriber-id {standard | *<circuit-id>*}

no ip dhcp relay information option subscriber-id

Function: This command is used to set the format of option82 sub-option1 (Circuit ID option) added to the DHCP request messages from interface, **standard** means the standard vlan name and physical port name format, like “Vlan2+Ethernet1/0/12”, ***<circuit-id>*** is the circuit-id contents of option82 specified by users, which is a string no longer than 64 characters. The “**no ip dhcp relay information option subscriber-id**” command will set the format of added option82 sub-option1 (Circuit ID option) as standard format.

Parameters: None

Command Mode: Interface configuration mode.

Default Settings: The system uses the standard format to set the circuit-id of option 82 by default.

User Guide: Because the option 82 information added for the switch should cooperate with the third party DHCP server, if the standard circuit-id format of the switch cannot satisfy the server’s

request, this method will be provided for users to specify the contents of circuit-id according to the situation of the server.

Example: Set the sub-option circuit-id of DHCP option82 as foobar.

Switch(config-if-vlan1)#ip dhcp relay information option subscriber-id foobar

4.17.11 ip dhcp relay information option subscriber-id format

Command: ip dhcp relay information option subscriber-id format {hex | acsii | vs-hp|vs-cisco}

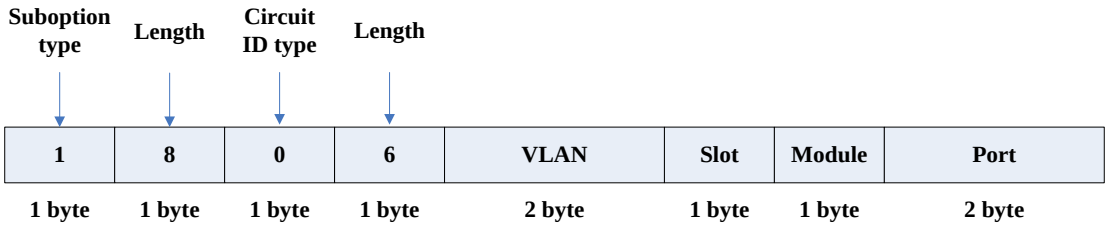
Function: Set subscriber-id format of Relay Agent option82.

Parameters: hex means that subscriber-id is VLAN and port information with hexadecimal format, acsii means that subscriber-id is VLAN and port information with ACSII format. vs-hp means that subscriber-id is compatible with the format of HP manufacturer.vs-cisco means that subscriber-id is compatible with the format of CISCO manufacturer.

Command Mode: Global mode

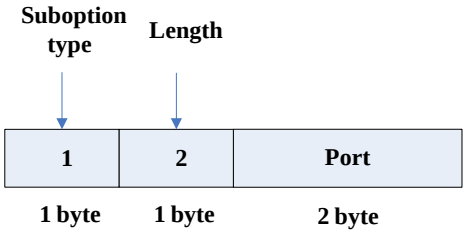
Default: ascii.

User Guide: VLAN and port information with ASCII format, such as “Vlan1+Ethernet1/0/11”, VLAN and port information with hexadecimal format defined as below:



VLAN field fills in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

Example: Set subscriber-id format of Relay Agent option82 as hexadecimal format.

Switch(config)#ip dhcp relay information option subscriber-id format hex

4.17.12 ip dhcp relay information policy

Command: ip dhcp relay information policy {drop | keep | replace}

no ip dhcp relay information policy

Function: This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The drop mode means that if the message has option82, then the system will drop it without processing; keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process; replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process. The "no ip dhcp relay information policy" will set the retransmitting policy of the option 82 DCHP message as "replace".

Parameters: None

Command Mode: Interface configuration mode.

Default Settings: The system uses replace mode to replace the option 82 segment in the existing message with its own option 82.

User Guide: Since the DHCP client messages might go through several DHCP Relay Agents when passed to the DHCP server, the latter Relay Agents on the path should set policies to decide how to process the option82 added by Relay Agents before them. The selection of option 82 retransmitting policies should take the configuration policy of the DHCP server into account.

Example: Set the retransmitting policy of DHCP messages option 82 as keep.

Switch(Config-if-Vlan1)# ip dhcp relay information policy keep

4.17.13 ip dhcp server relay information enable

Command: ip dhcp server relay information enable

no ip dhcp server relay information enable

Function: This command is used to enable the switch DHCP server to identify option82. The "no ip dhcp server relay information enable" command will make the server ignore the option 82.

Parameters: None

Command Mode: Global configuration mode

Default Setting: The system disable the option82 identifying function by default.

User Guide: If the users want the switch DHCP server to identify option82 and return option 82 information in the reply message, this command needs to be set, or, the switch DHCP server will ignore the option82.

Example: Set the DHCP server to support option82

Switch(Config-if-Vlan1)# ip dhcp server relay information enable

4.17.14 show ip dhcp relay information option

Command: show ip dhcp relay information option

Function: This command will display the state information of the DHCP option 82 in the system, including option82 enabling switch, the interface retransmitting policy, the circuit ID mode and the switch DHCP server option82 enabling switch.

Parameters: None.

Command Mode: Admin and Global Configuration Mode.

User Guide: Use this command to check the state information of Relay Agent option82 during

operation.

Example:

Switch#show ip dhcp relay information option

ip dhcp server relay information option(i.e. option 82) is disabled

ip dhcp relay information option(i.e. option 82) is enabled

Vlan2:

ip dhcp relay information policy keep

ip dhcp relay information option subscriber-id standard

Vlan3:

ip dhcp relay information policy replace

ip dhcp relay information option subscriber-id foobar

4.18 DHCP Snooping

4.18.1 debug ip dhcp snooping binding

Command: debug ip dhcp snooping binding

no debug ip dhcp snooping binding

Function: This command is use to enable the DHCP SNOOPING debug switch to debug the state of binding data of DHCP SNOOPING.

Command Mode: Admin mode

Usage Guide: This command is mainly used to debug the state of DHCP SNOOPING task when it adds ARP list entries, dot1x users and trusted user list entries according to binding data.

4.18.2 debug ip dhcp snooping event

Command: debug ip dhcp snooping event

no debug ip dhcp snooping event

Function: This command is use to enable the DHCP SNOOPING debug switch to debug the state of DHCP SNOOPING task.

Command Mode: Admin mode.

Usage Guide: This command is mainly used to debug the state of DHCP SNOOPING task and available of outputting the state of checking binding data and executing port action and so on.

4.18.3 debug ip dhcp snooping packet

Command: debug ip dhcp snooping packet

no debug ip dhcp snooping packet

Function: This command is used to enable the DHCP SNOOPING debug switch to debug the

message-processing procedure of DHCP SNOOPING.

Command Mode: Admin Mode.

Usage Guide: The debug information that the DHCP SNOOPING is processing messages, including every step in the message-processing procedure: adding alarm information, adding binding information, transmitting DHCP messages, adding/peeling option 82 and etc.

4.18.4 debug ip dhcp snooping packet interface

Command: debug ip dhcp snooping packet interface {[ethernet] *<InterfaceName>*}

no debug ip dhcp snooping packet {[ethernet] *<InterfaceName>*} Function: This command is used to enable the DHCP SNOOPING debug switch to debug the information that DHCP SNOOPING is receiving a packet.

Parameters: *<InterfaceName>:* Interface name.

Command Mode: Admin Mode.

Usage Guide: The information that DHCP Snooping is receiving messages from a specific port.

4.18.5 debug ip dhcp snooping ha

Command: debug ip dhcp snooping ha

no debug ip dhcp snooping ha

Function: This command is used to turn on the DHCP snooping debugging switch and debug the process of DHCP snooping handling HA.

Command mode: privileged user configuration mode.

Usage guide: DHCP snooping handles debugging information for HA. These debugging information include each step of the HA processing flow, such as sending and receiving HA messages.

4.18.6 debug ip dhcp snooping update

Command: debug ip dhcp snooping update

no debug ip dhcp snooping update

Function: This command is use to enable the DHCP snooping debug switch to debug the communication information between DHCP snooping and helper server.

Command Mode: Admin Mode.

Usage Guide: Debug the information of communication messages received and sent by DHCP snooping and helper server.

4.18.7 enable trustview key

Command: enable trustview key {0 | 7} *<password>*

no enable trustview key

Function: To configure DES encrypted key for private packets, this command is also the switch for

the private packets encrypt and hash function enabled or not.

Parameter: ***<password>*** is character string length less than 16, which use as encrypted key. 0 for un-encrypted text for the password, while 7 for encrypted.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: The switch communicates with the TrustView management system through private protocols. By default these packets are not encrypted. In order to prevent spoofing, it can be configured to encrypt these packets. And at the same time, the same password should be configured on TrustView server.

Example: Enable encrypt or hash function of private message.

Switch(config)# enable trustview key 0 test

4.18.8 ip dhcp snooping

Command: ip dhcp snooping enable

no ip dhcp snooping enable

Function: Enable the DHCP Snooping function.

Parameters: None.

Command Mode: Globe mode.

Default Settings: DHCP Snooping is disabled by default.

Usage Guide: When this function is enabled, it will monitor all the DHCP Server packets of non-trusted ports.

Example: Enable the DHCP Snooping function.

switch(config)#ip dhcp snooping enable

4.18.9 ip dhcp snooping action

Command: ip dhcp snooping action {shutdown | blackhole} [recovery <*second*>]

no ip dhcp snooping action

Function: Set or delete the automatic defense action of a port.

Parameters:

shutdown: When the port detects a fake DHCP Server, it will be shutdown.

blackhole: When the port detects a fake DHCP Server, the vid and source MAC of the fake packet will be used to block the traffic from this MAC.

recovery: Users can set to recover after the automatic defense action being executed.(no shut ports or delete correponding blackhole）.

second: Users can set how long after the execution of defense action to recover. The unit is second, and valid range is 10-3600.

Command Mode: Port mode

Default Settings: No default defense action.

Usage Guide: Only when DHCP Snooping is globally enabled, can this command be set. Trusted port will not detect fake DHCP Server, so, will never trigger the corresponding defense action. When a port turns into a trusted port from a non-trusted port, the original defense action of the

port will be automatically deleted.

Example: Set the DHCP Snooping defense action of port ethernet1/0/1 as setting blackhole, and the recovery time is 30 seconds.

switch(config)#interface ethernet 1/0/1

switch(Config-Ethernet1/0/1)#ip dhcp snooping action blackhole recovery 30

4.18.10 ip dhcp snooping action MaxNum

Command: ip dhcp snooping action {<maxNum>|default}

Function: Set the number of defense action that can be simultaneously took effect.

Parameters: ***<maxNum>***: the number of defense action on each port, the range of which is 1-200, and the value of which is 10 by default.

default: recover to the default value.

Command Mode: Globe mode

Default Settings: The default value is 10.

Usage Guide: Set the max number of defense actions to avoid the resource exhaustion of the switch caused by attacks. If the number of alarm information is larger than the set value, then the earliest defense action will be recovered forcibly in order to send new defense actions.

Example: Set the number of port defense actions as 100.

switch(config)#ip dhcp snooping action 100

4.18.11 ip dhcp snooping binding

Command: ip dhcp snooping binding enable

no ip dhcp snooping binding enable

Function: Enable the DHCP Snooping binding funciton

Parameters: None.

Command Mode: Globe mode

Default Settings: DHCP Snooping binding is disabled by default.

Usage Guide: When the function is enabled, it will record the binding information allocated by DHCP Server of all trusted ports. Only after the DHCP SNOOPING function is enabled, the binding function can be enabled.

Example: Enable the DHCP Snooping binding funciton.

switch(config)#ip dhcp snooping binding enable

Relative Command: ip dhcp snooping enable

4.18.12 ip dhcp snooping binding arp

Command: ip dhcp snooping binding arp

no **ip dhcp snooping binding arp**

Function: Enable the DHCP Snooping binding ARP funciton.

Parameters: None

Command Mode: Globe mode

Default Settings: DHCP Snooping binding ARP funciton is disabled by default.

Usage Guide: When this function is enbaled, DHCP SNOOPING will add binding ARP list entries according to binding information. Only after the binding function is enabled, can the binding ARP function be enabled. Binding ARP list entries are static entries without configuration of reservation, and will be added to the NEIGHBOUR list directly. The priority of binding ARP list entries is lower than the static ARP list entries set by administrator, so can be overwritten by static ARP list entries; but, when static ARP list entries are deleted, the binding ARP list entries can not be recovered untill the DHCP SNOOPING recapture the biding inforamtion. Adding binding ARP list entries is used to prevent these list entried from being attacked by ARP cheating. At the same time, these static list entries need no reauthenticaiton, which can prenvent the switch from the failing to reauthenticate ARP when it is being attacked by ARP scanning.

Only after the DHCP SNOOPING binding function is enabled, the binding ARP function can be set.

Example: Enable the DHCP Snooping binding ARP funciton.

switch(config)#ip dhcp snooping binding arp

Relative Command: ip dhcp snooping binding enable

4.18.13 ip dhcp snooping binding dot1x

Command: ip dhcp snooping binding dot1x

no ip dhcp snooping binding dot1x

Function: Enable the DHCP Snooping binding DOT1X funciton.

Parameters: None

Command Mode: Port mode

Default Settings: By default, the binding DOT1X funciton is disabled on all ports.

Usage Guide: When this function is enabled, DHCP SNOOPING will notify the DOT1X module about the captured bindng information as a DOT1X controlled user. This command is mutually exclusive to”ip dhcp snooping binding user-contro“command.

Only after the DHCP SNOOPING binding function is enabled, the binding dot1x function can be set.

Example: Enable the binding DOT1X funciton on port ethernet1/0/1.

switch(config)#interface ethernet 1/0/1

switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding dot1x

Relative Command: ip dhcp snooping binding enable

ip dhcp snooping binding user-control

4.18.14 ip dhcp snooping binding user

Command: ip dhcp snooping binding user <mac> address <ipaddress> vlan <vid> interface *[*Ethernet*] <ifname>*

no ip dhcp snooping binding user <*mac*> interface [Ethernet] <*ifname*>

Function: Configure the information of static binding users.

Parameters:

<*mac*>: The MAC address of the static binding user, whic is the only index of the binding user.

<*ipaddress*>: The IP address of the static binding user.

<*vid*>: The VLAN ID which the static binding user belongs to.

<ifname>: The access interface of static binding user.

Command Mode: Globe mode

Default Settings: DHCP Snooping has no static binding list entry by default.

Usage Guide: The static binding users is deal in the same way as the dynamic binding users captured by DHCP SNOOPING; the follwoing actions are all allowed: notifying DOT1X to be a controlled user of DOT1X, adding a trusted user list entry directly, adding a bingding ARP list entry. The static binding uses will never be aged, and have a priority higher than dynamic binding users. Only after the DHCP SNOOPING binding function is enabled, the static binding users can be enabled.

Example: Configure static binding users.

switch(config)#ip dhcp snooping binding user 00-03-0f-12-34-56 address 192.168.1.16 interface Ethernet 1/0/16

Relative Command: **ip dhcp snooping binding enable**

4.18.15 ip dhcp snooping binding user-control

Command: ip dhcp snooping binding user-control

no ip dhcp snooping binding user-control

Function: Enable the binding user funtion.

Parameters: None.

Command Mode: Port Mode.

Default Settings: By default, the binding user funciton is disabled on all ports.

Usage Guide: When this function is enabled, DHCP SNOOPING will treat the captured binding information as trusted users allowed to access all resources. This command is mutually exclusive to “ip dhcp snooping binding dot1x“ command.

Only after DHCP SNOOPING binding function is enabled, the binding user function can be set. This command is not limited by “ip dhcp snooping“ based on VLAN, but it is only limited by the global “ip dhcp snooping enable“ command.

Example: Enable the binding USER funciton on port ethernet1/0/1.

switch(config)#interface ethernet 1/0/1

switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding user-control

Relative Command: ip dhcp snooping binding enable

ip dhcp snooping binding dot1x

4.18.16 ip dhcp snooping binding user-control max-user

Command: ip dhcp snooping binding user-control max-user *<number>*

no ip dhcp snooping binding user-control max-user

Function: Set the max number of users allowed to access the port when enabling DHCP Snooping binding user funciton; the no operation of this command will restore default value.

Parameters: *<number>* the max number of users allowed to access the port, from 0 to 1024.

Command Mode: Port Configuration Mode.

Default Settings: The max number of users allowed by each port to access is 1024.

Usage Guide: This command defines the max number of trust users distributed according to binding information, with **ip dhcp snooping binding user-contrl** enabled on the port. By default, the number is 1024. Considering the limited hardware resources of the switch, the actual number of trust users distributed depends on the resource amount. If a bigger max number of users is set using this command, DHCP Snooping will distribute the binding informaiton of untrust users to hardware to be trust users as long as there is enough available resources. Otherwise, DHCP Snooping will change the distributed binging informaiton accordint to the new smaller max user number. When the number of distributed bingding informaiton entries reaches the max limit, no new DHCP will be able to become trust user or to access other network resouces via the switch.

Examples: Enable DHCP Snooping binding user funtion on Port ethernet1/0/1, setting the max number of user allowed to access by Port Ethernet1/0/1 as 5.

Switch(Config-If-Ethernet1/0/1)# ip dhcp snooping binding user-control max-user 5

Related Command: ip dhcp snooping binding user-control

4.18.17 ip dhcp snooping information enable

Command: ip dhcp snooping information enable

no ip dhcp snooping information enable

Function: This command will enable option 82 function of DHCP Snooping on the switch, the no operation of this command will disable that function.

Parameters: None.

Default Settings: Option 82 function is disabled in DHCP Snooping by default.

Command Mode: Global Configuration Mode.

Usage Guide: Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like vlan1+ethernet1/0/12. That of option2 in option 82 (remote ID option) is CPU MAC of the switch, like 00030f023301. If a DHCP request message with option 82 options is received, DHCP Snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP Snooping will dump those options in the message and forward it.

Examples: Enable option 82 function of DHCP Snooping on the switch.

Switch(config)#ip dhcp snooping enable

Switch(config)# ip dhcp snooping binding enable
Switch(config)# ip dhcp snooping information enable

4.18.18 ip dhcp snooping information option allow-untrusted (replace|)

Command：ip dhcp snooping information option allow-untrusted (replace|)
no ip dhcp snooping information option allow-untrusted (replace|)

Function: This command is used to set that allow untrusted ports of DHCP snooping to receive DHCP packets with option82 option. When the "replace" is setting, the potion82 option is allowed to replace. When disabling this command, all untrusted ports will drop DHCP packets with option82 option.

Parameter: None.

Command Mode: Global Mode

Default: Drop DHCP packets with option82 option received by untrusted ports.

Usage Guide: Usually the switch with DHCP snooping function connects the terminal user directly, so close allow-untrusted by default to avoid option82 option added by user privately. Please set uplink port as trust port when enabling the uplink of DHCP snooping function.

Example: Enable the function that receives DHCP packets with option82.

Switch(config)#ip dhcp snooping information option allow-untrusted

4.18.19 ip dhcp snooping information option delimiter

Command: ip dhcp snooping information option delimiter [colon | dot | slash | space]
no ip dhcp snooping information option delimiter

Function: Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash.

Parameters: None.

Default Settings: slash (“/”).

Command Mode: Global mode

Usage Guide: Divide parameters with the configured delimiters after users have defined them which are used to create suboption (remote-id, circuit-id) of option82 in global mode.

Example: Set the parameter delimiters as dot (“.”) for suboption of option82.

Switch(config)# ip dhcp snooping information option delimiter dot

4.18.20 ip dhcp snooping information option remote-id

Command: ip dhcp snooping information option remote-id {standard | *<remote-id>*}
no ip dhcp snooping information option remote-id

Function: Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (they are received by the port). The no command sets the additive suboption2 (remote ID option) format of option 82 as standard.

Parameters: standard means the default VLAN MAC format. ***<remote-id>*** means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.
Command Mode: Global Mode
Default: Use standard format to set remote-id.
Usage Guide: The additive option 82 needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format can not satisfy server's request.
Example: Set the suboption remote-id of DHCP option82 as street-1-1.
Switch(config)#ip dhcp snooping information option remote-id street-1-1

4.18.21 ip dhcp snooping information option self-defined remote-id

Command: ip dhcp snooping information option self-defined remote-id {hostname | mac | string WORD}
no ip dhcp snooping information option self-defined remote-id
Function: Set creation method for option82, users can define the parameters of remote-id suboption by themselves.
Parameters: WORD the defined character string of remote-id by themselves, the maximum length is 64.
Command Mode: Global Mode
Default: Using standard method.
Usage Guide: After configure this command, if users do not configure ip dhcp snooping information option remote-id globally, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occpies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp snooping information option delimiter** configuration).
Example: Set self-defined method and character string of remote-id suboption are mac and abc respectively for option82.
Switch(config)# ip dhcp snooping information option self-defined remote-id mac string abc

4.18.22 ip dhcp snooping information option self-defined remote-id format

Command: ip dhcp snooping information option self-defined remote-id format [ascii | hex]
Function: Set self-defined format of remote-id for snooping option82.
Parameters: None.
Command Mode: Global Mode
Default: ascii.
Usage Guide: self-defined format use ip dhcp snooping information option type self-defined

remote-id to create remote-id format.

Example: Set self-defined format of remote-id as hex for snooping option82.

Switch(config)# ip dhcp snooping information option self-defined remote-id format hex

4.18.23 ip dhcp snooping information option self-defined subscriber-id

Command: ip dhcp snooping information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac) | string WORD}

no ip dhcp snooping information option type self-defined subscriber-id

Function: Set creation method for option82, users can define the parameters of circute-id suboption by themselves.

Parameters: WORD the defined character string of circuit-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure circuit-id on port, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined subscriber-id format is ascii, the filled format of vlan such as “Vlan2”, the format of port such as “Ethernet1/0/1”, the format of mac and remote-mac such as “00-02-d1-2e-3a-0d”. If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp snooping information option delimiter** configuration).

Example: Set self-defined method of circuit-id suboption as vlan, port, mac and remote-mac for option82.

Switch(config)#ip dhcp snooping information option self-defined subscriber-id vlan port id remote-mac

4.18.24 ip dhcp snooping information option self-defined subscriber-id format

Command: ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]

Function: Set self-defined format of circuit-id for snooping option82.

Parameters: None.

Command Mode: Global Mode

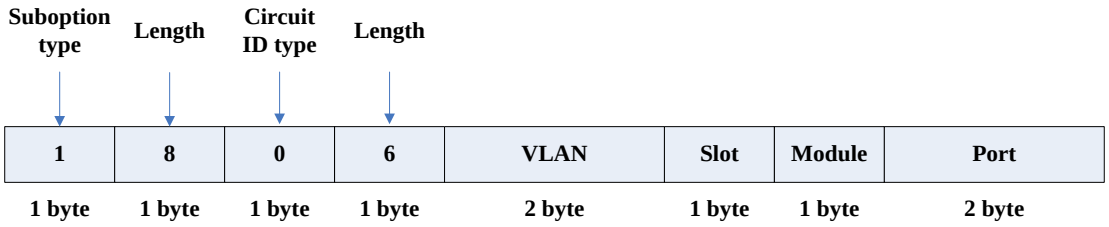
Default: ascii.

Usage Guide: self-defined format uses ip dhcp snooping information option type self-defined subscriber-id to create circuit-id format.

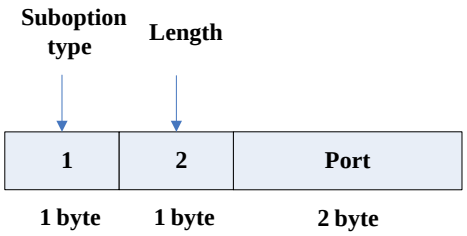
Example: Set self-defined format of circuit-id as hex for snooping option82.
Switch(config)#ip dhcp snooping information option self-defined subscriber-id format hex

4.18.25 ip dhcp snooping information option subscriber-id format

Command: ip dhcp snooping information option subscriber-id format {hex | acsii | vs-hp}
Function: This command is used to set subscriber-id format of DHCP snooping option82.
Parameters: hex means that subscriber-id is VLAN and port information with hexadecimal format, acsii means that subscriber-id is VLAN and port information with ACSII format. vs-hp means that subscriber-id is compatible with the format of HP manufacturer.
Command Mode: Global mode
Default: ascii.
User Guide : VLAN and port information with ASCII format, such as Vlan1+Ethernet1/0/11, VLAN and port information with hexadecimal format defined as below:



VLAN field fill in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.
The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.
Example: Set subscriber-id format of DHCP snooping option82 as hexadecimal format.
Switch(config)#ip dhcp snooping information option subscriber-id format hex

4.18.26 ip dhcp snooping timeout detection

Command: ip dhcp snooping timeout detection <0-7200>
no ip dhcp snooping timeout detection
Function: Set the traffic monitoring timeout for binding table entries.
Parameter: The configurable timeout range for traffic monitoring is 0-7200, with a default value

of 3. The unit is seconds.
Command mode: Global configuration mode.
Usage guide: When the bound table entry is in protected mode, after a certain period of time, it will check whether there is any traffic from the source MAC passing through during that time period; If there is traffic passing through, it will continue to be in protected mode; If there is no traffic passing through, a silent timer will be started and it will remain in protected mode during the silent period. If no traffic passes through during the silent period, delete the protected mode of the table entry.
give an example: (Config)#ip dhcp snooping timeout detection 100

4.18.27 ip dhcp snooping timeout quiet

Command：ip dhcp snooping timeout quiet <0-4294967295>
no ip dhcp snooping timeout quiet
Function：Set the traffic monitoring silence time of the bound table item。
Parameters：The configurable silent time range for traffic monitoring is 0-4294967295, and the default value is 0. In seconds。
Command Mode：Globle mode。
Usage Guide：When the binding table item is in protection mode, it will check whether there is traffic of the source mac in this period of time after each period of time; If traffic passes, it will continue to be in protection mode; If no traffic passes, the silent timer will be started and it will remain in the protection mode during the silent period. If no traffic passes during the silence period, the protection mode of the table item is deleted.

Example：(Config)#ip dhcp snooping timeout quiet 1000

4.18.28 ip dhcp snooping trust

Command: ip dhcp snooping trust
no ip dhcp snooping trust
Function: Set or delete the DHCP Snooping trust attributes of a port.
Parameters: None
Command Mode: Port mode
Default Settings: By default, all ports are non-trusted ports
Usage Guide: Only when DHCP Snooping is globally enabled, can this command be set. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted; all the security history records will be cleared (except the information in system log).
Example: Set port ethernet1/0/1 as a DHCP Snooping trusted port
switch(config)#interface ethernet 1/0/1
switch(Config- Ethernet 1/0/1)#ip dhcp snooping trust

4.18.29 ip dhcp snooping vlan

Command: IP DHCP snooping VLAN (WORD |)
no ip dhcp snooping vlan (WORD |)
Function: Enable DHCP snooping function in VLAN.
Parameter: No parameters. By default, DHCP snooping is enabled on all VLANs, otherwise DHCP snooping is enabled on the VLANs specified by the parameters.
Command mode: Global configuration mode.
Default situation: The dhcp snooping function is not enabled by default in VLAN.
Usage guide: No IP DHCP snooping VLAN<vlan-id>indicates disabling the DHCP snooping feature on the specified VLAN.
Example: Activate DHCP snooping function.
switch(config)#ip dhcp snooping vlan 10
switch(config)#no ip dhcp snooping vlan 10

4.18.30 ip user helper-address

Command: ip user *helper-address* <svr_addr> [*port* <udp_port>] source <*src*_addr> [secondary]
no ip user helper-address [secondary]
Function: Set the address and port of HELPER SERVER.
Parameters:
<svr_addr>: The IP address of HELPER SERVER IP in dotted-decimal notation.
udp_port: The UDP port of HELPER SERVER, the range of which is1—65535, and its default value is 9119.
src_addr: The local management IP address of the switch, in dotted-decimal notation.
sencondary: Whether it is a secondary SERVER address.
Command Mode: Global mode
Default Settings: There is no HELPER SERVER address by default.
Usage Guide: DHCP SNOOPING will send the monitored binding information to HELPER SERVER to save it. If the switch starts abnormally, it can recover the binding data from HELPER SERVER. The HELPER SERVER function usually is integrated into DCBI packet. The DHCP SNOOPING and HELPER SERVER use the UDP protocol to communicate, and guarantee the arrival of retransmitted data. HELPER SERVER configuration can also be used to sent DOT1X user data from the server, the detail of usage is described in the chapter of **dot1x configuration**.
Two HELPER SERVER addresses are allowed, DHCP SNOOPING will try to connect to PRIMARY SERVER in the first place. Only when the PRIMARY SERVER is unreachable, will the switch c HELPER SERVER connects to SECONDARY SERVER.
Please pay attention: source address is the effective management IP address of the switch, if the management IP address of the switch changes, this configuration should be updated in time.
Example: Set the local management IP address as 100.1.1.1, primary HELPER SERVER address as 100.1.1.100 and the port as default value.
switch(config)#interface vlan 1
switch(Config- If-Vlan1)#ip address 100.1.1.1 255.255.255.0
switch(Config-if-Vlan1)exit
switch(config)#ip user helper-address 100.1.1.100 source 100.1.1.1

4.18.31 ip user private packet version two

Command: ip user private packet version two

no ip user private packet version two

Function: The switch choose private packet version two to communicate with trustview.

Parameter: None.

Command Mode: Global Mode.

Default: The switch choose private packet version one to communicate with DCBI.

Usage Guide: If the DCBI access control system is applied, the switch should be configured to use private protocol of version one to communicate with the DCBI server. However, if TrustView is applied, version two should be applied.

Example: To configure the switch choose private packet version two to communicate with inter security management background system.

switch(config)#ip user private packet version two

4.18.32 show ip dhcp snooping

Command: show ip dhcp snooping [interface [ethernet] <*interfaceName*>]

Function: Display the current cofiguration information of dhcp snooping or display the records of defense actions of a specific port.

Parameters: <*interfaceName*>: The name of the specific port.

Command Mode: Admin and Global Configuration Mode.

Default Settings: None.

Usage Guide: If there is no specific port, then display the current cofiguration information of dhcp snooping, otherwise, display the records of defense actions of the specific port.

Example:

switch#show ip dhcp snooping

DHCP Snooping is enabled

DHCP Snooping binding arp: disabled

DHCP Snooping maxnum of action info:10

DHCP Snooping limit rate: 100(pps), switch ID: 0003.0F12.3456

DHCP Snooping droped packets: 0, discarded packets: 0

DHCP Snooping alarm count: 0, binding count: 0,

expired binding: 0, request binding: 0

interface	trust	action	recovery	alarm num	bind num
Ethernet1/0/1	trust	none	0second	0	0
Ethernet1/0/2	untrust	none	0second	0	0
Ethernet1/0/3	untrust	none	0second	0	0
Ethernet1/0/4	untrust	none	0second	0	1
Ethernet1/0/5	untrust	none	0second	2	0

Ethernet1/0/6	untrust	none	0second	0	0
Ethernet1/0/7	untrust	none	0second	0	0
Ethernet1/0/8	untrust	none	0second	0	1
Ethernet1/0/9	untrust	none	0second	0	0
Ethernet1/0/10	untrust	none	0second	0	0
Ethernet1/0/11	untrust	none	0second	0	0
Ethernet1/0/12	untrust	none	0second	0	0
Ethernet1/0/13	untrust	none	0second	0	0
Ethernet1/0/14	untrust	none	0second	0	0
Ethernet1/0/15	untrust	none	0second	0	0
Ethernet1/0/16	untrust	none	0second	0	0
Ethernet1/0/17	untrust	none	0second	0	0
Ethernet1/0/18	untrust	none	0second	0	0
Ethernet1/0/19	untrust	none	0second	0	0
Ethernet1/0/20	untrust	none	0second	0	0
Ethernet1/0/21	untrust	none	0second	0	0
Ethernet1/0/22	untrust	none	0second	0	0
Ethernet1/0/23	untrust	none	0second	0	0
Ethernet1/0/24	untrust	none	0second	0	0

Displayed Information	Explanation
DHCP Snooping is enable	Whether the DHCP Snooping is globally enabled or disabled.
DHCP Snooping binding arp	Whether the ARP binding function is enabled.
DHCP Snooping maxnum of action info	The number limitation of port defense actions
DHCP Snooping limit rate	The rate limitation of receiving packets
switch ID	The switch ID is used to identify the switch, usually using the CPU MAC address.
DHCP Snooping droped packets	The number of dropped messages when the received DHCP messages exceeds the rate limit.
discarded packets	The number of discarded packets caused by the communication failure within the system. If the CPU of the switch is too busy to schedule the DHCP SNOOPING task and thus can not handle the received DHCP messages, such situation might happen.
DHCP Snooping alarm count:	The number of alarm information.
binding count	The number of binding information.
expired binding	The number of binding information which is already expired but has not been deleted. The reason why the expired information is not deleted immediately might be that the switch needs to notify the helper server about the information, but the helper server has not

	acknowledged it.
request binding	The number of REQUEST information
interface	The name of port
trust	The truest attributes of the port
action	The automatic defense action of the port
recovery	The automatic recovery time of the port
alarm num	The number of history records of the port automatic defense actions
bind num	The number of port-relative binding information.

switch#show ip dhcp snooping int Ethernet1/0/1
interface Ethernet1/0/1 user config:
trust attribute: untrust
action: none
binding dot1x: disabled
binding user: disabled
recovery interval:0(s)
Alarm info: 0

Binding info: 0

Expired Binding: 0

Request Binding: 0

Displayed Information	Explanation
interface	The name of port
trust attribute	The truest attributes of the port
action	The automatic defense action of the port
recovery interval	The automatic recovery time of the port
maxnum of alarm info	The max number of automatic defense actions that can be recorded by the port
binding dot1x	Whether the binding dot1x function is enabled on the port
binding user	Whether the binding user function is enabled on the port.
Alarm info	The number of alarm information.
Binding info	The number of binding information.
Expired Binding	The expired binding information
Request Binding	REQUEST information

4.18.33 show ip dhcp snooping binding all

Command: show ip dhcp snooping binding all

Function: Display the current global binding information of DHCP snooping.

Parameters: None.

Command Mode: Admin and Global Configuration Mode.

Default Settings: None.

Usage Guide: This command can check the global binding information of DHCP snooping, each table entry includes the corresponding MAC address, IP address, port name, VLAN ID and the flag of the binding state. Besides, DHCP Snooping must be enabled globally, this command can be configured.

Example:

switch#show ip dhcp snooping binding all

ip dhcp snooping static binding count:1169, dynamic binding count:0

MAC	IP address	Interface	Vlan ID	Flag
00-00-00-00-11-11	192.168.40.1	Ethernet1/0/1	1	S
00-00-00-00-00-10	192.168.40.10	Ethernet1/0/2	1	D
00-00-00-00-00-11	192.168.40.11	Ethernet1/0/4	1	D
00-00-00-00-00-12	192.168.40.12	Ethernet1/0/4	1	D
00-00-00-00-00-13	192.168.40.13	Ethernet1/0/4	1	SU
00-00-00-00-00-14	192.168.40.14	Ethernet1/0/4	1	SU
00-00-00-00-00-15	192.168.40.15	Ethernet1/0/5	1	SL
00-00-00-00-00-16	192.168.40.16	Ethernet1/0/5	1	SL

The flag explanation of the binding state:

S The static binding is configured by shell command

D The dynamic binding type

U The binding is uploaded to the server

R The static binding is configured by the server

O DHCP response with the option82

L The hardware drive is announced by the binding

X Announcing dot1x module is successful

E Announcing dot1x module is failing

4.18.34 show trustview status

Command: show trustview status

Function: To show all kinds of private packets state information, which sending or receiving from TrustView (inter security management background system).

Parameter: None.

Command Mode: Admin and Global Configuration Mode.

Default: None.

Usage Guide: This command can be used for debugging the communication messages between the switch and the TrustView server, messages such as protocol version notification, encryption negotiation, free resource and web URL redirection, and the number of forced log-off messages, as well as the number of forced accounting update messages, can be displayed.

Example:

```
Switch#show trustview status
Primary TrustView Server 200.101.0.9:9119
    TrustView version2 message inform successed
    TrustView inform free resource successed
    TrustView inform web redirect address successed
    TrustView inform user binding data successed
TrustView version2 message encrypt/digest enabled
Key: 08:02:33:34:35:36:37:38
Rcvd 106 encrypted messages, in which MD5-error 0 messages, DES-error 0 messages
Sent 106 encrypted messages
Free resource is 200.101.0.9/255.255.255.255
Web redirect address for unauthencated users is <http://200.101.0.9:8080>
Rcvd 0 force log-off packets
Rcvd 19 force accounting update packets
Using version two private packet
```

4.19 DHCP option 60 and option 43

4.19.1 option 43 ascii LINE

Command: option 43 ascii LINE

no option 43

Function: Configure option 43 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 43.

Parameter: LINE: The configured option 43 character string with ascii format, its length range between 1 and 255.

Default: No option 43 character string is configured.

Command Mode: ip dhcp pool mode

Usage Guide: None.

Example: Configure option 43 with ascii format to be "AP 1000".

```
switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 43 ascii AP 1000
```

4.19.2 option 43 hex WORD

Command: option 43 hex WORD

no option 43

Function: Configure option 43 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 43.

Parameter: WORD: The configured option 43 character string with hex format, such as a1241b.

Default: No option 43 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: When using hex method to configure option 43, the string needs to be written according to TLV (Type-Length-Value) format. For example, issue ip address of 10.1.1.1 through option 43, then the hex string here should be 01040A010101; Type=0x01, it means IP address; Length=0x04, it means the length of IP address is 4 Bytes; Value=0x0A010101, it means the hexadecimal format of 10.1.1.1.

Example: Configure option 43 with hex format to be "01040a010101".

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 43 hex 01040a010101

4.19.3 option 43 ip A.B.C.D

Command: option 43 ip A.B.C.D

no option 43

Function: Configure option 43 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 43.

Parameter: A.B.C.D: The configured option 43 with IP format, such as 192.168.1.1.

Default: No option 43 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: Using this command to configure option 43, such as "192.168.1.1", then option 43 filled in packets is "C0A80101".

Example: Configure option 43 with IP format to be "192.168.1.1".

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 43 ip 192.168.1.1

4.19.4 option 60 ascii LINE

Command: option 60 ascii LINE

no option 60

Function: Configure option 60 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 60.

Parameter: LINE: The configured option 60 character string with ascii format, its length range between 1 and 255.

Default: No option 60 character string is configured.

Command Mode: ip dhcp pool mode

Usage Guide: None.

Example: Configure option 60 with ascii format to be "AP 1000".

switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 60 ascii AP 1000

4.19.5 option 60 hex WORD

Command: option 60 hex WORD

no option 60

Function: Configure option 60 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 60.

Parameter: WORD: The configured option 60 character string with hex format, such as a1241b.

Default: No option 60 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: None.

Example: Configure option 60 with hex format to be "41502031303030".

switch(config)#ip dhcp pool a
switch(dhcp-a-config)#option 60 hex 41502031303030

4.19.6 option 60 ip A.B.C.D

Command: option 60 ip A.B.C.D

no option 60

Function: Configure option 60 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 60.

Parameter: A.B.C.D: The configured option 60 with IP format, such as 192.168.1.1.

Default: No option 60 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: Using this command to configure option 60, such as "192.168.1.1", option 60 of packets matched with the configured option 60 is "C0A80101".

Example: Configure option 60 with IP format to be "192.168.1.1".

switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 60 ip 192.168.1.1

Chapter 5 Commands for Routing Protocol

5.1 Routing Protocol Overview

5.1.1 ip prefix-list description

Command: ip prefix-list <*list_name*> description <*description*>

no ip prefix-list <*list_name*> description

Function: Configure the description of the prefix-list. The "**no ip prefix-list <*list_name*> description**" command deletes the description contents.

Parameter: ***<list _name>*** is the name of the prefix-list; ***<description>*** is the description contents.

Default: None.

Command Mode: Global Mode

Usage Guide: This command can be used for explaining and describing a prefix-list, e.g. the application and attention matters of the prefix-list.

Example:

Switch#config terminal

Switch(config)#ip prefix-list 3 description This list is used by BGP

5.1.2 ip prefix-list seq

Command: ip prefix-list <*list_name*> [seq <*sequence_number*>] <deny | permit> < any / *ip_addr/mask_length* [ge <*min_prefix_len*>] [le <*max_prefix_len*>]>

no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any / *ip_addr/mask_length* [ge <*min_prefix_len*>] [le <*max_prefix_len*>]>]

Function: Configure the prefix-list. The "**no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any / *ip_addr/mask_length* [ge <*min_prefix_len*>] [le <*max_prefix_len*>]>]**" command deletes the prefix-list.

Parameter: ***<list _name>*** is the name of prefix-list, "**seq**" shows the following parameters is the sequence number, ***<sequence_number>*** is the sequence number, "**deny**" means deny this route, "**permit**" means permit this route, "**any**" means adaptive to all packets with any prefix as well as any mask length, ***ip_addr/mask_length*** shows the prefix address (dotted decimal notation) and the length of mask, "**ge**" means greater than or equal to, ***<min_prefix_len>*** is the minimum length of prefix to be matched (ranging between 0～32), "**le**" means less than or equal to, ***<max_prefix_len>*** is the maximum length of prefix to be matched (ranging between 0～32).

Default: None.

Command Mode: Global Mode

Usage Guide: A prefix-list is identified by a prefix-list name. Each prefix-list may include several

items each of which independently specifies a matching scope of network prefix-list type which is identified with a *sequence-number. sequence-number* specifies the sequence of matching check in the prefix-list. In the matching process the switch check in turn every items identified by "*sequence-number*" ascending. Once certain item obtains the conditions then the prefix-list filter is passed (without proceeding into the next item check).

Attentions should be paid on that at least one item match mode should be "permit" when more than one prefix-list items is defined. The deny mode items can be previously defined so to remove the unsuitable routing messages fast. However if all items are at deny mode then none of the routes would be able to pass the filter of this prefix-list. We here can define a "permit 0.0.0.0/0 ge 0 le 32" item after several defined "deny mode" items so to grant the passage for all other routing messages.

Example:

Switch#config terminal

Switch(config)#ip prefix-list mylist seq 12345 deny 10.0.0.0/8 le 22 ge 14

5.1.3 ip prefix-list sequence-number

Command: ip prefix-list sequence-number

no ip prefix-list sequence-number

Function: Enable the sequence-number auto-creation function, the "**no ip prefix-list sequence-number**" command closes the prefix-list sequence-number.

Parameter: None.

Default: Sequence-number auto-creation enabled.

Command Mode: Global Mode

Usage Guide: The command can be used to close the prefix-list sequence-number.

Example:

Switch(config)#no ip prefix-list sequence-number

5.1.4 match as-path

Command: match as-path *<list-name>*

no match as-path [*<list-name>*]

Function: Configure the AS path domain for matching the BGP routing messages. The "**no match as-path [*<list-name>*]**" deletes this configuration.

Parameter: *<list-name >* is the name of access-list.

Command Mode: route-map mode

Usage Guide: This command matches the AS path domain of the BGP routing message following the rules specified in the as-path list. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match as-path 60

5.1.5 match community

Command: match community <*community-list-name* | *community-list-num*> [exact-match]

no match community [<*community-list-name* | *community-list-num*> [exact-match]]

Function: Configure the community attributes of BGP routing messages. The "**no match community [<*community-list-name* | *community-list-num* > [exact-match]]**" command deletes this configuration.

Parameter: <*community-list-name* > is the name of the community-list, **<*community-list-num* >** is the community-list sequence number, ranging between 1～99 (Standard ACL) or 100～199 (Extended ACL), **[exact-match]** means precise matching.

Command Mode: route-map mode

Usage Guide: This command matches the community attributes of the BGP routing message following the rules specified in the community list. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match community 100 exact-match

5.1.6 match interface

Command: match interface <*interface-name* >

no match interface [<*interface-name* >]

Function: Configure to match the interfaces. The "**no match interface [<*interface-name* >]**" deletes this configuration.

Parameter: "**<*interface-name* >**" is the name of the interface.

Command Mode: route-map mode

Usage Guide: This command matches according to the next-hop messages in the route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed. This command is only used in RIP and OSPF protocols.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match interface vlan1

5.1.7 match ip

Command: match ip <address | next-hop> <*ip-acl -name* | *ip-acl -num* | prefix-list *list-name*>

no match ip <address | next-hop> [<*ip-acl -name* | *ip-acl -num* | prefix-list *list-name*>]

Function: Configure the routing prefix or next-hop. The "**no match ip <*address | next-hop*> [<*ip-acl -name* | *ip-acl -num* | prefix-list *list-name*>]**" deletes this configuration.

Parameter: <address > means matching the routing prefix, **<next-hop>**means matching the routing next-hop, ***<ip-acl -name* >** is the name of ip access-list, ***<ip-acl -num* >** is the ip access-list sequence number, ranging between 1～199 or 1300～2699 (extension scope), **prefix-list** means the matching should follow the prefix-list rules, ***list-name*** is the name of prefix-list.

Command Mode: route-map mode

Usage Guide: This command matches according to the next-hop messages or routing prefix in the route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match ip address prefix-list mylist

5.1.8 match ipv6 address

Command: match ipv6 address <*ipv6-acl-name | prefix-list list-name*>

no match ipv6 address [<*ipv6-acl-name | prefix-list list-name*>]

Function: Configure the prefix for ipv6 routing. If the no form command is enaled, the configuration will be removed.

Parameters: address is the routing prefix to be matched. **<ipv6-acl-name>** is the name of ipv6 access list. Or when the **prefix-list** is configured. **list-name** will be the list name to be matched.

Command Mode: route map mode

Usage Guide: When this command is enabled, the prefix-list in the routing table will be used for routing decision. And if matched, the permit deny operation in the route map will be executed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match ipv6 address prefix-list mylist

5.1.9 match ipv6 next-hop

Command: match ipv6 next-hop <*ipv6-address*>

no match ipv6 next-hop [<*ipv6-address*>]

Function: Configure the next hop for ipv6 routing. The no form command will disable the configuration.

Parameters: next-hop is the next station for routing. ipv6-address is the ipv6 address for the ip address of the interface on the next station.

Command Mode: route map mode

Usage Guide: If this command is configured, packets will be delivered according to the next hop information in the routing table. If matched, the permit or deny operation in the route map will be executed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5
Switch(config-route-map)# match ipv6 next-hop 2000::1

5.1.10 match metric

Command: match metric <*metric-val* >

no match metric [<*metric-val* >]

Function: Match the metric value in the routing message. The "**no match metric [<*metric-val* >]**" deletes the configuration.

Parameter: <*metric-val* > is the metric value, ranging between 0～4294967295.

Command Mode: route-map mode

Usage Guide: This command matches according to metric value in the route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match metric 60

5.1.11 match origin

Command: match origin <egp | igp | incomplete >

no match origin <egp | igp | incomplete >

Function: Configure to matching with the origin of the BGP routing message. The "**no match origin <egp | igp | incomplete >**" deletes the configuration.

Parameter: egp means the route is learnt from the external gateway protocols, **igp** means the route is learnt from the internal gateway protocols, **incomplete** means the route origin is uncertain.

Command Mode: route-map mode

Usage Guide: This command matches according to origin message in the BGP route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match origin egp

5.1.12 match route-type

Command: match route-type external <type-1 | type-2 >

no match route-type external [<type-1 | type-2 >]

Function: Configure to matching with the route type of OSPF routing message. The "**no match route-type external [<type-1 | type-2 >]**" deletes the configuration.

Parameter: type-1 means match with the OSPF type 1 external route, **type-2** means match with the OSPF type 2 external route.

Command Mode: route-map mode

Usage Guide: This command matches according to the type of OSPF routes (OSPF AS-external LSA type is either type 1 or type 2). If the matching succeeded, then the “permit” or “deny” action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match route-type external type-1

5.1.13 match tag

Command: match tag <*tag-val* >

no match tag [<*tag-val* >]

Function: Configure to matching with the tag domain of the OSPF routing message. The “**no match tag [<*tag-val* >]**” deletes this configuration.

Parameter: <*tag-val* > is the tag value, ranging between 0～4294967295.

Command Mode: route-map mode

Usage Guide: This command matches according to the tag value in the OSPF route. If the matching succeeded, then the “permit” or “deny” action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match tag 60

5.1.14 route-map

Command: route-map *<map_name>* {deny | permit} *<sequence_num>*

no route-map *<map_name>* [{deny | permit} *<sequence_num>*]

Function: Configure the route-map and entering the route-map mode. The “**no route-map *<map_name>* [{deny | permit} *<sequence_num>*]**” command deletes route-map.

Parameter: *<map_name>* is the name of route-map, **permit** sets route-map matching mode to permit mode, **deny** sets route-map matching mode to permit mode (**set** sub will not be executed under this mode), ***<sequence_num>*** is the route-map sequence number, ranging between 1～65535.

Default: None

Command Mode: Global Mode

Usage Guide: A route-map may consist of several nodes each of which is a check unit. The check sequence among nodes is identified by *sequence-number*. “permit” means the node filter will be passed if all match subs are obtained by current route and then further all the set sub of this node will be executed without entering the check in the next node; if the match subs can not be met, the proceed to the check in next node. Relation among different node should be “or”, namely one node check passed then the route filter is passed when the switch checks each node in turn in the route-map.

Attentions should be paid on that at least one node match mode should be “permit” when more than one node is defined. When a route-map is used for filtering routing messages, if certain routing message can not pass any node check, then it is considered denied by the route-map. If all nodes in the route-map are set to deny mode, then all routing message should not be able to pass that route-map.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match as-path 60

Switch(config-route-map)#set weight 30

5.1.15 set aggregator

Command: set aggregator as *<as-number> <ip_addr>*

no set aggregator as [*<as-number> <ip_addr>*]

Function: Assign an AS number for BGP aggregator. The “**no set aggregator as [*<as-number> <ip_addr>*]**” deletes this configuration.

Parameter: *<as-number >* is the AS number, ***<ip_addr>*** is the ip address of the aggregator shown in decimal notation.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set aggregator as 200 10.1.1.1

5.1.16 set as-path

Command: set as-path prepend <*as-num*>

no set as-path prepend [<*as-num*>]

Function: Add AS numbers in the AS path domain of the BGP routing message. The “**no set as-path prepend [<*as-num*>]**” command deletes this configuration.

Parameter: *<as-num >* is the AS number, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100), circulating inputting several numbers is available.

Command Mode: route-map mode

Usage Guide: To add AS number in the AS domain of the BGP, the AS path length should be lengthened so to affect the best neighbor path option. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set as-path prepend 200 100.100

5.1.17 set atomic-aggregate

Command: set atomic-aggregate

no set atomic-aggregate

Function: Configure the atomic aggregate attributes. The "**no set atomic-aggregate**" command deletes this configuration.

Parameter: None

Command Mode: route-map mode

Usage Guide: The BGP informs other BGP speaker by the atomic aggregate attributes. Local system selects a sub-specified route other than the more specified routes included in it. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set atomic-aggregate

5.1.18 set comm-list

Command: set comm-list <*community-list-nam*e | *community-list-num* > delete

no set comm-list <*community-list-nam*e | *community-list-num* > delete

Function: Configure to delete the community attributes from the inbound or outbound routing messages. The "**no set comm-list <*community-list-nam*e | *community-list-num* > delete**" command deletes the configuration.

Parameter: <*community-list-nam*e > is the name of community list, **<*community-list-num* >** is the sequence number of community list, ranging between 1～99 (standard community list) or 100～199 (extended community list).

Command Mode: route-map mode

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set comm-list 100 delete

5.1.19 set community

Command: set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]

no set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]

Function: Configure the community attributes of the BGP routing message. The "**no set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]**" command deletes this configuration.

Parameter: [*AA:NN*] is the community attribute value, **[internet]** is the internet scope, **[local-AS]** means this route do not announce outside the local AS (but can announce among the sub AS

within the confederation), **[no-advertise]** means this route do not send to any neighbor, **[no-export]** means this route do not send to EBGP neighbors, **[none]** means delete the community attributes from the prefix of this route, **[additive]** means add following existing community attributes.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set community local-as additive

5.1.20 set extcommunity

Command: set extcommunity <rt | soo> <*AA:NN*>

no set extcommunity <rt | soo> [<*AA:NN*>]

Function: Configure the extended community attributes of the BGP routing message. The "**no set extcommunity <rt | soo> [<*AA:NN*>]**" command deletes this configuration.

Parameter: <*rt*> is the route target, **<*soo*>** is the site of origin, **<*AA:NN*>** is the value of community attributes, amongst AA is AS number, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100), NN is a random two byte number.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example: Set rt as 100:10

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set extcommunity rt 100:10

Set soo as 200.200:10

Switch(config)#route-map r1 permit 10

Switch(config-route-map)#set extcommunity soo 200.200:10

5.1.21 set ip next-hop

Command: set ip next-hop <*ip_addr*>

no set ip next-hop [<*ip_addr*>]

Function: Configure the next-hop of the route. The "**no set ip next-hop [<*ip_addr*>]**" command deletes the configuration.

Parameter: <*ip_addr* > is the ip address of next-hop shown with dotted decimal notation.

Command Mode: route-map mode

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set ip next-hop 10.2.2.2

5.1.22 set local-preference

Command: set local-preference <*pre_val*>

no set local-preference [<*pre_val*>]

Function: Configure the local priority of BGP route. The "**no set local-preference [<*pre_val*>]**" command deletes this configuration.

Parameter: <*pre_val* > is the value of local priority, ranging between 0～4294967295.

Command Mode: route-map mode

Usage Guide: The local priority attribute is the priority level of a route. A route with a higher local priority level when compared with other route of the same destination, will be more preferred than other route. The local priority validates only within this AS and will not be transported to EBGP neighbors. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set local-preference 60

5.1.23 set metric

Command: set metric < *metric_val*>

no set metric [< *metric_val*>]

Function: Configure the metric value of the route. The "**no set metric [< *metric_val*>]**" command deletes the configuration.

Parameter: <*metric_val* > is the metric value, ranging between 1～4294967295.

Command Mode: route-map mode

Usage Guide: The metric value only affects the path option from external neighbors to local AS. The less the metric value is the higher is the priority. Under normal circumstances only the path metric value of the neighbors of the same AS will be compared. To extend the comparison to the metric values of different neighbor path, the bgp always-compare-med command should be configured. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set metric 60

5.1.24 set metric-type

Command: set metric-type <type-1 | type-2>

no set metric-type [<type-1 | type-2>]

Function: Configure the metric type of the OSPF routing message. The "**no set metric-type [<type-1 | type-2>]**" command deletes this configuration.

Parameter: type-1 means matches the OSPF type 1 external route; **type-2** means matches the OSPF type 2 external route.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set metric-type type-1

5.1.25 set origin

Command: set origin <egp | igp | incomplete >

no set origin [<egp | igp | incomplete >]

Function: Configure the origin code of the BGP routing message. The "**no set origin [<egp | igp | incomplete >]**" command deletes this configuration.

Parameter: egp means the route is learnt from the external gateway protocols, **igp** means the route is learnt from the internal gateway protocols, **incomplete** means the route origin is uncertain.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set origin egp

5.1.26 set originator-id

Command: set originator-id <*ip_addr*>

no set originator-id [<*ip_addr*>]

Function: Configure the origin ip address of the BGP routing message. The "**no set originator-id [<*ip_addr*>]**" command deletes the configuration.

Parameter: <*ip_addr*> is the ip address of the route source shown by dotted decimal notation.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set originator-id 10.1.1.1

5.1.27 set tag

Command: set tag <*tag_val*>

no set tag [<*tag_val*>]

Function: Configure the tag domain of OSPF routing messages. The "**no set tag [*<tag_val>*]**" command deletes this configuration.

Parameter: *<tag-val >* is the tag value, ranging between 0～4294967295.

Command Mode: route-map mode

Usage Guide: There is a route-tag domain at the AS-external-LSA type LSA. The domain is normally identified by other routing protocols. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set tag 60

5.1.28 set vpnv4 next-hop

Command: set vpnv4 next-hop *<ip_addr>*

no set vpnv4 next-hop [*<ip_addr>*]

Function: Configure the next-hop of BGP VPNv4 routing message. The no command deletes the configuration.

Parameter: *<ip_addr>* is the next-hop ip address of VPNv4 route shown by dotted decimal notation.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set vpnv4 next-hop 10.1.1.1

5.1.29 set weight

Command: set weight *<weight_val>*

no set weight [*<weight_val>*]

Function: Configure the weight value of BGP routing message. The "**no set weight [*<weight_val>*]**" command deletes this configuration.

Parameter: *<weight_val>* is weight value, ranging between 0～4294967295

Command Mode: route-map mode

Usage Guide: Weight value is adopted to facilitate the best path option and validates only within the local switch. While there are several route to the same destination the one with higher priority is more preferred. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set weight 60

5.1.30 show ip prefix-list <list-name>

Command: show ip prefix-list [<*list-name*> [<*ip_addr/len*> [first-match | longer] | seq <*sequence-number*>]]

Function: Show by prefix-list names.

Parameter: <*list-name*> is the name of prefix-list, **<*ip_addr/len*>** is the prefix ip address and the length of mask, **first-match** stands for the first route table matched with specified ip address, **longer** means longer prefix is required, **seq** means show by sequence number, **<*sequence-number*>** is the sequence number, ranging between 0～4294967295.

Default: None

Command Mode: Admin mode

Usage Guide: All prefix-list will be listed when no prefix-list name is specified.

Example:

```
Switch#show ip prefix-list
ip prefix-list 1: 1 entries
    deny any
ip prefix-list mylist: 1 entries
    deny 1.1.1.1/8
Switch#show ip prefix-list mylist 1.1.1.1/8
    seq 5 deny 1.1.1.1/8 (hit count: 0, recount: 0)
```

Displayed information	Explanation
ip prefix-list mylist: 1 entries	Show a prefix-list named mylist which includes 1 instance.
seq 5 deny 1.1.1.1/8 (hit count: 0, recount: 0)	Show the prefix-list contents sequence numbered 5. hit count: 0 means being hit 0 time, recount: 0 means referred 0 time.

5.1.31 show ip prefix-list <detail | summary>

Command: show ip prefix-list [<detail | summary> [<*list-name*>]]

Function: Display the contents of the prefix list.

Parameters: When **detail** is enabled, detail of prefix-list will be displayed. For **summary**, it is similar but a summary will be displayed. **<*list-name*>** is the name of the prefix list.

Default: None.

Command Mode: Privileged mode and configuration mode

Usage Guide: If no prefix list name is specified, all the prefix list will be displayed.

Example:

```
Switch#show ip prefix-list detail mylist
ip prefix-list mylist:
count: 2, range entries: 0, sequences: 5 - 10
seq 5 deny 1.1.1.1/8 (hit count: 0, refcount: 0)
seq 10 permit 2.2.2.2/8 (hit count: 0, refcount: 0)
```

Switch#show ip prefix-list summary mylist
ip prefix-list mylist:
count: 2, range entries: 0, sequences: 5 – 10

Displayed information	Explanation
ip prefix-list mylist:	To display the prefix list which named mylist.
count: 2, range entries: 0, sequences: 5 - 10	count : 2 means there are two prefix list instances. sequences: 5-10 means the sequence number. 5 is the starting sequence number, while 10 is the ending.
deny 1.1.1.1/8 (hit count: 0, refcount: 0)	deny 1.1.1.1/8 is contents of the prefix list. hit count:0 means the rule has been matched for zero times. And refcount:0 means the rule is referenced for zero times.

5.1.32 show route-map

Command: show route-map
Function: Show the content of route-map.
Parameter: None
Default: None
Command Mode: Admin mode
Usage Guide: None
Example:
Switch# show route-map
route-map a, deny, sequence 10
  Match clauses:
    as-path 60
  Set clauses:
    metric 10

Displayed information	Explanation
route-map a, deny, sequence 10	route-map a means the name of route map is a, deny means the deny mode, sequence 10 means the sequence number is 10
Match clauses:	Match sub
as-path 60	Detailed contents in the Match sub
Set clauses:	Set sub
metric 10	Detailed content in the Set clause

5.1.33 show router-id

Command: show router-id

Function: Show the content of router-id.
Default: None
Command Mode: Admin and Configuration Mode
Example:
1:
Switch#show router-id
Router ID: 20.1.1.1 (automatic)
2:
Switch#show router-id
Router ID: 20.1.1.2 (config)

5.2 Static Route

5.2.1 ip route

Command: ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>/<prefix-length>*} {*<gateway-address>* | *<gateway-interface>*} [*<distance>*]
no ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>/<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]
Function: Configure the static route. The "**no ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>/<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]**" command deletes the static route.
Parameter: The ***<ip-prefix>*** and ***<mask>*** are respectively destination IP address and subnet mask, shown in dotted decimal notation; ***<ip-prefix>*** and ***<prefix-length>*** are respectively the destination IP address and the length of prefix; ***<gateway-address>*** is the next-hop IP address shown in dotted decimal notation; ***<gateway-interface>*** is the next-hop interface, ***< distance >*** is the manage distance of route management, ranging between 1～255.
Default: The management distance of static routing is defaulted at 1.
Command Mode: Global Mode.
Usage Guide: When configuring the next-hop of static routing, both by specifying the next-hop IP address of the route data packet and the exit interface are available.
The default distance values of each route type in the layer 3 switch of our company are listed below:

Route Type	Distance Value
Direct Route	0
Static Route	1
OSPF	110
RIP	120
IBGP	200

EBGP	20

The direct route has the highest priority when each route management distance value remain unchanged and followed by static route, EBGP, OSPF, RIP, IBGP.

Example:

Example 1. Add a static route

Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1

Example 2. Add default route

Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

5.2.2 ip route vrf

Command: ip route vrf <vrf-name> {<ip-prefix> <mask>|<ip-prefix/prefix-length>} {<*gateway-address*>|null0} [<*1-255*>]

no ip route vrf <*vrf-name*> {<*ip-prefix*> <*mask*>|<*ip-prefix/prefix-length*>} {<*gateway-address*>|null0} [<*1-255*>]

Function: Configure the static route for the specific VRF. Before use this command, VPN route forwarding instance must be configured. The no form command will delete the configuration.

Parameters: <*vrf-name*>: The specific VRF name.

<*ip-prefix*>: The destination IP address.

<*mask*>: The sub-net mask shown in dotted decimal format.

<*prefix-length*>: The prefix length.

<*gateway-address*>: The next hop address.

null0: Black hole route.

<*1-255*>: Management distance.

Default: Not configured.

Command Mode: Global configuration mode.

Usage Guide: Configure the static route of VRF-A, the destination IP as 10.1.1.10, the mask as 24 bits, the next hop as 10.1.1.1, the management distance is default:

Switch(config)# ip route vrf VRF-A 10.1.1.10 255.255.255.0 10.1.1.1

Switch(config)#

5.2.3 show ip route

Command: show ip route [<*destination*>|<*destination* >|<*length*>|connected | static | rip| ospf | bgp | isis| kernel| statistics| database [connected | static | rip| ospf | bgp | isis| kernel] |fib[statistics]]

Function: Show the route table.

Parameter: <*destination*> is the destination network address; **<*destination* >/<*length*>** is the destination network address plus the length of prefix; **connected** is direct route; **static** is static route; **rip** is RIP route; **ospf** is OSPF route; **bgp** is BGP route; **isis** is ISIS route; **kernel** is kernel route; **statistics** shows the number of routes; **database** is route database; **fib** is kernel route table.

Command Mode: All modes

Usage Guide: Show all the contents in the route table including: route type, destination network, mask, next-hop address, interface, etc

Example: switch#show ip route

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default

Gateway of last resort is 210.0.0.3 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 210.0.0.3, Vlan1

C 127.0.0.0/8 is directly connected, Loopback

O IA 172.16.11.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47

O IA 172.16.12.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47

O IA 172.16.13.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47

O IA 172.16.14.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47

O IA 172.16.15.0/24 [110/50] via 210.14.0.1, Vlan3014, 00:00:47

O E2 172.16.100.0/24 [110/0] via 210.14.0.1, Vlan3014, 00:00:46

Displayed information	Explanation
C –connected	Direct route, namely the segment directly connected with the layer 3 switch
S –static	Static route, the route manually configured by users
R - RIP derived	RIP route, acquired by layer 3 switch through the RIP protocol.
O - OSPF derived	OSPF route, acquired by layer 3 switch through the OSPF protocol
A- OSPF ASE	Route introduced by OSPF
B- BGP derived	BGP route, acquired by the BGP protocol.
Destination	Target network
Mask	Target network mask
Nexthop	Next-hop IP address
Interface	Next-hop pass-by layer 3 swtich interfaces
Preference	Route priority. If other types of route to the target network exists, the kernel route will only shows those with high priority.

5.2.4 show ip route vrf

Command: show ip route vrf <name> [connected | static | rip| ospf | bgp | isis| kernel|statistics| database[connected | static | rip| ospf | bgp | isis|kernel]]

show ip route fib vrf <*name*> [default|main|local]

Function: Show the routing tables entries.

Parameters: <name> is the name of the forwarding instance of VPN route; **<*destination*>** is the destination address; **<destination>/<length>** are the network address for the destination as well as the length of the network mask; **connected** is for direct route; **static** is for static route; **rip** is for the RIP route protocol; **ospf** is for the OSPF route protocol; **bgp** is for the BGP route protocol; **isis** is for the ISIS route protocol; **kernel** is for the kernel route protocol; **statistics** are the number of route entries to be displayed; **database** is for the route database; **fib** is for the core route table.

Command Mode: All modes.

Usage Guide: To display the contents of the VPN route table, including route type, destination network address, address mask, the address and interface for the next hop, etc.

5.2.5 show ip route fib

This command is not supported by the switch.

5.3 RIP

5.3.1 accept-lifetime

Command: accept-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite}

no accept-lifetime

Function: Use this command to specify a key accept on the key chain as a valid time period. The "**no accept-lifetime**" command deletes this configuration.

Parameter: <*start-time*> parameter specifies the start time of the time period, of which the form should be:

<*start-time*>={<*hh:mm:ss*> <*month*> <*day*> <*year*>|<*hh:mm:ss*> <*day*> <*month*> <*year*>}

<*hh:mm:ss*> specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<*day*> specifies the date of valid, ranging between 1 -31

<*month*> specifies the month of valid shown with the first three letters of the month, such as Jan

<*year*> specifies the year of valid start, ranging between 1993 - 2035

<*end-time*> specifies the due of the time period, of which the form should be:

<*end-time*>={<*hh:mm:ss*> <*month*> <*day*> <*year*>|<*hh:mm:ss*> <*day*> <*month*> <*year*>}

<*hh:mm:ss*> specify the concrete valid time of **accept-lifetime** in hours,

minutes and second

<day> specifies the date of valid, ranging between 1 -31

<month> specifies the month of valid shown with the first three letters of the month, such as Jan

<year> specifies the year of valid start, ranging between 1993 - 2035

<seconds> the valid period of the key in seconds, ranging between 1-2147483646

Infinite means the key will never be out of date.

Default: No default configuration.

Command Mode: keychain-key mode

Usage Guide: None.

Example: The example below shows the accept-lifetime configuration of key 1 on the keychain named mychain.

Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)# key 1

Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

Related Command:

key

key-string

key chain

send-lifetime

5.3.2 address-family ipv4

Command: address-family ipv4 vrf <vrf-name>

no **address-family ipv4 vrf *<vrf-name>***

Function: Configure this command to enable the routing message switching among VRF and enter the address-family mode. The no command deletes the RIP instances related to this VPN routing/forwarding instance.

Parameter: ***<vrf-name>*** specifies the name of VPN routing/forwarding instances.

Command Mode: Router mode

Usage Guide: This command is only used on PE router. A VPN routing/forwarding instance must be generated with command ip vrf prior to using this command by which the VPN routing/forwarding instances can be related to RIP instances.

Example:

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# address-family ipv4 vrf VRF1

Switch(config-router-af)#

5.3.3 clear ip rip route

Command: clear ip rip route {*<A.B.C.D/M>* | kernel | static | connected | rip | ospf | isis | bgp | all}

Function: Clear specific route in the RIP route table.

Parameter: ***<A.B.C.D/M>*** Clear the routes which match the destination address from the RIP route table. Specifies the IP address prefix and its length of the destination address

kernel delete kernel routes from the RIP route table

static delete static routes from the RIP route table

connected delete direct routes from the RIP route table

rip only delete RIP routes from the RIP route table

ospf only delete OSPF routes from the RIP route table

isis only delete ISIS routes from the RIP route table

bgp only delete BGP routes from the RIP route table

all delete all routes from the RIP route table

Default: No default configurations.

Command Mode: Admin mode

Usage Guide: Use this command with the all parameter will delete all learnt route in the RIP route which will be immediately recovered except for rip route. The dynamic learnt RIP route can only be recovered by studying one more time.

Example: Switch# clear ip rip route 10.0.0.0/8

Switch# clear ip rip route ospf

5.3.4 debug rip

Command: debug rip [events| nsm| packet[recv|send][detail]| all]

no debug rip [events| nsm| packet[recv|send][detail]| all]

Function: Open various RIP adjustment switches and show various adjustment debugging messages. The "**no debug rip [events| nsm| packet[recv|send][detail]| all]**" command closes corresponding debugging switch.

Parameter: events shows the debugging messages of RIP events

nsm shows the communication messages between RIP and NSM

packet shows the debugging messages of RIP data packets

recv shows the messages of the received data packets

send shows the messages of the sent data packets

detail shows the messages of received or sent data packets

Default: Debug switch closed.

Command Mode: Admin mode and global mode

Example: Switch# debug rip packet

Switch#1970/01/01 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520

1970/01/01 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520

1970/01/01 01:01:47 IMI: RECV[Vlan1]: Receive from 20.1.1.2:520

5.3.5 debug rip redistribute message send

Command: debug rip redistribute message send

no debug rip redistribute message send

Function: To enable the debugging of sending messages for routing redistribution messages from OSPF process or BGP protocol for RIP. The no form of this command will disable the debugging messages.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch#debug rip redistribute message send

Switch#no debug rip redistribute message send

5.3.6 debug rip redistribute route receive

Command: debug rip redistribute route receive

no debug rip redistribute route receive

Function: To enable debugging of received messages from NSM for RIP. The no form of this command will disable debugging of received messages from NSM for RIP.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch#debug rip redistribute route receive

Switch#no debug rip redistribute route receive

5.3.7 default-information originate

Command: default-information originate

no default-information originate

Function: Allow the network 0.0.0.0 to be redistributed into the RIP. The "**no default-information originate**" disables this function.

Parameter: None

Default: Disabled

Command Mode: Router mode and address-family mode

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# default-information originate

5.3.8 default-metric

Command: default-metric <*value*>

no default-metric

Function: Set the default metric value of the introduced route. The "**no default-metric**" command restores the default value to 1.

Parameter: <*value*> is the metric value to be set, ranging between 1~16.

Default: Default route metric value is 1.

Command Mode: Router mode and address-family mode

Usage Guide: default-metric command is used for setting the default route metric value of the routes from other routing protocols when distributed into the RIP routes. When using the **redistribute** commands for introducing routes from other protocols, the default route metric value specified by **default-metric** will be adopted if no specific route metric value is set.

Example: Set the default route metric value to 3 for introducing routes from other routing protocols into the RIP routes.

Switch(config-router)#default-metric 3

Relevant Commands: redistribute

5.3.9 distance

Command: distance <*number*> [<*A.B.C.D/M*>] [<*access-list-name | access-list-number* >]

no distance [<*A.B.C.D/M*>]

Function: Set the managing distance with this command. The "**no distance [<*A.B.C.D/M*>]**" command restores the default value to 120.

Parameter: <*number*> specifies the distance value, ranging from 1 to 255. ***<A.B.C.D/M>*** specifies the network prefix and its length. ***<access-list-name | access-list-number >*** specifies the access-list number or name applied.

Default: The default managing distance of RIP is 120.

Command Mode: Router mode and address-family mode

Usage Guide: In case there are routes from two different routing protocols to the same destination, the managing distance is then used for selecting routes. The less the managing distance of the route protocol is, the more reliable will be the route acquired from the protocol.

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# distance 8 10.0.0.0/8 mylist

5.3.10 distribute-list

Command: distribute-list {<*access-list-number* | *access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]

no distribute-list {<*access-list-number*| *access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]

Function: This command uses access-list or prefix-list to filter the route update packets sent and received. The "**no distribute-list {<*access-list-number*| *access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]**" command cancels this route filter function.

Parameter: ***<access-list-number |access-list-name>*** is the name or access-list number to be applied. ***<prefix-list-name>*** is the name of the prefix-list to be applied. ***<ifname>*** specifies the name of interface to be applied with route filtering.
Default: The function in default situation is disabled.
Command Mode: Router mode and address-family mode
Usage Guide: The filter will be applied to all the interfaces in case no specific interface is set.
Example: Switch# config terminal
Switch(config)# router rip
Switch(config-router)# distribute-list prefix myfilter in vlan 1

5.3.11 exit-address-family

Command: exit-address-family
Function: Exit address-family mode
Command Mode: address-family mode
Example: Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf IPI
Switch(config-router-af)# exit-address-family
Switch(config-router)#

5.3.12 ip rip aggregate-address

Command: ip rip aggregate-address A.B.C.D/M
no ip rip aggregate-address A.B.C.D/M
Function: To configure RIP aggregation route. The no form of this command will delete this configuration.
Parameter: A.B.C.D/M:IPv4 address and mask length.
Command Mode: Router Mode or Interface Configuration Mode.
Default: Disabled.
Usage Guide: If to configure aggregation route under router mode, RIP protocol must be enabled. If configured under interface configuration mode, RIP protocol may not be enabled, but the aggregation router can operation after the RIP protocol be enabled on interface.
Example: To configure aggregation route as 192.168.20.0/22 globally.
Switch(config)#router rip
Switch(config-router) #ip rip agg 192.168.20.0/22

5.3.13 ip rip authentication key-chain

Command: ip rip authentication key *<name-of-chain>*
no ip rip authentication key-chain
Function: Use this command to enable RIPV2 authentication on an interface and further configures the adopted key chain. The "**no ip rip authentication key-chain**" command cancels

the authentication.

Parameter: ***<name-of-chain>*** is the name of the adopted key chain. There may be spaces in the string. The input ends with an enter and the string should not be longer than 256 bytes.

Default: Not configured.

Command Mode: Interface Configuration Mode.

Usage Guide: If the authentication is only configured without configuring the key chain or password used by the interface, the authentication does no effect. If mode has not been configured prior to configuring this command, the mode will be set to plaintext authentication. The "no ip rip authentication key" command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication key my key

Relevant Commands: key, key chain

5.3.14 ip rip authentication mode

Command: ip rip authentication mode {text|md5}

no ip rip authentication mode {ext|md5}

Function: Configure the authentication mode; the "**no ip rip authentication mode {ext|md5}**" command restores the default authentication mode namely text authentication mode.

Parameter: text means text authentication; **md5** means MD5 authentication.

Default: Not configured authentication.

Command Mode: Interface Configuration Mode.

Usage Guide: RIP-I do not support authentication which the RIP-II supports two authentication modes: text authentication (i.e. Simple authentication) and data packet authentication (i.e. MD5 authentication). This command should be used associating the ip rip authentication key or ip rip authentication string. Independently configuration will not lead to authentication process.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication mode md5

Related Command: ip rip authentication key-chain, ip rip authentication string

5.3.15 ip rip authentication string

Command: ip rip authentication string *<text>*

no ip rip authentication string

Function: Set the password used in RIP authentication. The "**no ip rip authentication string**" cancels the authentication.

Parameter: ***<text>*** is the password used in authentication of which the length should be 1-16 characters with space available. The password should end with enter.

Command Mode: Interface mode

Usage Guide: The ip rip authentication key will not be able to be configured when this command is configured, key id value is required in MD5 authentication which is 1 when use this command. The mode will be set to plaintext authentication in case no mode configuration is available. The "**no ip rip authentication string**" command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode. Input ip rip authentication string aaa aaa to set the password as aaa aaa which is 7 characters.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication string guest

Related Command: ip rip authentication mode

5.3.16 ip rip authentication cisco-compatible

Command: ip rip authentication cisco-compatible

no ip rip authentication cisco-compatible

Function: After configured this command, the cisco RIP packets will be receivable by configuring the plaintext authentication or MD5 authentication.

Parameter: None

Default: Not configured

Command Mode: Interface mode

Usage Guide: After authentication is configured on the cisco router, the RIP packets will exceeds the length of the defined standard length of the protocol once the number of route items is greater than 25. By configuring this command the over-lengthen RIP packets will be receivable other than denied.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication cisco-compatible

Related Command: ip rip authentication mode

5.3.17 ip rip receive-packet

Command: ip rip receive-packet

no ip rip receive-packet

Function: Set the interface to be able to receivable RIP packets; the "**no ip rip receive-packet**" command sets the interface to be unable to receivable RIP packets.

Default: Interface receives RIP packets.

Command Mode: Interface Configuration Mode.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip receive-packet

Related Command: ip rip send-packet

5.3.18 ip rip receive version

Command: ip rip receive version { 1 | 2|1 2 }

no ip rip receive version

Function: Set the version information of the RIP packets the interface receives. The default version is 2; the "**no ip rip receive version**" command restores the value set by using the version command.

Parameter: 1 and 2 respectively stands for RIP version 1 and RIP version 2, 1 2 stands for the RIP versions 1, 2.

Default: Version 2

Command Mode: Interface Configuration Mode.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip receive version 1 2

Related Command: version

5.3.19 ip rip send-packet

Command: ip rip send-packet

no ip rip send-packet

Function: Set the Interface to be able to receive the RIP packets; the "**no ip rip send-packet**" sets the interface to be unable to receive the RIP packets.

Default: Interface sends RIP packets.

Command Mode: Interface Configuration Mode.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip send-packet

Related Command: ip rip receive-packet

5.3.20 ip rip send version

Command: ip rip send version { 1 | 2 | 1-compatible | 1 2}

no ip rip send version

Function: Set the version information of the RIP packets the interface receives. The default version is 2; the "**no ip rip send version**" command restores the value set by using the version command.

Parameter: 1 and 2 respectively stands for RIP version 1 and RIP version 2, 1 2 stands for the RIP versions 1, 2.

Default: Version 2

Command Mode: Interface Configuration Mode.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip send version 1

Related Command: version

5.3.21 ip rip split-horizon

Command: ip rip split-horizon [poisoned]

no ip rip split-horizon

Function: Enable split horizon. The "**no ip rip split-horizon**" disables the split horizon.

Parameter: [poisoned] means configure the split horizon with poison reverse.

Default: Split Horizon with poison reverse by default.

Command Mode: Interface Configuration Mode.

Usage Guide: The split horizon is for preventing the Routing Loops, namely preventing the layer 3 switches from broadcasting the routes which is learnt from the same interface on which the route to be broadcasted.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip split-horizon poisoned

5.3.22 key

Command: key <*keyid*>

no key <*keyid*>

Function: This command is for managing and adding keys in the key chain. The "**no key <*keyid*>**" command deletes one key.

Parameter: <*keyid*> is key ID, ranging between 0-2147483647.

Command Mode: Keychain mode and keychain-key mode

Usage Guide: The command permits entering the keychain-key mode and set the passwords corresponding to the keys.

Example: Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)# key 1

Switch(config-keychain-key)#

Relevant Commands: key chain, key-string, accept-lifetime, send-lifetime

5.3.23 key chain

Command: key chain <*name-of-chain*>

no key chain < *name-of-chain* >

Function: This command is for entering a keychain manage mode and configure a keychain. The "**no key chain < *name-of-chain* >**" deletes one keychain.

Parameter: <*name-of-chain*> is the name string of the keychain the length of which is not specifically limited.

Command Mode: Global Mode

Example: Switch# config terminal

Switch(config)# key chain mychain
Switch(config-keychain)#

Relevant Commands: key, key-string, accept-lifetime, send-lifetime

5.3.24 key-string

Command: key-string *<text>*
no key-string *<text>*

Function: Configure a password corresponding to a key. The "**no key-string *<text>***" command deletes the corresponding password.

Parameter: *<text>* is a character string without length limit. However when referred by RIP authentication only the first 16 characters will be used.

Command Mode: Keychain-key mode

Usage Guide: This command is for configure different passwords for keys with different ID.

Example: Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string prime

Related Command: key, key chain, accept-lifetime, send-lifetime

5.3.25 maximum-prefix

Command: maximum-prefix <*maximum-prefix*> [<*threshold*>]
no maximum-prefix

Function: Configure the maximum number of RIP routes in the route table. The "**no maximum-prefix**" command cancels the limit.

Parameter: *<maximum-prefix>* the maximum number of RIP route, ranging between 1-65535; a warning is given when the number rate of current route exceeds ***<threshold>*** ranging between 1-100, default at 75.

Command Mode: router mode

Usage Guide: The maximum RIP route only limits the number of routes learnt through RIP but not includes direct route or the RIP static route configured by the route command. The base on which the comparison is performed is the number of route marked R in the show ip route database, and also the number of RIP routes displayed in the show ip route statistics command.

Example: Switch# config terminal
Switch(config)# router rip
Switch(config-router)# maximum-prefix 150

5.3.26 neighbor

Command: neighbor <*A.B.C.D*>
no neighbor <*A.B.C.D*>

Function: Specify the destination address requires targeted-peer sending. The "**no neighbor**

<A.B.C.D>" command cancels the specified address and restores all gateways to trustable.

Parameter: *<A.B.C.D>* is the specified destination address for the sending, shown in dotted decimal notation.

Default: Not sending to any targeted-peer destination address.

Command Mode: Router mode

Usage Guide: When used accompany with passive-interface command it can be configured to only sending routing messages to specific neighbor.

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# neighbor 1.1.1.1

Related Command: passive-interface

5.3.27 network

Command: network *<A.B.C.C/M|ifname>*

no network *<A.B.C.C/M|ifname>*

Function: Configure the RIP protocol network.

Parameter: *<A.B.C.C/M|>* is the IP address prefix and its length in the network.

<ifname> is the name of a interface.

Default: Not running RIP protocol

Command Mode: Router mode and address-family mode

Usage Guide: Use this command to configure the network for sending or receiving RIP update packets. If the network is not configured, all interfaces of the network will not be able to send or receive data packets.

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# network 10.0.0.0/8

Switch(config-router)# network vlan 1

Related Command: show ip rip, clear ip rip

5.3.28 offset-list

Command: offset-list <*access-list-number |access-list-name*> {in|out} *<number >* [*<ifname>*]

no offset-list <*access-list-number |access-list-name*> {in|out} *<number >* [*<ifname>*]

Function: Add an offset value to the metric value of the routes learnt by RIP. The "**no offset-list <*access-list-number |access-list-name*> {in|out} *<number >* [*<ifname>*]**" command disables this function.

Parameter: *< access-list-number |access-list-name>* is the access-list or name to be applied. ***<number >*** is the added offset value, ranging between 0-16; ***<ifname>*** is the specific interface name

Default: Default offset value is the metric value defined by the system.

Command Mode: Router mode and address-family mode

Example: Switch# config terminal
Switch(config)# router rip
Switch(config-router)# offset-list 1 in 5 vlan 1
Related Command: access-list

5.3.29 passive-interface

Command: passive-interface *<ifname>*
no passive-interface *<ifname>*
Function: Set the RIP layer 3 switch blocks RIP broadcast on specified interface, on which the RIP data packets will only be sent to layer 3 switches configured with neighbor.
Parameter: *<ifname>* is the name of specific interface.
Default: Not configured
Command Mode: Router mode
Example: Switch# config terminal
Switch(config)# router rip
Switch(config-router)# passive-interface vlan 1
Related Command: show ip rip

5.3.30 recv-buffer-size

Command: recv-buffer-size*<size>*
no recv-buffer-size
Function: This command configures the size of UDP receiving buffer zone of RIP; the "**no recv-buffer-size**" command restores the system default.
Parameter: *<size>* is the buffer zone size in bytes, ranging between 8192-2147483647.
Default: 8192 bytes.
Command Mode: Router mode
Example: Switch# config terminal
Switch(config)# router rip
Switch(config-router)# recv-buffer-size 23456789

5.3.31 redistribute

Command: redistribute {kernel |connected| static| ospf [<process-id>] | isis| bgp} [metric<*value*>] [route-map<*word*>]
no redistribute {kernel |connected| static| ospf [<process-id>] | isis| bgp} [metric<*value*>] [route-map<*word*>]
Function: Introduce the routes learnt from other routing protocols into RIP.
Parameter: kernel introduce from kernel routes;
connected introduce from direct routes;
static introduce from static routes;
ospf introduce from OSPF routes. process-id is OSPF process ID, if there is no

parameter that means the process by default, range between 1 to 65535;

isis introduce from ISIS routes;

bgp introduce from BGP routes;

<value> is the metric value assigned to the introduced route, ranging between 0 to 16;

<word> is the probe pointing to the route map for introducing routes.

Command Mode: Router Mode and address-family Mode

Usage Guide: Under the address-family mode, the parameter kernel and ISIS is unavailable.

Example:

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# redistribute kernel route-map ipi

To redistribute OSPFv2 routing information to RIP.

Switch(config)# router rip

Switch(config-router)# redistribute ospf 2

5.3.32 redistribute ospf (vrf command)

This command is not supported by the switch.

5.3.33 route

Command: route *<A.B.C.D/M>*

no route *<A.B.C.D/M>*

Function: This command configures a static RIP route. The "**no route *<A.B.C.D/M>***" command deletes this route.

Parameter: Specifies this destination IP address prefix and its length.

Command Mode: Router mode

Usage Guide: The command adds a static RIP route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIP route database.

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# route 1.0.0.0/8

5.3.34 router rip

Command: router rip

no router rip

Function: Enable the RIP routing process and enter the RIP mode; the "**no router rip**" command closes the RIP routing protocol.

Default: Not running RIP route.

Command Mode: Global mode

Usage Guide: This command is the switch for starting the RIP routing protocol which is required to be open before configuring other RIP protocol commands.

Example: Enable the RIP protocol mode

Switch(config)#router rip

Switch(config-router)#

5.3.35 send-lifetime

Command: send-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite}

no send-lifetime

Function: Use this command to specify a key on the keychain as the time period of sending keys. The "**no send-lifetime**" cancels this configuration.

Parameter: <*start-time*> parameter specifies the starting time of the time period, which is:

***<start-time>*={*<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>*}**

<hh:mm:ss> Specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> Specifies the date of valid, ranging between 1 -31

<month> Specifies the month of valid shown with the first three letters of the month, such as Jan

<year> Specifies the year of valid start, ranging between 1993 - 2035

<end-time> Specifies the due of the time period, of which the form should be:

***<end-time>*={*<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>*}**

<hh:mm:ss> Specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> Specifies the date of valid, ranging between 1 -31

<month> Specifies the month of valid shown with the first three letters of the month, such as Jan

<year> Specifies the year of valid start, ranging between 1993 -2035

<seconds> is the valid period of the key in seconding and ranging between 1-2147483646

Default: No default configuration

Command Mode: Keychain-key mode

Usage Guide: Refer to the 3.13 RIP authentication section.

Example: The example below shows the send-lifetime configuration on the keychain named mychain for key 1.

Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)# key 1

Switch(config-keychain-key)# send-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

Related Command: key, key-string, key chain, accept-lifetime

5.3.36 show debugging rip

Command: show debugging rip

Function: Show RIP event debugging, RIP packet debugging and RIP nsm debugging status.
Command Mode: Any mode.
Example: Switch# show debugging rip
RIP debugging status:
RIP event debugging is on
RIP packet detail debugging is on
RIP NSM debugging is on

5.3.37 show ip protocols rip

Command: show ip protocols rip
Function: Show the RIP process parameter and statistics information.
Command Mode: Any mode.
Example:
show ip protocols rip
Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 8 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: static
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
Vlan1 2 2
Routing for Networks:
Vlan1
Vlan2
Routing Information Sources:
Gateway Distance Last Update Bad Packets Bad Routes
20.1.1.1 120 00:00:31 0 0
Distance: (default is 120)

Displayed information	Explanation
Sending updates every 30 seconds with +/-50%, next due in 8 seconds	Sending update every 30 secs
Timeout after 180 seconds, garbage collect after 120 seconds	The route time-out event period is 180 secs, the garbage collect time is 120 seconds
Outgoing update filter list for all interface is not set	Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set	Incoming update filter list for all interface is not set
Default redistribution metric is 1	Default redistribution metric is 1

Redistributing: static	Redistributing the static route into the RIP route
Default version control: send version 2, receive version 2 Interface Send Recv Key-chain Ethernet1/0/3 2 2	The configuration of interface receiving and sending packets. Receive version is 2, keychain 1 not configured.
Routing for Networks: Vlan1 Vlan2	The segment running RIP is the Vlan 1 and Vlan 2
Routing Information Sources: Gateway Distance Last Update Bad Packets Bad Routes 20.1.1.1 120 00:00:31 0 0	Routing information sources The badpacketand bad routes from the gateway 20.1.1.1 are all 0. 31 seconds have passed since the last route update. The manage distance is 120
Distance: (default is 120)	Default manage distance is 120

5.3.38 show ip rip

Command: show ip rip

Function: Show the routes in the RIP route data base.

Command Mode: Any mode.

Example:

show ip rip

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP

	Network	Next Hop	Metric	From	If	Time
R	12.1.1.0/24	20.1.1.1	2	20.1.1.1	Vlan1	02:51
R	20.1.1.0/24		1		Vlan1	

Amongst R stands for RIP route, namely a RIP route with the destination network address 12.1.1.0, the network prefix length as 24, next-hop address at 20.1.1.1. It is learnt from the Ethernet port E1/0/3 with a metric value of 2, and still has 2 minutes 51 seconds before time out.

5.3.39 show ip rip database

Command: show ip rip database

Function: Show the routes in the RIP route database.

Command Mode: Any mode

Example: Switch# show ip rip database

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,

B -BGP

	Network	Next Hop	Metric From	If	Time
R	10.1.1.0/24		1	Vlan1	
R	20.1.1.0/24		1	Vlan2	

Command: show ip rip

5.3.40 show ip rip database vrf

Command: show ip rip database vrf <vrf-name>

Function: This command display the RIP database messages related to the VPN routing/forwarding instances.

Parameter: ***<vrf-name>*** specifies the name of VPN routing/forwarding instances.

Command Mode: Any Mode.

Example: Switch# show ip rip database vrf IPI

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,

B - BGP

Network	Next Hop	Metric From	If	Time
R 10.1.1.0/24		1	Vlan1	00:46

5.3.41 show ip rip interface

Command: show ip rip interface [<*ifname*>]

Function: Show the RIP related messages.

Parameter: ***<ifname>*** is the name of the interface to show the messages.

Command Mode: Any mode.

Example: Switch# show ip rip interface vlan 1

Vlan1 is up, line protocol is up

Routing Protocol: RIP

Receive RIP packets

Send RIP packets

Passive interface: Disabled

Split horizon: Enabled with Poisoned Reversed

IP interface address:10.1.1.1/24

5.3.42 show ip rip interface vrf

Command: show ip rip interface vrf <vrf-name> **[*<ifname>*]**

Function: This command shows RIP interface relevant to VPN routing/forwarding instances.

Parameter: ***<vrf-name>*** specifies the name of VPN routing/forwarding instances.

<ifname> is the name of the interfaces.

Command Mode: Any Mode.

Example: Switch# show ip rip interface vrf IPI Vlan1
Ethernet1/1 is up, line protocol is up
Routing Protocol: RIP
VPN Routing/Forwarding: vpnb
Receive RIP packets
Send RIP packets
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
11.1.1.1/24

Displayed information	Explanation
Vlan1 is up, line protocol is up	Interface is UP.
Routing Protocol: RIP	The protocol running on the interface is RIP.
VPN Routing/Forwarding: vpnb	Interface relates to the VPN routing/forwarding instances.
Receive RIP packets	The interface can receive RIP packets.
Send RIP packets	The interface can send RIP packets.
Passive interface: Disabled	Passive-interface disabled.
Split horizon: Enabled with Poisoned Reversed	Configure a split horizon with poison reversed.
IP interface address: 11.1.1.1/24	The IP address of the interface.

5.3.43 show ip rip aggregate

Command: show ip rip aggregate
Function: To display the information of IPv4 aggregation route.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Default: None.
Usage Guide: This command is used to display which interface the aggregation route be configured, Metric, Count, Suppress and so on. If configured under global mode, then the interface display "----", "Metric" is metric. "Count" is the number of learned aggregation routes. "Suppress" is the times of aggregation.
Example: To display the information of IPv4 aggregation route.
Switch(Config-if-Vlan1)#show ip rip agg

Aggregate information of rip

Network	Aggregated Ifname	Metric	Count	Suppress
192.168.0.0/16	Vlan1	1	2	0
192.168.4.0/22	----	1	2	0
192.168.4.0/24	----	1	1	1

Vlan1 1 1 1

Displayed information	Explaination
Network	Route prefix and prefix length.
Aggregated Ifname	To configure the interface name of the aggregation route. If the route aggregated globally, then display “----”.
Metric	Metric of aggregation route.
Count	The number of learned aggregation route.
Suppress	The times of aggregated for aggregation route.

5.3.44 show ip rip redistribute

Command: show ip rip redistribute [vrf <*NAME*>]

Function: To display the routing information introduced from external process of RIP.

Parameters: VRF name, if no parameter is appended, all the routing redistribution information of RIP for all VRF.

Default: Not shown by default.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: None.

Example:

Switch#show ip rip redistribute

5.3.45 show ip vrf

Command: show ip vrf [*<vrf-name>*]

Function: This command shows the RIP instances messages related to the VPN routing/forwarding instances.

Parameter: ***<vrf-name>*** specifies the name of the VPN routing/forwarding instances.

Command Mode: Any Mode.

Usage Guide: The command also exist in other routing protocols, when using this command, messages of other routing protocol processes related to the VPN routing/forwarding instances will also be displayed.

Example: Switch# show ip vrf IPI

VRF IPI, FIB ID 1

Router ID: 11.1.1.1 (automatic)

Interfaces:

Vlan1

!

VRF IPI; (id=1); RIP enabled Interfaces:

Ethernet1/8

Name Interfaces

IPI Vlan1

Name	Default RD	Interfaces
IPI		Vlan1

5.3.46 timers basic

Command: timers basic *<update> <invalid> <garbage>*

no timers basic

Function: Adjust the RIP timer update, timeout, and garbage collecting time. The "**no timers basic**" command restores each parameter to their default values.

Parameter: ***<update>*** time interval of sending update packet, shown in seconds and ranging between 5-2147483647; ***<invalid>*** time period after which the RIP route is advertised dead, shown in seconds and ranging between 5-2147483647; ***<garbage>*** is the hold time in which the a route remains in the routing table after advertised dead, shown in seconds and ranging between 5-2147483647.

Default: ***<update>*** defaulted at 30; ***<invalid>*** defaulted at 180; ***<garbage>*** defaulted at 120

Command Mode: Router mode

Usage Guide: The system is defaulted broadcasting RIPng update packets every 30 seconds; and the route is considered invalid after 180 seconds but still exists for another 120 seconds before it is deleted from the routing table.

Example: Set the RIP update time to 20 seconds and the timeout period to 80 second, the garbage collecting time to 60 seconds.

Switch(Config-Router)#timers basic 20 80 60

5.3.47 version

Command: version {1| 2}

no version

Function: Configure the version of all RIP data packets sent/received by router interfaces: the "**no version**" restores the default configuration.

Parameter: 1 is version 1 rip; **2** is version 2 rip.

Default: Sent and received data packet is version 2 by default.

Command Mode: Router mode and address-family mode

Usage Guide: 1 refers to that each interface of the layer 3 switch only sends/receives the RIP-I data packets. 2 refers to that each interface of the layer 3 switch only sends/receives the RIP-II data packets. The RIP-II data packet is the default version.

Example: Configure the version of all RIP data packets sent/received by router interfaces to version 2.

Switch(config-router)#version 2

Related Command: ip rip receive version

ip rip send version

5.4 OSPF

5.4.1 area authentication

Command: area <*id*> authentication [message-digest md5]

no area <*id*> authentication

Function: Configure the authentication mode of the OSPF area; the "**no area <*id*> authentication**" command restores the default value.

Parameter: <*id*> is the area number which could be shown in digit, ranging from 0 to 4294967295, or in IP address. **message-digest md5** is proved by MD5 authentication, or be proved by simple plaintext authentication if not choose this parameter.

Default: No authentication.

Command Mode: OSPF protocol mode

Usage Guide: Set the authentication mode to plaintext authentication or MD5 authentication. The authentication mode is also configurable under interface mode of which the priority is higher than those in the area. It is required to use **ip ospf authentication-key** to set the password while no authentication mode configured at the interface and the area is plaintext authentication, and use ip ospf message-digest key command to configure MD5 key if is MD5 authentication. The area authentication mode could not affect the authentication mode of the interface in this area.

Example: Set the authentication mode in area 0 to MD5.

Switch(config-router)#area 0 authentication message-digest

5.4.2 area default-cost

Command: area <*id*> default-cost <*cost*>

no area <*id*> default-cost

Function: Configure the cost of sending to the default summary route in stub or NSSA area; the "**no area <*id*> default-cost**" command restores the default value.

Parameter: <*id*> is the area number which could be shown as digits 0～16777214, or as an IP address; **<*cost*>** ranges between <0-16777214>.

Default: Default OSPF cost is 1.

Command Mode: OSPF protocol mode

Usage Guide: The command is only adaptive to the ABR router connected to the stub area or NSSA area.

Example: Set the default-cost of area 1 to 10.

Switch(config-router)#area 1 default-cost 10

5.4.3 area filter-list

Command: area <*id*> filter-list {access|prefix} {in|out}

no area <*id*> filter-list {access|prefix} {in|out}

Function: Configure the filter broadcasting summary routing on the ABR; the "**no area <*id*>**

filter-list {access|prefix} {in|out}" command restores the default value.

Parameter: <*id*> is the area number which could be shown in digits ranging between 0～4294967295, or as an IP address; access-list is appointed for use in access, so is prefix-list for prefix; **<*name*>** is the name of the filter, the length of which is between 1-256; in means from other areas to this area, out means from this area to other areas.

Default: No filter configured.

Command Mode: OSPF protocol mode

Usage Guide: This command is used for restraining routes from specific area from spreading between this area and other areas.

Example: Set a filter on the area 1.

Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255

Switch(config)#access-list 1 permit any

Switch(config)#router ospf 100

Switch(config-router)#area 1 filter-list access 1 in

5.4.4 area nssa

Command: area <*id*> nssa [TRANSLATOR| no-redistribution |DEFAULT-ORIGINATE | no-summary]

no area <*id*> nssa [TRANSLATOR| no-redistribution | DEFAULT-ORIGINATE | no-summary]

Function: Set the area to Not-So-Stubby-Area (NSSA) area.

Parameter: <*id*> is the area number which could be digits ranging between 0~4294967295, and also as an IP address.

TRANLATOR = translator-role {candidate|never|always}, specifies the LSA translation mode for routes: **candidate** means if the router is elected translator, Type 7 LSA can be translated to Type-5 LSA, the default is **candidate.**

never means the router will never translate Type 7 LSA to Type 5 LSA.

always means the route always translate Type 7 LSA to Type 5 LSA.

no-redistribution means never distribute external-LSA to NSSA.

DEFAULT-ORIGINATE=default-information-originate [metric <0-16777214>] [metric-type <*1-2*>], generate the Type-7 LSA.

metric <*0-16777214*> specifies the metric value.

metric-type <*1-2*> specifies the metric value type of external-LSA , default value is 2.

no-summary shows not injecting area route to the NSSA.

Default: No NSSA area defined by default.

Command Mode: OSPF protocol mode

Usage Guide: The same area can not be both NSSA and stub at the same time.

Example: Set area 3 to NSSA.

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#area 0.0.0.51 nssa

Switch(config-router)#area 3 nssa default-information-originate metric 34 metric-type 2

translator-role candidate no-redistribution

5.4.5 area range

Command: area <*id*> range <*address*> [advertise| not-advertise| substitute]

no area <*id*> range <*address*>

Function: Aggregate OSPF route on the area border. The "**no area <*id*> range <*address*>**" cancels this function.

Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

<*address*>=<*A.B.C.D/M*> specifies the area network prefix and its length.

advertise: Advertise this area, which is the default.

not-advertise : Not advertise this area.

substitute= substitute <*A.B.C.D/M*>: advertise this area as another prefix.

<*A.B.C.D/M*>: Replace the network prefix to be advertised in this area.

Default: Not set.

Command Mode: OSPF protocol mode

Usage Guide: Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this command on ABR. This route consists of all single networks belong to specific range.

Example:

Switch#config terminal

Switch(config)# router ospf 100

Switch(config-router)# area 1 range 192.16.0.0/24

5.4.6 area stub

Command: area <*id*> stub [no-summary]

no area <*id*> stub [no-summary]

Function: Define an area to a stub area. The "**no area <*id*> stub [no-summary]**" command cancels this function.

Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

no-summary: The area border routes stop sending link summary announcement to the stub area.

Default: Not defined.

Command Mode: OSPF protocol mode

Usage Guide: Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.

Example:

Switch # config terminal

Switch (config)# router ospf 100
Switch (config-router)# area 1 stub
Related Command: area default-cost

5.4.7 area virtual-link

Command: area <*id*> virtual-link A.B.C.D {AUTHENTICATION |AUTH_KEY | INTERVAL}
no area <*id*> virtual-link A.B.C.D [AUTHENTICATION | AUTH_KEY | INTERVAL]
Function: Configure a logical link between two backbone areas physically divided by non-backbone area. The "**no area <*id*> virtual-link A.B.C.D [AUTHENTICATION | AUTH_KEY | INTERVAL]**" command removes this virtual-link.
Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.
AUTHENTICATION = authentication [message-digest[message-digest-key <1-255> md5 <LINE>] |null|AUTH_KEY].
authentication : Enable authentication on this virtual link.
message-digest: Authentication with MD-5.
null : Overwrite password or packet summary with null authentication.
AUTH_KEY= authentication-key <*key*>.
<key>: A password consists of less than 8 characters.
INTERVAL= [dead-interval | hello-interval | message-digest-key<1-255>md5<LINE> | retransmit-interval | transmit-delay] <value>.
***<value>*:>:** The delay or interval seconds, ranging between 1~65535.
***<dead-interval>*:** A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds.
***<hello-interval>*:** The time interval before the router sends a hello group message, default is 10 seconds.
<message-digest-key>: Authentication key with MD-5.
***<retransmit-interval>*:** The time interval before a router retransmitting a group message, default is 5 seconds.
***<transmit-delay>*:** The time delay before a router sending a group messages, default is 1 second.
Default: None.
Command Mode: OSPF protocol mode
Usage Guide: In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone area routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network.
Example:
Switch#config terminal
Switch(config) #router ospf 100
Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20

Relevant Commands: area authentication, show ip ospf, show ip ospf virtual-links

5.4.8 auto-cost reference-bandwidth

Command: auto-cost reference-bandwidth <*bandwith*>

no auto-cost reference-bandwidth

Function: This command sets the way in which OSPF calculate the default metric value. The "**no auto-cost reference-bandwidth**" command only configures the cost to the interface by types.

Parameter: <*bandwith*> reference bandwidth in Mbps, ranging between 1~4294967.

Default: Default bandwidth is 100Mbps.

Command Mode: OSPF protocol mode

Usage Guide: The interface metric value is acquired by divide the interface bandwith with reference bandwidth. This command is mainly for differentiate high bandwidth links. If several high bandwidth links exist, their cost can be assorted by configuring a larger reference bandwidth value.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#auto-cost reference-bandwidth 50

Relative Command: ip ospf cost

5.4.9 compatible rfc1583

Command: compatible rfc1583

no compatible rfc1583

Function: This command configures to rfc1583 compatible. The "**no compatible rfc1583**" command close the compatibility.

Default: Rfc 2328 compatible by default.

Command Mode: OSPF protocol mode

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#compatible rfc1583

5.4.10 clear ip ospf process

Command: clear ip ospf [<*process-id*>] process

Function: Use this command to clear and restart OSPF routing processes. One certain OSPF process will be cleared by specifying the process ID, or else all OSPF processes will be cleared.

Default: No default configuration.

Command Mode: Admin mode

Example:

Switch#clear ip ospf process

5.4.11 debug ospf events

Command: debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]

no debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]

Function: Open debugging switches showing various OSPF events messages; the "**no debug ospf events [abr|asbr|lsa|nssa|os|router|vlink**]" command closes the debugging switch.

Default: Closed

Command Mode: Admin and global mode

Example:

Switch#debug ospf events router

5.4.12 debug ospf ifsm

Command: debug ospf ifsm [status|events|timers]

no debug ospf ifsm [status|events|timers]

Function: Open debugging switches showing the OSPF interface states; the "**no debug ospf ifsm [status|events|timers]**" command closes this debugging switches.

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ospf ifsm events

5.4.13 debug ospf lsa

Command: debug ospf lsa [generate|flooding|install|maxage|refresh]

no debug ospf lsa [generate|flooding|install|maxage|refresh]

Function: Open debugging switches showing showing link state announcements; the "**no debug ospf lsa [generate|flooding|install|maxage|refresh]**" closes the debugging switches.

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ospf lsa generate

5.4.14 debug ospf nfsm

Command: debug ospf nfsm [status|events|timers]

no debug ospf nfsm [status|events|timers]

Function: Open debugging switches showing OSPF neighbor state machine; the "**no debug ospf nfsm [status|events|timers]**" command closes this debugging switch.

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ospf nfsm events

5.4.15 debug ospf nsm

Command: debug ospf nsm [interface|redistribute]

no debug ospf nsm [interface|redistribute]

Function: Open debugging switches showing OSPF NSM, the "**no debug ospf nsm [interface|redistribute]**" command closes this debugging switch.

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ospf nsm interface

5.4.16 debug ospf packet

Command: debug ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | detail]

no debug ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | detail]

Function: Open debugging switches showing OSPF packet messages; the "**no debug ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | detail]**" command closes this debugging switch.

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ospf packet hello

5.4.17 debug ospf route

Command: debug ospf route [ase|ia|install|spf]

no debug ospf route [ase|ia|install|spf]

Function: Open debugging switches showing OSPF related routes; the "**no debug ospf route [ase|ia|install|spf]**" command closes this debugging switch.

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ospf route spf

5.4.18 debug ospf redistribute message send

Command: debug ospf redistribute message send

no debug ospf redistribute message send

Function: To enable debugging of sending command from OSPF process redistributed to other OSPF process routing. The no form of command disables debugging of sending command from OSPF process redistributed to other OSPF process routing.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable debugging of sending command from OSPF process redistributed to other OSPF process routing.

Switch#debug ospf redistribute message send

5.4.19 debug ospf redistribute route receive

Command: debug ospf redistribute route receive

no debug ospf redistribute route receive

Function: To enable/disable debugging switch of received routing message from NSM for OSPF process.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable debugging switch of received routing message from NSM for OSPF process.

Switch# debug ospf redistribute route receive

5.4.20 default-information originate

Command: default-information originate [always | METRIC | METRICTYPE | ROUTEMAP]

no default-information originate

Function: This command create a default external route to OSPF route area; the "**no default-information originate**" closes this feature.

Parameter: always: Whether default route exist in the software or not, the default route is always advertised.

METRIC = metric <*value*>: Set the metric value for creating default route, **<*value*>** ranges between 0~16777214, default metric value is 0.

METRICTYPE = metric-type {1|2} set the OSPF external link type of default route.

1 Set the OSPF external type 1 metric value.

2 Set the OSPF external type 2 metric value.

ROUTEMAP = route-map <*WORD*>.

<WORD> specifies the route map name to be applied.

Default: Default metric value is 10; default OSPF external link type is 2.

Command Mode: OSPF protocol mode

Usage Guide: When introducing route into OSPF route area with this command, the system will behaves like an ASBR.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#default-information originate always metric 23 metric-type 2 route-map myinfo

Relevant Commands: route-map

5.4.21 default-metric

Command: default-metric <*value*>

no default-metric

Function: The command set the default metric value of OSPF routing protocol; the "**no default-metric**" returns to the default state.

Parameter: <*value*>, metric value, ranging between 0~16777214.

Default: Built-in, metric value auto translating.

Command Mode: OSPF protocol mode

Usage Guide: When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#default-metric 100

5.4.22 distance

Command: distance {<*value*>|ROUTEPARAMETER}

no distance ospf

Function: Configure OSPF manage distance base on route type. The "**no distance ospf**" command restores the default value.

Parameter: <*value*>, OSPF routing manage distance, ranging between 1~235

ROUTEPARAMETER= ospf {ROUTE1|ROUTE2|ROUTE3}.

ROUTE1= external <external-distance>, Configure the distance learnt from other routing area.

<external-distance> distance value, ranging between 1~255.

ROUTE2= inter-area <inter-distance>, configure the distance value from one area to another area.

<inter-distance> manage distance value, ranging between 1~255.

ROUTE3= intra-area <intra-distance> Configure all distance values in one area.

<intra-distance> Manage distance value, ranging between 1~255.

Default: Default distance value is 110.

Command Mode: OSPF protocol mode

Usage Guide: Manage distance shows the reliability of the routing message source. The distance value may range between 1~255. The larger the manage distance value is, the lower is its reliability.

Example:
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#distance ospf inter-area 20 intra-area 10 external 40

5.4.23 distribute-list

Command: distribute-list <*access-list-name*> out {kernel |connected| static| rip| isis| bgp}
no distribute-list out {kernel |connected| static| rip| isis| bgp}
Function: Filter network in the routing update. The "**no distribute-list out {kernel |connected| static| rip| isis| bgp}**" command disables this function.
Parameter: < *access-list-name*> is the access-list name to be applied.
out: Filter the sent route update.
kernel Kernel route.
connected Direct route.
static Static route.
rip RIP route.
isis ISIS route.
bgp BGP route.
Command Mode: OSPF protocol mode
Usage Guide: When distributing route from other routing protocols into the OSPF routing table, we can use this command.
Example: Example below is the advertisement based on the access-list list 1 of the BGP route.
Switch#config terminal
Switch(config)#access-list l1 permit 172.10.0.0 0.0.255.255
Switch(config)#router ospf 100
Switch(config-router)#redistribute bgp
Switch(config-router)#distribute-list 1 out bgp

5.4.24 filter-policy

Command: filter-policy <*access-list-name*>
no filter-policy
Function: Use access list to filter the route obtained by OSPF, the no command cancels the route filtering.
Parameter: <*access-list-name*>: Access list name will be applied, it can use numeric standard IP access list and naming standard IP access list to configure.
Default: There is no default configuration.
Command Mode: OSPF protocol mode
Usage Guide: This command is used to filter the route obtained by OSPF. Do not filter any routes when the specified access list is not exist, for the routes which do not match permit rule of access list, they will be filtered. One access list can be set for this command, only the last configuration

takes effect when configuring many times.

Example: Use access list 1 to filter the routes which do not belong to 172.10.0.0/16 segment.

Switch#config terminal

Switch(config)#access-list 1 permit 172.10.0.0 0.0.255.255

Switch(config)#router ospf

Switch(config-router)#filter-policy 1

5.4.25 host area

Command: host <*host-address*> area <*area-id*> [cost <*cost*>]

no host <*host-address*> area <*area-id*> [cost <*cost*>]

Function: Use this command to set a stub host entire belongs to certain area. The "**[no] host <*host-address*> area <*area-id*> [cost <*cost*>]**" command cancels this configuration.

Parameter: <*host-address*> is host IP address show in dotted decimal notation.

<area-id> area ID shown in dotted decimal notation or integer ranging between 0~4294967295.

<cost> specifies the entire cost, which is a integer ranging between 0~65535 and defaulted at 0.

Default: No entire set.

Command Mode: OSPF protocol mode

Usage Guide: With this command you can advertise certain specific host route out as stub link. Since the stub host belongs to special router in which setting host is not important.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#host 172.16.10.100 area 1

Switch(config-router)#host 172.16.10.101 area 2 cost 10

5.4.26 ip ospf authentication

Command: ip ospf [<*ip-address*>] authentication [message-digest md5|sm3]

no ip ospf [<*ip-address*>] authentication

Function: Specify the authentication mode required in sending and receiving OSPF packets on the interfaces; the "**no ip ospf [<*ip-address*>] authentication**" command cancels the authentication.

Parameter: <*ip-address*> is the interface IP address, shown in dotted decimal notation.

Md5: Use MD5 authentication.

Sm3: Use SM3 authentication.

Default: Authentication not required in receiving OSPF packets on the interface.

Command Mode: Interface Configuration Mode.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf authentication message-digest

5.4.27 ip ospf authentication-key

Command: ip ospf [<*ip-address*>] authentication-key <*0 LINE | 7 WORD | LINE*>

no ip ospf [<*ip-address*>] authentication

Function: Specify the authentication key required in sending and receiving OSPF packet on the interface; the no command cancels the authentication key.

Parameter: <*ip-address*> is the interface IP address shown in dotted decimal notation; **<LINE>** specifies authentication key. If key option is 0, specify plaintext key. If key option is 7, specify encrypted string. If no option, specify plaintext key by default.

Default: Authentication not required in receiving OSPF packets on the interface.

Command Mode: Interface Configuration Mode.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf authentication-key 0 password

5.4.28 ip ospf cost

Command: ip ospf [<*ip-address*>] cost <*cost*>

no ip ospf [<*ip-address*>] cost

Function: Specify the cost required in running OSPF protocol on the interface; the "**no ip ospf [<*ip-address*>] cost**" command restores the default value.

Parameter: <*ip-address*> is the interface IP address shown in dotted decimal notation.

<cost > is the cost of OSPF protocol ranging between 1~65535.

Default: Default OSPF cost on the interface is auto-figure out based bandwidth.

Command Mode: Interface Configuration Mode.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf cost 3

5.4.29 ip ospf database-filter

Command: ip ospf [<*ip-address*>] database-filter all out

no ip ospf [<*ip-address*>] database-filter

Function: The command opens LSA database filter switch on specific interface; the "**no ip ospf [<*ip-address*>] database-filter**" command closes the filter switch.

Parameter: <*ip-address*> is the interface IP address shown in dotted decimal notation;

all: All LSAs.

out: Sent LSAs.

Default: Filter switch Closed.

Command Mode: Interface Configuration Mode.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf database-filter all out

5.4.30 ip ospf dead-interval

Command: ip ospf [<*ip-address*>] dead-interval *<time >*
no ip ospf [<*ip-address*>] dead-interval

Function: Specify the dead interval for neighboring layer 3 switch; the "**no ip ospf [<*ip-address*>] dead-interval**" command restores the default value.

Parameter: <*ip-address*> is the interface IP address shown in dotted decimal notation;
<time > is the dead interval length of the neighboring layer 3 switches, shown in seconds and ranging between 1~65535.

Default: The default dead interval is 40 seconds (normally 4 times of the hello-interval).

Command Mode: Interface Configuration Mode.

Usage Guide: If no Hello data packet received after the **dead-interval** period then this layer 3 switch is considered inaccessible and invalid. This command modifies the dead interval value of neighboring layer 3 switch according to the actual link state. The set **dead-interval** value is written into the Hello packet and transmitted. To ensure the normal operation of the OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the **hello-interval** value.

Example:
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf dead-interval 80

5.4.31 ip ospf disable all

Command: ip ospf disable all
no ip ospf disable all

Function: Stop OSPF group process on the interface.

Command Mode: Interface Configuration Mode.

Usage Guide: This command resets the network area command and stops group process on specific interface.

Example:
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf disable all

5.4.32 ip ospf hello-interval

Command: ip ospf [<*ip-address*>] hello-interval *<time>*
no ip ospf [<*ip-address*>] hello-interval

Function: Specify the hello-interval on the interface; the "**no ip ospf [<*ip-address*>] hello-interval**" restores the default value.

Parameter: ***<ip-address>*** is the interface IP address shown in dotted decimal notation;

<time> is the interval sending HELLO packet, shown in seconds and ranging between 1～65535.

Default: The hello-interval on the interface is 10 seconds.

Command Mode: Interface Configuration Mode.

Usage Guide: HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set **hello-interval** value will be written into the HELLO packet and transmitted. The less the **hello-interval** value is, the sooner the network topological structure is discovered as well larger the cost. The ensure the normal operation of OSPF protocol the **hello-interval** parameter between the layer 3 switches adjacent to the interface must be in accordance.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf hello-interval 20

Relevant Commands: ip ospf dead-interval

5.4.33 ip ospf message-digest-key

Command: ip ospf [<*ip-address*>] message-digest-key <*key_id*> MD5 <*0 LINE | 7 WORD | LINE*>

no ip ospf [<*ip-address*>] message-digest-key <*key_id*>

Function: Specify the key id and value of MD5 authentication on the interface; the no command restores the default value.

Parameter: ***<ip-address>*** is the interface IP address show in dotted decimal notation;

<key_id> ranges between 1-255;

<LINE> is OSPF key. If key option is 0, specify plaintext key. If key option is 7, specify encrypted string. If no option, specify plaintext key by default.

Default: MD5 key is not configured.

Command Mode: Interface Configuration Mode.

Usage Guide: MD5 key encrypted authentication is used for ensure the safety between the OSPF routers on the network. Same key id and key should be configured between neighbors when using this command, or else no adjacent relationship will not be created.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf message-digest-key 2 MD5 0 yourpassword

5.4.34 ip ospf mtu

Command: ip ospf mtu <*mtu*>

no ip ospf mtu

Function: Specify the mtu value of the interface as the OSPF group structure according; the "**no ip ospf mtu**" command restores the default value.
Parameter: ***<mtu>*** is the interface mtu value ranging between 576~65535.
Default: Use the interface mtu acquired from the kernel.
Command Mode: Interface Configuration Mode.
Usage Guide: The interface value configured by this command is only used by OSPF protocol other than updated into kernel.
Example:
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf mtu 1480

5.4.35 ip ospf mtu-ignore

Command: ip ospf <*ip-address*> mtu-ignore
no ip ospf <*ip-address*> mtu-ignore
Function: Use this command so that the mtu size is not checked when switching DD; the "**no ip ospf <*ip-address*> mtu-ignore**" will ensure the mtu size check when performing DD switch.
Parameter: ***<ip-address>*** is the interface IP address show in dotted decimal notation.
Default: Check mtu size in DD switch.
Command Mode: Interface Configuration Mode.
Example:
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf mtu-ignore

5.4.36 ip ospf network

Command: ip ospf network {broadcast | non-broadcast | point-to-point | point-to-multipoint}
no ip ospf network
Function: This command configures the OSPF network type of the interface; the "**no ip ospf network**" command restores the default value.
Parameter: broadcast: Set the OSPF network type to broadcast.
non-broadcast: Set the OSPF network type to NBMA.
point-to-point: Set the OSPF network type to point-to-point.
point-to-multipoint: Set the OSPF network type to point-to-multipoint.
Default: The default OSPF network type is broadcast.
Command Mode: Interface Configuration Mode.
Example: The configuration below set the OSPF network type of the interface vlan 1 to point-to-point.
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf network point-to-point

5.4.37 ip ospf priority

Command: ip ospf [<*ip-address*>] priority <*priority*>

no ip ospf [<*ip-address*>] priority

Function: Configure the priority when electing "Defined layer 3 switch" at the interface. The "**no ip ospf [<*ip-address*>] priority**" command restores the default value.

Parameter: <*ip-address*> is the interface IP address show in dotted decimal notation.

<priority> is the priority of which the valid value ranges between 0～255.

Default: The default priority when electing DR is 1.

Command Mode: Interface Configuration Mode.

Usage Guide: When two layer 3 switches connected to the same segments both want to be the "Defined layer 3 switch", the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be elected as "Defined layer 3 switch" or "Backup Defined layer 3 switch".

Example: Configure the priority of DR electing. Configure the interface vlan 1 to no election right, namely set the priority to 0.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf priority 0

5.4.38 ip ospf retransmit-interval

Command: ip ospf [<*ip-address*>] retransmit-interval <*time*>

no ip ospf [<*ip-address*>] retransmit-interval

Function: Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The "**no ip ospf [<*ip-address*>] retransmit-interval**" command restores the default value.

Parameter: <*ip-address*> is the interface IP address show in dotted decimal notation.

<time> is the retransmit interveral of link state announcements between the interface and adjacent layer 3 switches, shown in seconds ang raning between 1～65535.

Default: Default retransmit interval is 5 seconds.

Command Mode: Interface Configuration Mode.

Usage Guide: When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches.

Example: Configure the LSA retransmit interval of interface vlan 1 to 10 seconds.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf retransmit-interval 10

5.4.39 ip ospf transmit-delay

Command: ip ospf [<*ip-address*>] transmit-delay *<time>*

no ip ospf [<*ip-address*>] transmit-delay

Function: Set the transmit delay value of LSA transmitting; the "**no ip ospf [<*ip-address*>] transmit-delay**" restores the default value.

Parameter: <*ip-address*> is the interface IP address show in dotted decimal notation.

<*time*> is the transmit delay value of link state announcements between the interface and adjacent layer 3 switches, shown in seconds ang raning between 1～3600.

Default: Default transmit delay value of link state announcements is 1 second.

Command Mode: Interface Configuration Mode.

Usage Guide: The LSA ages with time in the layer 3 switches, but not in the network transmitting process. By adding the **transit-delay** prior to sending the LSA, the LSA will be sent before aged.

Example: Set the LSA transmit delay of interface vlan1 to 3 seconds.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf transmit-delay 3

5.4.40 key

Command: key <*keyid*>

no key <*keyid*>

Function: This command is for managing and adding keys in the key chain. The "**no key <*keyid*>**" command deletes one key.

Parameter: <*keyid*> is key ID, ranging between 0-2147483647.

Command Mode: keychain Mode and keychain-key Mode

Usage Guide: The command permits entering the keychain-key mode and set the passwords corresponding to the keys.

Example: Switch#config terminal

Switch(config)#key chain mychain

Switch(config-keychain)#key 1

Switch(config-keychain-key)#

Relevant Commands: key chain, key-string, accept-lifetime, send-lifetime

5.4.41 key chain

Command: key chain *<name-of-chain>*

no key chain *< name-of-chain >*

Function: This command is for entering a keychain manage mode and configure a keychain. The "**no key chain *< name-of-chain >***" command deletes one keychain.

Parameter: *<name-of-chain>* is the name string of the keychain the length of which is not specifically limited.

Command Mode: Global Mode and Keychain Mode.

Example: Switch#config terminal

Switch(config)#key chain mychain

Switch(config-keychain)#

5.4.42 log-adjacency-changes detail

Command: log-adjacency-changes detail

no log-adjacency-changes detail

Function: Configure to keep a log for OSPF adjacency changes or not.

Parameter: None.

Default: Don't l keep a log for OSPF adjacency changes by default.

Command Mode: OSPF Protocol Configuration Mode

Usage Guide: When this command is configured, the OSPF adjacency changes information will be recorded into a log.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#log-adjacency-changes detail

5.4.43 max-concurrent-dd

Command: max-concurrent-dd *<value>*

no max-concurrent-dd

Function: This command set the maximum concurrent number of dd in the OSPF process; the "**no max-concurrent-dd**" command restores the default.

Parameter: *<value>* ranges between ***<1-65535>***, which is the capacity of processing the concurrent dd data packet.

Default: Not set, no concurrent dd limit.

Command Mode: OSPF protocol mode

Usage Guide: Specify the max concurrent number of dd in the OSPF process.

Example: Set the max concurrent dd to 20.

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#max-concurrent-dd 20

5.4.44 neighbor

Command: neighbor A.B.C.D [*<cost>*| priority *<value>* | poll-interval *<value>*]

no neighbor A.B.C.D [*<cost>*| priority *<value>* | poll-interval *<value>*]

Function: This command configures the OSPF router connecting NBMA network. The "**no neighbor A.B.C.D [*<cost>*| priority *<value>* | poll-interval *<value>*]**" command removes this configuration.

Parameter: <*cost*>, OSPF neighbor cost value ranging between 1-65535;

priority <*value*>, neighbor priority defaulted at 0 and ranges between 0-255;

poll-interval <*value*>, 120s by default, which the polling time before neighbor relationship come into shape , ranging between 1-65535.

Default: No default configuration.

Command Mode: OSPF protocol mode

Usage Guide: Use this command on NBMA network to configure neighbor manually. Every known non-broadcasting neighbor router should be configured with a neighbor entry. The configured neighbor address should be the main address of the interface. The poll-interval should be much larger than the hello-interval.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90

Switch(config-router)#neighbor 1.2.3.4 cost 15

5.4.45 network area

Command: network NETWORKADDRESS area <*area-id*>

no network NETWORKADDRESS area <*area-id*>

Function: This command enables OSPF routing function one the interface with IP address matched with the network address. The "**no network NETWORKADDRESS area <*area-id*>**" command removes the configuration and stop OSPF on corresponding interface.

Parameter: NETWORKADDRESS = A.B.C.D/M | A.B.C.D X.Y.Z.W, Shown with the network address prefix or the mask. Wildcast mask if shown in mask;

<*area-id*> is the ip address or area number shown in point divided demical system, if shown in demcial integer, it ranges between 0~4294967295.

Default: No default.

Command Mode: OSPF protocol mode

Usage Guide: When certain segment belongs to certain area, interface the segment belongs will be in this area, starting hello and database interaction with the connected neighbor.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#network 10.1.1.0/24 area 1

5.4.46 ospf abr-type

Command: ospf abr-type {cisco|ibm|shortcut|standard}

no ospf abr-type

Function: Use this command to configure an OSPF ABR type. The "**no ospf abr-type**" command restores the default value.

Parameter: cisco, Realize through cisco ABR;

ibm, Realize through ibm ABR;

shortcut, Specify a shortcut-ABR;

standard, Realize with standard(RFC2328)ABR.

Default: Cisco by default.

Command Mode: OSPF protocol mode

Usage Guide: For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host environment.

Example: Configure abr as standard.

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#ospf abr-type standard

5.4.47 ospf router-id

Command: ospf router-id <*address*>

no ospf router-id

Function: Specify a router ID for the OSPF process. The "**no ospf router-id**" command cancels the ID number.

Parameter: <*address*>, IPv4 address format of router-id.

Default: No default configuration.

Command Mode: OSPF protocol mode

Usage Guide: The new router-id takes effect immediately.

Example: Configure router-id of ospf 100 to 2.3.4.5.

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#ospf router-id 2.3.4.5

5.4.48 overflow database

Command: overflow database <*maxdbsize* > [{hard|soft}]

no overflow database

Function: This command is for configuring the max LSA number. The "**no overflow database**" command cancels the limit.

Default: Not configured.

Parameter: < *maxdbsize* >Max LSA numbers, ranging between 0~4294967294.

soft: Soft limit, warns when border exceeded.

hard: Hard limit, directly close ospf instance when border exceeded.

If there is not soft or hard configured, the configuration is taken as hard limit.

Command Mode: OSPF Protocol Mode.

Example:

Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#overflow database 10000 soft

5.4.49 overflow database external

Command: overflow database external [<*maxdbsize* > <*maxtime*>]

no overflow database external [<*maxdbsize* > <*maxtime*>]

Function: The command is for configuring the size of external link database and the waiting time before the route exits overflow state. The "**no overflow database external [<*maxdbsize* > <*maxtime*>]**" restores the default value.

Parameter: < *maxdbsize* > size of external link database, ranging between 0~4294967294, defaulted at 4294967294.

< *maxtime* > the seconds the router has to wait before exiting the database overflow, ranging between 0~65535.

Command Mode: OSPF protocol mode

Example:

Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#overflow database external 5 3

5.4.50 passive-interface

Command: passive-interface <*ifname*> [<*ip-address*>]

no passive-interface <*ifname*>[<*ip-address*>]

Function: Configure that the hello group not sent on specific interfaces. The "**no passive-interface <*ifname*> [<*ip-address*>]**"command cancels this function.

Parameter: <*ifname*> is the specific name of interface.

<*ip-address*> IP address of the interface in dotted decimal format.

Default: Not configured.

Command Mode: OSPF protocol mode

Example:

Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#passive-interface vlan1

5.4.51 redistribute

Command: redistribute {kernel |connected| static| rip| isis| bgp} [NAME] [metric<*value*>] [metric-type {1|2}][route-map<*word*>][tag<*tag-value*>]

no redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>][tag<*tag-value*>]

Function: Introduce route learnt from other routing protocols into OSPF.

Parameter: kernel introduce from kernel route.

connected introduce from direct route.

static introduce from static route.

rip introduce from the RIP route.

isis introduce from ISIS route.

bgp introduce from BGP route.

metric <*value*> is the introduced metric value, ranging between 0-16777214.

metric-type {1|2} is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default.

route-map <*word*> point to the probe of the route map for introducing route.

tag<*tag-value*> external identification number of the external route, ranging between 0~4294967295, defaulted at 0.

[NAME] isis area tag

Command Mode: OSPF Protocol Mode.

Usage Guide: Learn and introduce other routing protocol into OSPF area to generate AS-external_LSAs.

Example:

Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#redistribute bgp metric 12

5.4.52 redistribute ospf

Command: redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>]

no redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>]

Function: To redistribute of process ID routing to this process. The no form of command deletes the redistribution of process ID routing to this process. When input the optional parameters of metric, metric type and routermap, then restores default configuration.

Parameter: process-id is OSPF process ID, 0 by default.

metric <*value*> is the metric for redistributed routing, range between 0 to 16777214.

metric-type {1|2} is the metric type for redistributed routing, only can be 1 or 2, and 2 by default.

route-map <*word*> is the pointer to the introduced routing map.

Default: Not redistributed any OSPF routing by default.

Command Mode: OSPF Protocol Mode.

Usage Guide: When process-id is not input, that means OSPF routing will be redistributed by default (Process-id is 0).

Example:

Switch(config-router)#redistribute ospf

5.4.53 router ospf

Command: router ospf <*process_id*> <*vrf-name*>

no router ospf *<process_id> <vrf-name>*

Function: This command is for relating the OSPF process and one VPN, after the configuration succeeded, all configuration conmmands of this OSPF are relating with the VPN. The no command deletes the OSPF instance with VPN routing/ forward instance.

Parameter: ***<process_id>*** specifies the ID of the OSPF process to be created, the ranging from 1 to 65535.

<vrf-name> specifies the name of VPN routing/ forward instance.

Command Mode: Global mode

Usage Guide: Before using this command, using ip vrf command creates one VPN routing/ forward instance at first, VPN routing/ forward instance is relating with OSPF instance by this command

Example:

Switch#config terminal

Switch(config)#router ospf 100 VRF1

Switch(config-router)#network 10.1.1.0/24 area 0

5.4.54 show ip ospf

Command: show ip ospf [<*process-id*>]

Function: Display OSPF main messages.

Parameter: ***<process-id>*** is the process ID, ranging between 0~65535.

Default: Not displayed

Command Mode: Admin and configuration mode

Example:

Switch#show ip ospf

Routing Process "ospf 0" with ID 192.168.1.1

Process uptime is 2 days 0 hour 30 minutes

Conforms to RFC2328, and RFC1583Compatibility flag is disabled

Supports only single TOS(TOS0) routes

Supports opaque LSA

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Refresh timer 10 secs

Number of external LSA 0. Checksum Sum 0x000000

Number of opaque AS LSA 0. Checksum Sum 0x000000

Number of non-default external LSA 0

External LSA database is unlimited.

Number of LSA originated 0

Number of LSA received 0

Number of areas attached to this router: 1

Area 0 (BACKBONE) (Inactive)

Number of interfaces in this area is 0(0)
Number of fully adjacent neighbors in this area is 0
Area has message digest authentication
SPF algorithm executed 0 times
Number of LSA 0. Checksum Sum 0x000000

Routing Process "ospf 10" with ID 0.0.0.0
Process bound to VRF test
Process uptime is 4 days 23 hours 51 minutes
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 0
Number of LSA received 0
Number of areas attached to this router: 1
Area 0 (BACKBONE) (Inactive)
Number of interfaces in this area is 0(0)
Number of fully adjacent neighbors in this area is 0
Area has no authentication
SPF algorithm executed 0 times
Number of LSA 0. Checksum Sum 0x000000

5.4.55 show ip ospf border-routers

Command: show ip ospf [<*process-id*>] border-routers

Function: Display the intra-domain route entries for the switch to reach ABR and ASBR of all instances.

Parameter: ***<process-id>*** is the process ID, ranging between 0~65535.

Default: Not displayed

Command Mode: Admin and configuration mode

Example:

Switch#show ip ospf border-routers
OSPF process 0 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.15.0.1 [10] via 10.10.0.1, Vlan1, ASBR, Area 0.0.0.0
i 172.16.10.1 [10] via 10.10.11.50, Vlan2, ABR, ASBR, Area 0.0.0.0

5.4.56 show ip ospf database

Command: show ip ospf [<*process-id*>] database[{
adv-router [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]
| asbr-summary[{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}] | externel [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]
| network [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]
| nssa-external [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}] | opaque-area [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]
| opaque-as [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]
|opaque-link [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]
| router [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]
| summary [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}] |self-originate | max-age }]

Function: Display the OSPF link state data base messages.

Parameter: ***<process-id>*** is the process ID, ranging between 0~65535

<linkstate_id> Link state ID, shown in point divided demical system

<advertiser_router> is the ID of Advertising router, shown in point divided demcial IP address format

Default: Not displayed

Command Mode: Admin and configuration mode

Usage Guide: According to the output messages of this command, we can view the OSPF link state database messages.

Example:

Switch#show ip ospf database

Router Link States (Area 0.0.0.2)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
192.168.1.2	192.168.1.2	254	0x80000031	0xec21	1
192.168.1.3	192.168.1.3	236	0x80000033	0x0521	2

Net Link States (Area 0.0.0.2)

Link ID	ADV Router	Age	Seq#	CkSum
20.1.1.2	192.168.1.2	254	0x8000002b	0xece4

Summary Link States (Area 0.0.0.2)

Link ID	ADV Router	Age	Seq#	CkSum	Route
6.1.0.0	192.168.1.2	68	0x8000002b	0x5757	6.1.0.0/22
6.1.1.0	192.168.1.2	879	0x8000002a	0xf8bc	6.1.1.0/24
22.1.1.0	192.168.1.2	308	0x8000000c	0xc8f0	22.1.1.0/24

ASBR-Summary Link States (Area 0.0.0.2)

Link ID	ADV Router	Age	Seq#	CkSum
192.168.1.1	192.168.1.2	1702	0x8000002a	0x89c7

AS External Link States

Link ID	ADV Router	Age	Seq#	CkSum	Route
2.2.2.0	192.168.1.1	1499	0x80000056	0x3a63	E2 2.2.2.0/24 [0x0]
2.2.3.0	192.168.1.1	1103	0x8000002b	0x0ec3	E2 2.2.3.0/24 [0x0]

5.4.57 show ip ospf interface

Command: show ip ospf interface *<interface>*
Function: Display the OSPF interface messages.
Parameter: ***<interface>*** is the name of interface
Default: Not displayed
Command Mode: Admin and configuration mode
Example:

```
Switch#show ip ospf interface
Loopback is up, line protocol is up
  OSPF not enabled on this interface
Vlan1 is up, line protocol is up
  Internet Address 10.10.10.50/24, Area 0.0.0.0
    Process ID 0, Router ID 10.10.11.50, Network Type BROADCAST, Cost: 10
    Transmit Delay is 5 sec, State Waiting, Priority 1
    No designated router on this network
    No backup designated router on this network
    Timer intervals configured, Hello 35, Dead 35, Wait 35, Retransmit 5
      Hello due in 00:00:16
Neighbor Count is 0, Adjacent neighbor count is 0
```

5.4.58 show ip ospf neighbor

Command: show ip ospf [*<process-id>*] neighbor [{*<neighbor_id>* |all |detail [all] |interface *<ifaddress>*}]
Function: Display the OSPF adjacent point messages.
Parameter: ***<process-id>*** is the process ID ranging between 0~65535
<neighbor_id> is the dotted decimal notation neighbor ID
all: Display messages of all neighbors
detail: Display detailed messages of all neighbors
<ifaddress> Interface IP address
Default: Not displayed

Command Mode: Admin and configuration mode

Usage Guide: OSPF neighbor state can be checked by viewing the output of this command.

Example:

Switch#show ip ospf neighbor

OSPF process 0:

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	Full/Backup	00:00:32	6.1.1.1	Vlan1
192.168.1.3	1	Full/DR	00:00:36	20.1.1.3	Vlan2
192.168.1.3	1	Full/ -	00:00:30	20.1.1.3	VLINK2

Displayed information	Explanation
Neighbor ID	ID Neighbor ID
Priority	Priority
State	Neighbor relation state
Dead time	Neighbor dead time
Address	Interface Address
Interface	Interface name

5.4.59 show ip ospf redistribute

Command: show ip ospf [<*process-id*>] redistribute

Function: To display the routing message redistributed from external process of OSPF.

Parameter: ***<process-id>*** is the process ID ranging between 0~65535.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: None.

Example:

Switch#show ip ospf redistribute

ospf process 1 redistribute information：
ospf process 2
ospf process 3
bgp
ospf process 2 redistribute information：
ospf process 1
bgp
ospf process 3 redistribute information：
ospf process 1
bgp

Switch#show ip ospf 2 redistribute

ospf process 2 redistribute information：
ospf process 1
bgp

5.4.60 show ip ospf route

Command: show ip ospf [<*process-id*>] route
Function: Display the OSPF routing table messages.
Parameter: ***<process-id>*** is the process ID ranging between 0~65535
Default: Not displayed
Command Mode: Admin and configuration mode
Example:
Switch#show ip ospf route

O 10.1.1.0/24 [10] is directly connected, Vlan1, Area 0.0.0.0
O 10.1.1.4/32 [10] via 10.1.1.4, Vlan1, Area 0.0.0.0
IA 11.1.1.0/24 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0
IA 11.1.1.2/32 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0
IA 12.1.1.0/24 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0
IA 12.1.1.2/32 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0
O 13.1.1.0/24 [10] is directly connected, Vlan4, Area 0.0.0.3
O 14.1.1.0/24 [10] is directly connected, Vlan5, Area 0.0.0.4
IA 15.1.1.0/24 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3
IA 15.1.1.2/32 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3
E1 100.1.0.0/16 [21] via 10.1.1.1, Vlan1
E1 100.2.0.0/16 [21] via 10.1.1.1, Vlan1

5.4.61 show ip ospf virtual-links

Command: show ip ospf [<*process-id*>] virtual-links
Function: Display the OSPF virtual link message.
Parameter: ***<process-id>*** is the process ID ranging between 0~65535.
Default: Not displayed
Command Mode: Admin and configuration mode
Example:
Switch#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
  Transit area 0.0.0.1 via interface Vlan1
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
  Transit area 0.0.0.1 via interface Vlan1
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in inactive

Adjacency state Down

5.4.62 show ip route process-detail

Command: show ip route [database] process-detail

Function: Display the IP routing table with specific process ID or Tag.

Parameters: The parameter of database means displaying all the routers, no parameter means only displaying effective routers.

Default: Not importing any router of OSPF process by default.

Command Mode: Admin mode and configure mode.

Usage Guide: None.

Example:

Switch#show ip route database process-detail

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

> - selected route, * - FIB route, p - stale info

C *> 127.0.0.0/8 is directly connected, Loopback

O 192.168.2.0/24 [110/10] is directly connected, Vlan2, 00:06:13, process 12

C *> 192.168.2.0/24 is directly connected, Vlan2

5.4.63 show ip route vrf process-detail

This command is not supported by the switch.

5.4.64 show ip protocols

Command: show ip protocols

Function: Display the running routing protocol messages.

Default: None

Command Mode: Admin and configuration mode

Example:

Switch#show ip protocols

Use “show ip protocols” command will show the messages of the routing protocol running on current layer 3 switch

For example, the displayed messages are:

Routing Protocol is "ospf 0"

Invalid after 0 seconds, hold down 0, flushed after 0

Outgoing update filter list for all interfaces is

Incoming update filter list for all interfaces is

```
  Redistributing:
  Routing for Networks:
    10.1.1.0/24
    12.1.1.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
    Address         Mask          Distance List

Routing Protocol is "bgp 0"
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
  Address         FiltIn FiltOut DistIn DistOut Weight RouteMap
Incoming Route Filter:
```

5.4.65 summary-address

Command: summary-address *<A.B.C.D/M>* [{not-advertise|tag*<tag-value>*}]

Function: Summarize or restrain external route with specific address scope.

Parameter: *<A.B.C.D/M>* address scope, shown in dotted decimal notation IPv4 address plus mask length.

not-advertised restrain the external routes.

tag*<tag-value>* is the identification label of the external routes, which ranges between 0~4294967295, and is defaulted at 0.

Command Mode: OSPF protocol mode.

Usage Guide: When routes are introduced into OSPF from other routing protocols, it is required to advertise every route in a external LSA. This command is for advertise one summary route for those introduced routes contained in specific network address and masks, which could greatly reduces the size of the link state database.

Example:

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#summary-address 172.16.0.0/16 tag 3
```

5.4.66 timers spf

Command: timers spf *<spf-delay> <spf-holdtime>*

no timers spf

Function: Adjust the value of the route calculating timer. The "**no timers spf**" command restores relevant values to default.

Parameter: ***<spf-delay>*** 5 seconds by default.

<spf-holdtime> 10 seconds by default.

Command Mode: OSPF protocol mode.

Usage Guide: This command configures the delay time between receiving topology change and SPF calculation, further configured the hold item between two discontinuous SPF calculation.

Example:

Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#timers spf 5 10

5.5 BGP

5.5.1 address-family

Command: address-family ***<AFI>*** ***<SAFI>***

Function: Enter address-family mode.

Parameter: ***<AFI>*** address-family, such as IPv4, IPv6, etc;

<SAFI>: sub address-family, such as unicast, multicast, VRF

Default: None.

Command Mode: BGP routing mode.

Usage Guide: Since the BGP-4 supports multi-protocol, it is available to get different configuration for each address-family. Actually the configuration outside address-family mode is configuring the default address-family (normally IPv4 unicast). To configure non default mode, enter this address-family mode.

If support MCE, VRF has to be enabled and connected with the corresponding address-family. Configuration performed with this command to specific VRF, is independent from IPv4 unicast address-family. The VRF configuration is performed by using ip vrf <NAME> command under global mode. The address-family configuration is only available after the VRF is set.

If support MPLS VPN, VRF has to be enabled on the border routers; to realize VPN, create neighbors for BGP with the VRF address family on the private network, and with VPNv4 address-family on the public network. When configuring VPNv4 address-family with this command, IPv4 unicast address connection is available. Its neighbor configuration could be the same with IPv4 unicast only by using neighbor A.B.C.D activate on this neighbor to enable this address-family.

Example:

1) Enter IPv4 unicast address-family mode.

Switch(config-router)# address-family ipv4 unicast

2) In the example below a VRF name test is created, and then enter the BGP address-family for its configuration.

Switch(config)#ip vrf test
Switch(config-vrf)#exit
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf test
Switch(config-bgp-vrf)#
Related Command: exit-address-family

5.5.2 aggregate-address

Command: aggregate-address *<ip-address/M>* [summary-only] [as-set]
no aggregate-address *<ip-address/M>* [summary-only] [as-set]
Function: Configure the aggregate-address. The "**no aggregate-address *<ip-address/M>* [summary-only] [as-set]**" command deletes the aggregate-address.
Parameter: *<ip-address/M>*: IP address, length of mask.
[summary-only]: Send summary only ignoring specific route.
[as-set]: Show AS on the path in list, each AS is shown once.
Default: No aggregate configuration.
Command Mode: Address-family mode.
Usage Guide: Address aggregation reduces spreading routing messages outside. Use summary-only option so to spread aggregate route to the neighbors without spreading specific route. as-set option will list AS from each route covered by the aggregation only once without repeat.
Example:
Switch(config-bgp-ipv4)# aggregate-address 100.1.0.0/16 summary-only
Switch(config-bgp-ipv4)# aggregate-address 100.2.0.0/16 summary-only as-set
Switch(config-bgp-ipv4)# aggregate-address 100.3.0.0/16 as-set
Related Command: bgp aggregate-nexthop-check, no bgp aggregate-nexthop-check

5.5.3 bgp aggregate-nexthop-check

Command: bgp aggregate-nexthop-check
no bgp aggregate-nexthop-check
Function: Configures whether BGP checks all the route next-hop in aggregating. The "**no bgp aggregate-nexthop-check**" command cancels this configuration, namely not check the next-hop accordance of aggregate route.
Parameter: None.
Default: No nexthop checked during aggregating.
Command Mode: Global mode
Usage Guide: When check is enabled, the aggregate will not be performed if the next-hop of the covered routes are not in accordance. When checking is disabled, all covered route will be aggregated into the aggregate route.
Example:
Switch(config)#bgp aggregate-nexthop-check

Relevant Command: aggregate-address, no aggregate-address

5.5.4 bgp always-compare-med

Command: bgp always-compare-med

no bgp always-compare-med

Function: Configures If MED comparation is always performed. The "**no bgp always-compare-med**" command cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Normally the BGP compares the MED only when the AS is the same. By using this configuration, MED of routes from different AS source will also be compared.

Example: The AS (200) receives the same route prefix form the two AS (100 and 300) carrying different MED, configure the MED comparison is always performed.

Switch(config-router)#bgp always-compare-med

5.5.5 bgp asnotation asdot

Command: bgp asnotation asdot

no bgp asnotation asdot

Function: Show AS number and match the regular expression with ASDOT method. The no command cancels this method.

Parameter: None.

Default: ASPLAIN method.

Command mode: BGP route mode

Usage Guide: To change the method that show AS number and match the regular expression, it must configure "clear ip bgp *" to rebuild all BGP neighbor relationships after this command is configured.

Example: Show AS number and match the regular expression with ASDOT method.

Switch(config)#router bgp 200

Switch(config-router)#bgp asnotation asdot

Related Command: None.

5.5.6 bgp bestpath as-path ignore

Command: bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Function: Set to ignore the AS-PATH length. The "**no bgp bestpath as-path ignore**" command cancels this configuration.

Parameter: None.

Default: Not set.

Command Mode: BGP route mode

Usage Guide: Length of AS-PATH will be compared in BGP pathing, and its length can be ignored by using this configuration.

Example:

Set to ignore the AS-PATH length:

Switch(config)#router bgp 200

Switch(config-router)#bgp bestpath as-path ignore

Related Command: bgp bestpath compare-confed-aspath, bgp bestpath compare-routerid, bgp bestpath med, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-routerid, no bgp bestpath med

5.5.7 bgp bestpath compare-confed-aspath

Command: bgp bestpath compare-confed-aspath

no bgp bestpath compare-confed-aspath

Function: Set to concern the confederation AS-PATH length. The "**no bgp bestpath compare-confed-aspath**" command cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Normally only the length of external AS-PATH will be compared in BGP pathing. By using this configuration, lengths of AS inner confederation AS-PATH will be compared at the same time.

Example: Configure confederation AS-PATH length.

Switch(config-router)#bgp bestpath compare-confed-aspath

5.5.8 bgp bestpath compare-routerid

Command: bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Function: Compare route ID; the "**no bgp bestpath compare-routerid**" command cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Normally the first arrived route from the same AS (with other conditions equal) will be chosen as the best route. By using this command, source router ID will also be compared.

Example: Device (10.1.1.66, AS200) receives the same route prefix from two devices (10.1.1.64 and 10.1.1.68) of the same AS (100), configure the device to compare route ID.

Switch(config-router)#bgp bestpath compare-routerid

Related Command: bgp bestpath compare-confed-aspath, bgp bestpath compare-confed-aspath, bgp bestpath med, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-confed-aspath, no bgp bestpath med

5.5.9 bgp bestpath med

Command: bgp bestpath med {[confed] [missing-as-worst]}

no bgp bestpath med {[confed] [missing-as-worst]}

Function: Configure to compare the MED attributes in the confederation path and to consider the value is the largest when MED is unavailable . The "**no bgp bestpath med {[confed] [missing-as-worst]}**" command cancels this configuration.

Parameter: [confed]: Compare MED in the confederation path.

[missing-is-worst]: Consider as max MED value when missing.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Choose whether MED is compared among confederations by this command. If MED is missing, it is considered max when missing-is-worst or else 0.

Example: Configure to compare the MED attributes in the confederation path and to consider the value is the largest when MED is unavailable.

Switch(config-router)#bgp bestpath med confed missing-as-worst

Relevant Commands: bgp bestpath compare-confed-aspath, bgp bestpath compare-confed-aspath, bgp bestpath compare-routerid, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-routerid

5.5.10 bgp client-to-client reflection

Command: bgp client-to-client reflection

no bgp client-to-client reflection

Function: Configures whether the route reflection is performed. The "**no bgp client-to-client reflection**" cancels this configuration.

Parameter: None.

Default: Reflection defaulted when client is configured.

Command Mode: BGP route mode

Usage Guide: After configured reflection client with neighbor {<ip-address>|<TAG>} route-reflector-client, the router performs routing reflection in default condition. The NO form of this command cancels the route reflection among CLIENT, (reflection among Clients and non-CLIENT is not disturbed).

Example: Configure to cancel the route reflection.

Switch(config-router)#no bgp client-to-client reflection

Relevant Commands: neighbor route-reflector-client, no neighbor route-reflector-client

5.5.11 bgp cluster-id

Command: bgp cluster-id {*<ip-address>*|*<01-4294967295>*}

no bgp cluster-id {[*<ip-address>*]|*<0-4294967295>*}

Function: Configure the route reflection ID during the route reflection. The "**no bgp cluster-id**

{[*<ip-address>*]*|<0-4294967295>*}" command cancels this configuration.

Parameter: ***<ip-address>|<1-4294967295>***: cluster-id which is shown in dotted decimal notation or a 32 digit number.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: A cluster consists of one routing reflector and its clients in an area. However in order to increase the redundancy level, sometime more than one routing reflectors may be deployed in one area. Router-id is for identifying the router exclusively in an area, and cluster-id is required for two or more reflector identification.

Example: Configure the route reflection cluster-id is 1.1.1.1.

Switch(config-router)#bgp cluster-id 1.1.1.1

Related Command: neighbor route-reflector-client

5.5.12 bgp confederation identifier

Command: bgp confederation identifier <*as-id*>

no bgp confederation identifier [<*as-id*>]

Function: Create a confederation configuration. The "**no bgp confederation identifier [<*as-id*>]**" command deletes a confederation.

Parameter: ***<as-id>*:** ID number of the confederation AS, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100).

Default: No confederation.

Command Mode: BGP route mode

Usage Guide: Confederation is for divide large AS into several smaller AS, while still identified as the large AS. Create large AS number with this command.

Example:

Switch(config-router)# bgp confederation identifier 600

Related Command: bgp confederation peers, no bgp confederation peers

5.5.13 bgp confederation peers

Command: bgp confederation peers <as-id> [<as-id>..]

no bgp confederation peers <*as-id*> [<*as-id*>..]

Function: Add/delete one or several AS to a confederation.

Parameter: ***<as-id>:*** ID numbers of the AS included in the confederation, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100), which could be multiple.

Default: No members.

Command Mode: BGP route mode.

Usage Guide: Confederation is for divide large AS into several smaller AS, while still identified as the large AS. Use this command to add/delete confederation members.

Example: Create a confederation, ID is 600, add 100, 200, 100.300 members.

Switch(config-router)# bgp confederation identifier 600

Switch(config-router)#bgp confederation peers 100 200 100.300

5.5.14 bgp dampening

Command: bgp dampening [*<1-45>*] [*<1-20000>* *<1-20000>* *<1-255>*] [*<1-45>*]

no bgp dampening

Function: Configure the route dampening.The "**no bgp dampening**" command cancels the route dampening function.

Parameter: ***<1-45>***: Respectively the penalty half-lives of accessible and inaccessible route, namely the penalty value is reduced to half of the previous value, in minutes.

<1-20000>: Respectively the penalty reuse border and restrain border.

<1-255>: Maximum restrain route time, in minutes.

Default: Half-life of accessible route is 15 minutes, 15 minutes for inaccessible. The restrain border is 2000, reuse border is 750, and maximum restrain time is 60 minutes.

Command Mode: Address-family mode.

Usage Guide: Abundant route update due to unstable route could be reduced with route dampening technology, of which the algorithm is lay penalty on the route when the route fluctuates, and when penalty exceeds the restrain border this route will no longer be advertised. The penalty value will be reduced by time by the half-life index regulation if the route keeps stable and finally be advertised again when the penalty falls below the border or the restrain time exceeds the maximum restrain time. This command is for enabling/disabling the route dampening and configuring its parameters.

Example: Enable the route dampening and use the parameter configuration by default.

Switch(config-bgp-ipv4)# bgp dampening

5.5.15 bgp default

Command: bgp default {ipv4-unicast|local-preference <*0-4294967295*>}

no bgp default {ipv4-unicast|local-preference [<*0-4294967295*>]}

Function: Set the BGP defaults, the "**no bgp default {ipv4-unicast|local-preference [<*0-4294967295*>]}**" command cancels this configuration.

Parameter: ipv4-unicast: Configure the default using IPv4-unicast to set up neighbor connection.

local-preference<*0-4294967295*>: Configure the default local priority.

Default: The IPv4 unicast is default enabled when BGP is enabled. The default priority is 100.

Command Mode: BGP route mode.

Usage Guide: IPv4 unicast address-family is default enabled in BGP. Cancel this setting with no bgp default ipv4-unicast command so to not enable this address-family in default. Default local priority can be configured through bgp default local-preference command.

Example: Configure the default local priority to be 500.

Configure in 10.1.1.66:

Switch(config)#router bgp 200

Switch(config-router)# bgp default local-preference 500

5.5.16 bgp deterministic-med

Command: bgp deterministic-med

no bgp deterministic-med

Function: Use the best MED for the same prefix in the AS to compare with other AS. The "**no bgp deterministic-med**" cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Normally if same prefix routes from several paths, each path will be compared. With this configuration, the system will only use the path with the smallest MED in the AS (when other main attributes equal) to compare with other AS. After the best one is elected, select the path among AS with no regard to MED value.

Example: Set BGP to use the best MED for the same prefix in the AS to compare with other AS.

Switch(config-router)#bgp deterministic-med

5.5.17 bgp enforce-first-as

Command: bgp enforce-first-as

no bgp enforce-first-as

Function: Enforces the first AS position of the route AS-PATH contain the neighbor AS number or else disconnect this peer when the BGP is reviving the external routes. The "**no bgp enforce-first-as**" command cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: This command is usually for avoiding unsafe or unauthenticated routes.

Example:

Switch(config-router)#bgp enforce-first-as

5.5.18 bgp fast-external-failover

Command: bgp fast-external-failover

no bgp fast-external-failover

Function: Fast reset when the BGP neighbor connection varies at the interface other than wait for TCP timeout. The "**no bgp fast-external-failover**" command cancels this configuration.

Parameter: None.

Default: Configured.

Command Mode: BGP route mode

Usage Guide: This command is for immediately cutting of the neighbor connection when the interface is down.

Example:

Switch(config-router)# bgp fast-external-failover

5.5.19 bgp inbound-route-filter

Command: bgp inbound-route-filter

no bgp inbound-route-filter

Function: The bgp do not install the RD routing message which does not exist locally. The no command means the RD will be installed with no regard to the local existence of the RD.

Parameter: None.

Command Mode: BGP mode.

Usage Guide: Normally when the switch plays as PE, whether the route bgp acquired from VPN is saved in BGP depends on if the VRF configured in this PE has got matched information. With the no command the BGP will save the routing message with no regard to the matched information.

Example:

Switch(config)#router bgp 100

Switch(config-router)#no bgp inbound-route-filter

5.5.20 bgp inbound-max-route-num

Command: bgp inbound-max-route-num <0-500000>

no bgp inbound-max-route-num

Function: Set the number limit of routers learnt by the bgp process from its neighbors.

Parameters: The number limit of routers, ranging from 0 to 500000.

Default: The number limit is 50000 by default.

Command Mode: BGP routing mode.

Usage Guide: Limit the number of routers learnt by the bgp process from its neighbors with this command.

Example: The following configuration will limit max number of routers that the bgp process receives from its neighbors as 20000.

Switch(config-router)# bgp inbound-max-route-num 20000

5.5.21 bgp log-neighbor-changes

Command: bgp log-neighbor-changes

no bgp log-neighbor-changes

Function: Output log message when BGP neighbor changes. The "**no bgp log-neighbor-changes**" command cancels this configuration.

Parameter: None.

Default: default configured.

Command Mode: BGP route mode

Usage Guide: Can display neighbor change messages on the monitor.

Example:

Switch(config-router)# bgp log-neighbor-changes

5.5.22 bgp network import-check

Command: bgp network import-check

no bgp network import-check

Function: Set whether check the IGP accessibility of the BGP network route or not. The "**no bgp network import-check**" command sets to not checking the IGP accessibility.

Parameter: None.

Default: default configured.

Command Mode: BGP route mode

Usage Guide: Checking the IGP accessibility of the route advertised by BGP is to check the existence of next-hop and its IGP accessibility.

Example: Set to check the IGP accessibility of BGP network route.

Switch(config-router)# bgp network import-check

5.5.23 bgp rfc1771-path-select

Command: bgp rfc1771-path-select

no bgp rfc1771-path-select

Function: After this attribute is set, path selecting will follow the way defined in rfc 1771, namely not checking the AS internal metric, or comparing the internal METRIC.

Parameter: None.

Default: Following

Command Mode: Global mode

Usage Guide: After this attribute is set, path selecting will follow the way defined in rfc 1771, namely not checking the AS internal metric, when different AS exist, which should be perform without this attribute set.

Example: Configure to follow the rfc1771 path selecting.

Switch(config)# bgp rfc1771-path-select

5.5.24 bgp rfc1771-strict

Command: bgp rfc1771-strict

no bgp rfc1771-strict

Function: Set whether strictly follows the rfc1771 restrictions. The "**no bgp rfc1771-strict**" command set to not strictly following.

Parameter: None.

Default: Not following rfc 1771 restrictions.

Command Mode: Global mode

Usage Guide: With this attribute set, generation types of routes from protocols such as RIP, OSPF, ISIS, etc will be regarded as IGP (internal generated), or else as incomplete.

Example: Configure to stricly follow the rfc1771 restrictions.

Switch(config)#bgp rfc1771-strict

5.5.25 bgp router-id

Command: bgp router-id *<A.B.C.D>*

no bgp router-id [*<A.B.C.D>*]

Function: Configure the router ID manually. The no operation cancels this configuration.

Parameter: *<A.B.C.D>*: Router ID.

Default: Automatically acquire router ID.

Command Mode: BGP route mode

Usage Guide: Manually set the router ID with this command.

Example: Set the Router ID to be 1.1.1.1.

Switch(config-router)# bgp router-id 1.1.1.1

5.5.26 bgp scan-time

Command: bgp scan-time *<0-60>*

no bgp scan-time [*<0-60>*]

Function: Set the time interval of the periodical next-hop validation; the "**no bgp scan-time [*<0-60>*]**" command restores to the default value.

Parameter: *<0-60>*: Validation time interval.

Default: Default interval is 60s.

Command Mode: BGP route mode

Usage Guide: Validate the next-hop of BGP route, this command is for configuring the interval of this check. Set the parameter to 0 if you don't want to check.

Example: Set the time interval of periodical next-hop validation to be 30s.

Switch(config-router)# bgp scan-time 30

5.5.27 clear ip bgp

Command: clear ip bgp * [*vrf* <vrf-name>] *[in | out* | soft [*in | out]*]

Function*:* Reboot the connection between BGP of vrf-name and all peers.

Parameter: <*vrf-name*>: Configure the instance name of VPN, the ranging from 1 to 64;

in: The in soft configuration is updated;

out: The out soft configuratin is updated;

soft: The soft reboot.

Default: None.

Command Mode: Admin mode

Usage Guide: Reboot BGP when configuring clear ip bgp * command; send the requestment message to neighbor when configuring in parameter; sent the route to neighbor when configuring out parameter. If configure soft, BGP will not be reseted.

Example:

Switch#clear ip bgp * vrf VRF-A

Switch#

5.5.28 clear ip bgp dampening

Command: clear ip bgp [<*address-family*>] dampening [<ip-address>|<ip-address/M>]

Function: Used for resetting BGP routing dampening.

Parameter: <*address-family*>: address-family, such as "ipv4 unicast".

***<ip-address>*:** IP address.

***<ip-address/M>*:** IP address and mask.

Default: None.

Command Mode: Admin mode

Usage Guide: It is possible to clear BGP routing dampening messages and state by different parameters (such as address-family or IPv4 address).

Example: Clear BGP routing dampening and state of IPv4 unicast cluster.

Switch#clear ip bgp ipv4 unicast dampening

Related Command: bgp dampening

5.5.29 clear ip bgp flap-statistics

Command: clear ip bgp [*<address-family>*] flap-statistics [*<ip-address>|<ip-address/M>*]

Function: For resetting BGP routing dampening statistics messages.

Parameter: *<address-family >*: address-family such as "ipv4 unicast".

<ip-address>: IP address.

<ip-address/M>: IP address and mask.

Default: None.

Command Mode: Admin mode.

Usage Guide: It is possible to clear BGP routing dampening statistic messages and state by different parameters (such as address-family or IPv4 address).

Example: Clear the BGP dampening statistic messages of IPv4 unicast cluster.

Switch#clear ip bgp ipv4 unicast flap-statistics

5.5.30 debug bgp

Command: debug bgp [*<MODULE>*|all]

no debug bgp [*<MODULE>*|all]

Function: For BGP debugging. The "**no debug bgp [*<MODULE>*|all]**" command closes the BGP debugging messages

Parameter: *<MODULE>*: BGP module names, including dampening、events、filters、fsm、keepalives、nsm、updates, etc.

Default: None

Command Mode: Admin mode

Usage Guide: For monitoring BGP events and the encountered errors, warning messages.

Example: Display the debugging messages of all bgp modules.

Switch#debug bgp all

5.5.31 debug bgp redistribute message send

Command: debug bgp redistribute message send

no debug bgp redistribute message send

Function: To enable debugging switch of sending messages for redistribution of routing information from external process such as OSPF and RIP to BGP. The no command will disable the debugging switch.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch# debug bgp redistribute message send

Switch# no debug bgp redistribute message send

5.5.32 debug bgp redistribute route receive

Command: debug bgp redistribute route receive

no debug bgp redistribute route receive

Function: To enable debugging switch of received messages from NSM for BGP. The no form of this command will disable debugging switch of received messages from NSM for BGP.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch#debug bgp redistribute route receive

Switch#no debug bgp redistribute route receive

5.5.33 distance

Command: distance <1-255> <ip-address/M> [<WORD>]

no distance *<1-255>* *<ip-address/M>* [*<WORD>*]

Function: Set the manage distance of the routing prefix. The "**no distance *<1-255>* *<ip-address/M>* [*<WORD>*]**" command restores to the default value.

Parameter: ***<1-255>***: Manage distance.

<ip-address/M>: Routing prefix.

<WORD>: Access-list name.

Default: Not set.

Command Mode: BGP route mode

Usage Guide: Set the manage distance for specified BGP route as the path selecting basis.

Example: Set the manage distance for route 90 10.1.1.64/32 to be 90.

Switch(config-router)# distance 90 10.1.1.64/32

5.5.34 distance bgp

Command: distance bgp <*1-255*> <*1-255*> <*1-255*>

no distance bgp [<*1-255*> <*1-255*> <*1-255*>]

Function: Set the BGP protocol management distance. The "**no distance bgp [<*1-255*> <*1-255*> <*1-255*>]**" command restores the manage distance to default value.

Parameter: ***<1-255>*** Respectively the EBGP, IBGP and LOCAL manage distance of the BGP.

Default: Default EBGP is 20, others are 200.

Command Mode: BGP route mode

Usage Guide: Set the manage distance for BGP routing as the NSM path selecting basis.

Example: Set the manage distance for BGP routing as 15, the manage distance for IBGP and local routing as 150.

Switch(config-router)# distance bgp 15 150 150

5.5.35 exit-address-family

Command: exit-address-family

Function: Exit the BGP address-family mode.

Parameter: None.

Default: None.

Command Mode: BGP address-family mode

Usage Guide: Use this command to exit the mode so to end the address-family configuration when configuring address-family under BGP.

Example:

Switch(config)#router bgp 100

Switch(config-router)#address-family ipv4 unicast

Switch(config-bgp-ipv4)# exit-address-family

Switch(config-router)#

Related Command: address-family

5.5.36 import map

Command: import map <map-name>

no import map <*map-name*>

Function: Use this command to configure the route-map regulations when introducing routes into VRF.

Parameter: ***<map-name>*** is the route-map name used.

Default: None.

Command Mode: VRF mode.

Usage Guide: Use the route map command route-map NAME permit|deny <1-65535> to create the route-map and establish the regulations. Using this command will apply regulations to the route introducing of this VRF.

Example: This example configures a route map1, then configures VRF test to use the route map.

```
Switch(config)#route-map map1 permit 15
Switch(config-map)#match interface Vlan1
Switch(config-map)#set weight 655
Reconfiguring VRF test with this route-map
Switch(config-map)#exit
Switch(config)#ip vrf test
Switch(config-af)#rd 100:10
Switch(config-af)#route-target both 100:10
Switch(config-af)#import map map1
Switch#show ip bgp vpn all
     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24      11.1.1.64                0             0 200 ?
*>i15.1.1.0/24      10.1.1.68                0    100      655 300 ?
*> 20.1.1.0/24      11.1.1.64                0             0 200 ?
*>i100.1.1.0/24     10.1.1.68                0    100      655 300 ?
Route Distinguisher: 100:10
*>i15.1.1.0/24      10.1.1.68                0    100        0 300 ?
*>i100.1.1.0/24     10.1.1.68                0    100        0 300 ?
```

As we can see, the weight of the route from the VPN changes to 655 after introduced into VRF test.

5.5.37 ip as-path access-list

Command: ip as-path access-list <.LINE> {<permit>|<deny>} <LINE>

no ip as-path access-list *<.LINE>* {*<permit>|<deny>*} *<LINE>*

Function: Configure the AS-PATH access-list. The "**no ip as-path access-list *<.LINE>* {*<permit>|<deny>*} *<LINE>***" command deletes this access-list.

Parameter: *<.LINE>*: name of access-list.

<LINE>: matched strings in the AS-PATH.

Default: None.

Command Mode: Global mode.

Usage Guide: Use this command to configure the access-list related to AS-PATH, so to supply the conditions for pass/filter.

Example: Configure the access-list named ASPF, filter the AS-PATH contained route 100.

```
Switch(config)#ip as-path access-list ASPF deny ^100$
```

5.5.38 ip community-list

Command: ip community-list {*<LISTNAME>* / *<1-199>* | [expanded *<WORD>*] | [standard *<WORD>*]} {deny | permit} *<.COMMUNITY>*

no ip community-list {*<LISTNAME>* / *<1-199>* | [expanded *<WORD>*] | [standard *<WORD>*]} [{deny | permit} *<.COMMUNITY>*]

Function: Configure the community-list. The "**no ip community-list {*<LISTNAME>*|*<1-199>*|[expanded *<WORD>*]|[standard *<WORD>*]} [{deny|permit} *<.COMMUNITY>*]" command deletes the community list.

Parameter: ***<LISTNAME>***: name of community list.

<1-199>: Standard or extended community number.

<WORD>: Standard or extended community number.

<.COMMUNITY >: Members of the community list, which may be the combination of aa:nn, or internet, local-AS, no-advertise, and no-export. It can be shown in regular expressions under extended conditions.

Default: None.

Command Mode: Global mode

Usage Guide: With this command we can configure the community-list so to supply terms for the pass/filter/search.

Example: Configure the ip community-list named LN, permit community attribute as 100:10.

Switch(config)# ip community-list LN permit 100:10

5.5.39 ip extcommunity-list

Command: ip extcommunity-list {*<1-199>*|[expanded *<WORD>*]|[standard *<WORD>*]} {deny|permit} *<.COMMUNITY>*

no ip extcommunity-list {*<1-199>*|[expanded *<WORD>*]|[standard *<WORD>*]} {deny|permit} *<.COMMUNITY>*

Function: Configure the extended community-list. The "**no ip extcommunity-list {*<1-199>*|[expanded *<WORD>*]|[standard *<WORD>*]} {deny|permit} *<.COMMUNITY>***" command is for deleting the extended community list.

Parameter:

<1-199>: Standard or extended community number.

<WORD>: Standard or extended community number.

<.COMMUNITY >: Members of the community list, which may be the combination of aa:nn, or internet, local-AS, no-advertise, and no-export. It can be shown in regular expressions under extended conditions.

Default: None.

Command Mode: Global mode

Usage Guide: With this command we can configure the community-list so to supply terms for the pass/filter/search.

Example: Configure the excommunity-list named LN, permit community attribute as 100:10.

Switch(config)# ip extcommunity-list expanded LN permit 100:10

5.5.40 neighbor activate

Command: neighbor {*<ip-address>*|*<TAG>*} activate

no neighbor {*<ip-address>*|*<TAG>*} activate

Function: Configure the address family routing which do or do not switch specific address-family

with BGP neighbors. The "**no neighbor {*<ip-address>*|*<TAG>*} activate**" command is for setting the route which do not switch the specified address family.

Parameter: ***<ip-address>***: IP address of the neighbor.

<TAG>: Name of peer group.

Default: Enable the routing switch of IP unicast address-family, and disable other address-families.

Command Mode: Address-family mode.

Usage Guide: IP unicast is configured under BGP route mode. Configure whether specific address-family is switched under address-family mode. If this option on any side between local side and partner is not enabled, the address-family route will not be acquired by the partner even if the corresponding address family routes acquired before will be cancelled after this option is disabled.

Example: Configure to exchange the unicast route with neighbor 2002::2.

Switch(config-bgp-ipv4)#neighbor 2002::2 activate

Switch(config-bgp-ipv4)#no neighbor 2002::2 activate

Switch(config-router-af)#

5.5.41 neighbor advertisement-interval

Command: neighbor {*<ip-address>*|*<TAG>*} advertisement-interval *<0-600>*

no neighbor {*<ip-address>*|*<TAG>*} advertisement-interval [*<0-600>*]

Function: Configure the update interval of specific neighbor route. The "**no neighbor {*<ip-address>*|*<TAG>*} advertisement-interval [*<0-600>*]**" command restores to default.

Parameter: ***<ip-address>***: IP address of the neighbor.

<TAG>: Name of the peer group.

***<0-600>*:** Advertise interval, in seconds.

Default: Default IBGP is 5s, default EBGP is 30s.

Command Mode: BGP route mode.

Usage Guide: Reduce this value will improve the route updating speed while also consumes more bandwidth.

Example: Set the route update interval as 20s with neighbor 10.1.1.64.

Switch(config-router)#neighbor 10.1.1.64 advertisement-interval 20

5.5.42 neighbor allowas-in

Command: neighbor {*<ip-address>*|*<TAG>*} allowas-in [*<1-10>*]

no neighbor {*<ip-address>*|*<TAG>*} allowas-in

Function: Configure the counts same AS is allowed to appear in the neighbor route AS table. The "**no neighbor {*<ip-address>*|*<TAG>*} allowas-in**" restores to not allow any repeat.

Parameter: ***<ip-address>***: IP address of the neighbor.

<TAG>: Name of the peer group.

<1-10>: Allowed count of same AS number.

Default: In default conditions AS is not allowed repeating in the same route, and when set the

repeat count it is defaulted at 3 when <1-10> parameters not set.

Command Mode: Address family mode.

Usage Guide: Normally BGP will not allow same AS number appears in the route more than one time. The system will deny a route when its AS number appears in the AS-PATH. However to support some special needs, especially the VPN support, the extended BGP allows the AS re-appear counts by configuration. This command is for configure the re-appear counts.

Example: Allow the same AS to appear in the route three times for neighbor 10.1.1.66.

Switch(config-bgp-ipv4)#neighbor 10.1.1.66 allowas-in

5.5.43 neighbor as-override

Command: neighbor {<ip-address> | <TAG>} as-override

no neighbor {*<ip-address>* | *<TAG>*} as-override

Function: Cover a number of AS path and configure this command before create the neighbor. The no command deletes the configuration.

Parameters: <*ip-address*>: The specific neighbor address.

***<TAG>*:** The specific neighbor number.

Default: None.

Command Mode: VRF address family mode

Usage Guide: After configure this command, the route from the neighbor will cover the existed AS number.

Example:

Switch (config)#router bgp 100

Switch (config-router)#address-family ipv4 vrf VRF-A

Switch(config-bgp-vrf)#neighbor 3.0.0.1 remote-as 65001

Switch(config-bgp-vrf)# neighbor 3.0.0.1 as-override

Switch(config-bgp-vrf)#

5.5.44 neighbor attribute-unchanged

Command: neighbor {*<ip-address>*|*<TAG>*} attribute-unchanged [as-path] [med] [next-hop]

no neighbor {*<ip-address>*|*<TAG>*} attribute-unchanged [as-path] [med] [next-hop]

Function: Configure certain attributes which is kept unchanged for transmitting, namely the attribute transparent transmission. The "**no neighbor {*<ip-address>*|*<TAG>*} attribute-unchanged [as-path] [med] [next-hop]**" command means the attribute transparent transmission is not performed.

Parameter: *<ip-address>*: IP address of the neighbor.

***<TAG>*:** Name of the peer group.

Default: No attribute transparent defined.

Command Mode: Address-family mode.

Usage Guide: With this configuration specified route attributes will not change when transmitted to the specified neighbor. The BGP route mode is the IPv4 unicast address mode configuration. No parameter refers to above three parameter are configured together.

Example: Set the attribute of route as-path, med, next-hop unchanged for neighbor 10.1.1.64.

Switch(config-bgp-ipv4)#neighbor 10.1.1.64 attribute-unchanged

5.5.45 neighbor capability

Command: neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}

no neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}

Function: Configure dynamic update between neighbors and the route refresh capability negotiation. The "**no neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}**" command do not enable the specific capability negotiation.

Parameter: *<ip-address>*: Neighbor IP address.

***<TAG>*:** Name of peer group.

Default: Not configure the dynamic update capability but the route refresh capability.

Command Mode: BGP route mode.

Usage Guide: This is an extended BGP capability. With this configuration supported capabilities by both side will be negotiated in the OPEN messages, and the partner will respond if this capability is supported by the partner and send NOTIFICATION if not. The originating side will then send an OPEN excluded the capability to reestablish the connection. The dynamic capability refers to when the address family negotiation changes, the connection don't have to be restarted. Route refresh refers to sending refresh request when configuring some soft reconfigurable attributes and the partner will retransmit the existing route to the originating side. With route refresh attribute, the connection will not have to be restarted but be refreshed with the clear ip bgp * soft in command.

Example:

Switch(config-router)#neighbor 10.1.1.64 capability dynamic

Switch(config-router)# no neighbor 10.1.1.64 capability route-refresh

5.5.46 neighbor capability orf prefix-list

Command: neighbor {*<ip-address>*|*<TAG>*} capability orf prefix-list {*<both>*|*<send>*|*<receive>*}

no neighbor {*<ip-address>*|*<TAG>*} capability orf prefix-list {*<both>*|*<send>*|*<receive>*}

Function: Configure the out route filter capability negotiation between neighbors. The "**no neighbor {*<ip-address>*|*<TAG>*} capability orf prefix-list {*<both>*|*<send>*|*<receive>*}**" command set to not perform the negotiation.

Parameter: *<ip-address>*: Neighbor IP address.

***<TAG>*:** Name of peer group.

Default: ORF capability not configured.

Command Mode: Address-family mode.

Usage Guide: This is an extended BGP capability. With this configuration supported capabilities

by both side will be negotiated in the OPEN messages, and the partner will respond if this capability is supported by the partner and send NOTIFICATION if not. The originating side will then send an OPEN excluded the capability to reestablish the connection. With this capability, the side configured with in prefix-list filter rules will transmit its own filter rules to the peer, the peer group will apply this rule as its own out rules, so to avoid sending route which will be denied by the partner.

Example: Set to perform the out route filter capability negotiation with neighbor 10.1.1.66.

Switch(config-bgp-ipv4)#neighbor 10.1.1.66 capability orf prefix-list both

Relevant Commands: neighbor capability, no neighbor capability

5.5.47 neighbor collide-established

Command: neighbor {*<ip-address>*|*<TAG>*} collide-established

no neighbor {*<ip-address>*|*<TAG>*} collide-established

Function: Enable the collision check and settlement in the TCP connection collision. The "**no neighbor {*<ip-address>*|*<TAG>*} collide-established**" command disables the TCP connection collision settlement.

Parameter: ***<ip-address>***: Neighbor IP address.

<TAG>: Name of the peer.

Default: Disabled and Unavailable.

Command Mode: BGP route mode.

Usage Guide: This command is for settling the problem that multi-connection among peers due to TCP connection collision. Connections created with this option on will always be check even at established state. And it will be checked if local side IP is larger than partner IP when collides. If yes, the original connection will be deleted, and if not the option will be configured to only checks when the connection originated from local side at open sent and open confirm state.

Example: Set to perform the TCP connection collision check and settlement with neighbor 10.1.1.64.

Switch(config-router)#neighbor 10.1.1.64 collide-established

5.5.48 neighbor default-originate

Command: neighbor {*<ip-address>*|*<TAG>*} default-originate [route-map *<WORD>*]

no neighbor {*<ip-address>*|*<TAG>*} default-originate [route-map *<WORD>*]

Function: Configures whether enables transmitting default route to the specific neighbor. The "**no neighbor {*<ip-address>*|*<TAG>*} default-originate [route-map *<WORD>*]**" command configures not sending default route to neighbors.

Parameter: ***<ip-address>***: IP address of the neighbor.

<TAG>: Name of the peer.

<WORD>: Name of route map.

Default: Not sending default route.

Command Mode: Address-family mode.

Usage Guide: With this option, the default route of local side will be transmitted to partner, or

else not. It supplies with options of which one to supply the default route. if several neighbors of the partner supply default route, the best one will be elected according to path selecting principles. According to route mirror, it can be chosen when to send the default route.

Example: Set to transmit the local default route to neighbor 10.1.1.64.

Switch(config-router)#neighbor 10.1.1.64 default-originate

Switch(config-router)#

Then the default route from BGP will appear in partner route list.

Relevant Commands: route-map

5.5.49 neighbor description

Command: neighbor {*<ip-address>*|*<TAG>*} description *<.LINE>*

no neighbor {*<ip-address>*|*<TAG>*} description

Function: Configure the description string of the peer or peer group. The "**no neighbor {*<ip-address>*|*<TAG>*} description**" command deletes the configurations of this string.

Parameter: ***<ip-address>***: Neighbor IP address.

<TAG>: Name of peer group.

<.LINE>: Description string consists of displayable characters less than 80.

Default: Description string is empty.

Command Mode: BGP route mode.

Usage Guide: Configure the introduction of the peer or peer group.

Example: Set the description string as tester with neighbor 10.1.1.64.

Switch(config-router)#neighbor 10.1.1.64 description tester

Switch(config-router)#

5.5.50 neighbor distribute-list

Command: neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}

no neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}

Function: Configure the policy applied in partner route update transmission. The "**no neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}**" command cancels the policy configuration.

Parameter: ***<ip-address>***: Neighbor IP address.

<TAG>: Name of peer group.

<1-199>*|*<1300-2699>*|*<WORD>: Number or name of the access-list.

Default: Policy not applied.

Command Mode: Address-family mode.

Usage Guide: Configure the policies with access-list command and apply this command on route sending and receiving. It will filter the update route from partner when use in mode, and will filter the route from local side to partner with out mode.

Example: Send into neighbor route 10.1.1.66, to filter the route with the aim 100.1.0.0.

Switch(config)#access-list 101 deny ip 100.1.0.0 0.0.1.255 any

Switch(config)#access-list 101 permit ip any any

Switch(config)#router bgp 100

Switch(config-router)#address-family ipv4 unicast

Switch(config-bgp-ipv4)# neighbor 10.1.1.66 distribute-list 101 in

Related Command: ip access-list

5.5.51 neighbor dont-capability-negotiate

Command: neighbor {*<ip-address>*|*<TAG>*} dont-capability-negotiate

no neighbor {*<ip-address>*|*<TAG>*} dont-capability-negotiate

Function: Set to not perform capability negotiate in creating connections. The "**no neighbor {*<ip-address>*|*<TAG>*} dont-capability-negotiate**" command cancels this configuration.

Parameter: *<ip-address>*: Neighbor IP address.

***<TAG>*:** Name of the peer group.

Default: Capability negotiation performed.

Command Mode: BGP route mode.

Usage Guide: As the negotiation is the default, it can be disabled with this configuration when it is known that the partner BGP version is old which don't support capability negotiation.

Example: Last addition capability negotiation will not be realized in the connection by configuring as follows.

Switch(config-router)#neighbor 10.1.1.64 dont-capability-negotiate

5.5.52 neighbor ebgp-multihop

Command: neighbor {*<ip-address>*|*<TAG>*} ebgp-multihop [*<1-255>*]

no neighbor {*<ip-address>*|*<TAG>*} ebgp-multihop [*<1-255>*]

Function: Configures the EBGP neighbors can existing in different segment as well as its hop count (TTL). The "**no neighbor {*<ip-address>*|*<TAG>*} ebgp-multihop [*<1-255>*]**" set that the EBGP neighbors must be in the same segment.

Parameter: *<ip-address>*: Neighbor IP address.

<TAG>: Name of the peer group.

<1-255>: Allowed hop count.

Default: Must be in the same segment.

Command Mode: BGP route mode.

Usage Guide: Without this command, EBGP peers are required to be in the same segment and after this command is configured, peer addresses may from different segments. The allowed hop count can be configured and will be 255 if not.

Example:

Three device 10.1.1.64(AS100) and 11.1.1.120(AS300) connected respectively to the two interface 10.1.1.66 and 10.1.1.100 of another device. IGP accessibilities of 10.1.1.64 and 11.1.1.120 on both side routes are ensured through static configuration. The neighbor

relationship is established only after both side are configured as follows:
on 10.1.1.64
Switch(config-router)#neighbor 11.1.1.120 ebgp-multihop
on 11.1.1.120
Switch(config-router)#neighbor 10.1.1.64 ebgp-multihop
After this, switches in different segments will be able to create BGP neighbor relationship.

5.5.53 neighbor enforce-multihop

Command: neighbor {*<ip-address>*|*<TAG>*} enforce-multihop
no neighbor {*<ip-address>*|*<TAG>*} enforce-multihop
Function: Enforce the multihop connection to the neighbor. The "**no neighbor {*<ip-address>*|*<TAG>*} enforce-multihop**" command cancels this configuration.
Parameter: *<ip-address>*: Neighbor IP address.
***<TAG>*:** Name of peer group.
Default: Not enforced.
Command Mode: BGP route mode.
Usage Guide: In fact the direct route can not be enforced to multihop, however will be treated as a multihop connection with this configuration, namely the check originally only performed on IBGP and EBGP of non-direct routes will be performed on all after this attribute set. The nexthop direct connected check will not be performed at exit in enforce multihop conditions.
Example: Enforce neighbor 10.1.1.66 as multihop connection.
Switch(config-router)#neighbor 10.1.1.66 enforce-multihop

5.5.54 neighbor filter-list

Command: neighbor {*<ip-address>*|*<TAG>*} filter-list *<.LINE>* {*<in>*|*<out>*}
no neighbor {*<ip-address>*|*<TAG>*} filter-list *<.LINE>* {*<in>*|*<out>*}
Function: Access-list control for AS-PATH. The "**no neighbor {*<ip-address>*|*<TAG>*} filter-list *<.LINE>* {*<in>*|*<out>*}**" cancels the AS-PATH access-list control.
Parameter: *<ip-address>*: Neighbor IP address.
***<TAG>*:** Name of peer group.
***<LINE>*:** AS-PATH access-list name configured through ip as-path access-list *<.LINE> <permit|deny> <LINE>.*
Default: Not configured.
Command Mode: Address-family mode.
Usage Guide: After first configured the IP AS-PATH access-list, apply this option to specified neighbor will be able to send/receive routes with specified AS numbers in the AS list. Accepting or denying depends on the configuration of the access-list, while sending and receiving are configured by this command.
Example:
Configure the AS-PATH access control list, "ASPF" is the name of the access-list. The route with AS number of 100 will not be able to update to the partner due to the filter table control.

Switch(config)#ip as-path access-list ASPF deny 100
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-bgp-ipv4)# redistribute static
Switch(config-bgp-ipv4)# neighbor 10.1.1.66 filter-list aspf out
Relevant Commands: ip as-path access-list

5.5.55 neighbor interface

Command: neighbor *<ip-address>* interface *<IFNAM>*
no neighbor *<ip-address>* interface *<IFNAM>*
Function: Specify the interface to the neighbor. The "**no neighbor *<ip-address>* interface *<IFNAM>***"of the command cancels this configuration.
Parameter: *<ip-address>*: Neighbor IP address.
***<IFNAME>*:** Interface name, e.g. "Vlan 2".
Default: Not configured.
Command Mode: BGP route mode.
Usage Guide: Specifies the exit interface to the neighbor with this command. Interface destination accessibility should be ensured.
Example: Set the interface to neighbor 10.1.1.64 as interface vlan 2。
Switch(config-router)# neighbor 10.1.1.64 interface Vlan2

5.5.56 neighbor maximum-prefix

Command: neighbor {*<ip-address>*|*<TAG>*} maximum-prefix *<1-4294967295>* [*<1-100>* *<warning-only>*]
no neighbor {*<ip-address>*|*<TAG>*} maximum-prefix *<1-4294967295>* [*<1-100>* *<warning-only>*]
Function: Control the number of route prefix from the neighbor. The "**no neighbor {*<ip-address>*|*<TAG>*} maximum-prefix *<1-4294967295>* [*<1-100>* *<warning-only>*]**" command cancels this configuration.
Parameter: *<ip-address>*: Neighbor IP address.
<TAG>: Name of the peer.
<1-4294967295>: Max prefix value allowed.
<1-100>: Percentage of the max value at which it warns.
<warning-only>: Warning only or not.
Default: Not limited.
Command Mode: Address-family mode.
Usage Guide: Due to concerns of too much route updates from neighbors (e.g. attack), the max number of prefix acquired from a neighbor is limited, and will warns when the number hits certain rate. If the warning-only option is set, then there will be warning only, if not, the connection to the neighbor will be cut till clear the records with clear ip bgp command.
Example: Configure the maximum number of route prefix from neighbor 10.1.1.64 is 12, and it

warns when the number of route prefix reaches 6, and the connection will be cut when the number hit 13.

Switch(config-bgp-ipv4)#neighbor 10.1.1.64 maximum-prefix 12 50

5.5.57 neighbor next-hop-self

Command: neighbor {*<ip-address>*|*<TAG>*} next-hop-self

no neighbor {*<ip-address>*|*<TAG>*} next-hop-self

Function: Ask the neighbor to point the route nexthop sent by the local side to local side. The "**no neighbor {*<ip-address>*|*<TAG>*} next-hop-self**" command cancels this configuration.

Parameter: ***<ip-address>***: Neighbor IP address.

<TAG>: Name of peer group.

Default: Not configured by default.

Command Mode: Address-family mode.

Usage Guide: In the EBGP environment, the nexthop will automatically point to the source neighbor. However in IBGP environment, the nexthop remains the same for route in the same segment. If it is not broadcast network, errors will be encountered. This command is for force self as the nexthop of the neighbor under IBGP.

Example:

Switch(config-bgp-ipv4)#neighbor 10.1.1.66 next-hop-self

5.5.58 neighbor override-capability

Command: neighbor {*<ip-address>*|*<TAG>*} override-capability

no neighbor {*<ip-address>*|*<TAG>*} override-capability

Function: Whether enable overriding capability negotiation. The "**no neighbor {*<ip-address>*|*<TAG>*} override-capability**" command restores the capability negotiation.

Parameter: ***<ip-address>***: Neighbor IP address.

<TAG>: Name of the peer group.

Default: Disabled.

Command Mode: BGP route mode.

Usage Guide: With this attribute, error notify due to unsupported capability negotiation the neighbors required will not be sent.

Example:

Switch(config-router)#neighbor 10.1.1.64 override-capability

Related Command: neighbor capability

5.5.59 neighbor passive

Command: neighbor {*<ip-address>*|*<TAG>*} passive

no neighbor {*<ip-address>*|*<TAG>*} passive

Function: Configure whether the connecting request is positively sent in the connection with specified neighbor; the "**no neighbor {*<ip-address>*|*<TAG>*} passive**" command restores to

positively send the connecting request.

Parameter: ***<ip-address>***: Neighbor IP address.

<TAG>: Name of peer group.

Default: Positively send the connecting request.

Command Mode: BGP route mode.

Usage Guide: With this attribute set, the local side will not positively send the TCP connecting request after the neighbors are configured, but stays in listening mode waiting for the connecting request from partners.

Example:

Switch(config-router)#neighbor 10.1.1.64 passive

After configured with this attribute and reestablishing the connection , the local side do not attempt to create connection but stays in ACTIVE state waiting for the TCP connection request from the partner.

5.5.60 neighbor peer-group (Creating)

Command: neighbor *< TAG>* peer-group

no neighbor *< TAG>* peer-group

Function: Create/delete a peer group. The "**no neighbor *< TAG>* peer-group**" command deletes a peer group.

Parameter: *<TAG>*: Name of the peer group of which the largest length contains 256 characters.

Default: No peer group.

Command Mode: BGP route mode.

Usage Guide: By configuring the peer group, a group of peers with the same attributes will be configured at the same time so to reduce the configuration staff labor. Assign members to the peer group with neighbor <ip-address> peer-group <TAG> command.

Example:

Switch(config-router)#neighbor pg peer-group

Switch(config-router)#neighbor 10.1.1.64 peer-group pg

Switch(config-router)#neighbor pg remote-as 100

Related Command: neighbor peer-group (Configuring group members)

5.5.61 neighbor peer-group (Configuring group members)

Command: neighbor *<ip-address>* peer-group *<TAG>*

no neighbor *<ip-address>* peer-group *<TAG>*

Function: Assign/delete peers in the group. The "**no neighbor *<ip-address>* peer-group *<TAG>***" command deletes the peers from the peer group.

Parameter: *<ip-address>*: Neighbor IP address.

***<TAG>*:** Name of peer group.

Default: No peer group.

Command Mode: BGP route mode.

Usage Guide: By configuring the peer group, a group of peers with the same attributes will be configured at the same time so to reduce the configuration staff labor. Create peer group with above command and assign members into the group with this command.

Example: Refer to above examples.

Related Command: neighbor peer-group (Creating)

5.5.62 neighbor port

Command: neighbor <*ip-address*> port <*0-65535*>

no neighbor <*ip-address*> port [<*0-65535*>]

Function: Specify the TCP port number of the partner through which the communication carries. The "**no neighbor <*ip-address*> port [<*0-65535*>]**" command restores the port number to default value.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of the peer group.

<*0-65535*>: TCP port number.

Default: Default port number is 179.

Command Mode: BGP route mode.

Usage Guide: This is a configuration when the partner may connect through ports not specified by BGP.

Example:

Switch(config-router)#neighbor 10.1.1.64 port 1023

5.5.63 neighbor prefix-list

Command: neighbor {<*ip-address*>|<*TAG*>} prefix-list <*LISTNAME|number*> {<*in|out*>}

no neighbor {<*ip-address*>|<*TAG*>} prefix-list <*LISTNAME|number*> {<*in*>|<*out*>}

Function: Configure the prefix restrictions applied in sending or receiving routes from specified neighbors.The "**no neighbor {<*ip-address*>|<*TAG*>} prefix-list <*LISTNAME|number*> {<*in*>|<*out*>}**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of the peer group.

<*LISTNAME|number*>: Name or sequence number of the prefix-list.

<*in|out*>: Direction on which the restrictions applied.

Default: No prefix restrictions applied.

Command Mode: Address-family mode.

Usage Guide: Specify the prefix and its scope by configuring ip prefix-list and determines whether this scope is permitted or denied. Only the route with permitted prefix will be sent or received.

Example:

Switch(config)#ip prefix-list prw permit 100.1.0.0/22 ge 23 le 25

Switch(config)#router bgp 200

Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)#redistribute static
Switch(config-bgp-ipv4)neighbor 10.1.1.66 prefix-list prw out

5.5.64 neighbor remote-as

Command: neighbor {*<ip-address>*|*<TAG>*} remote-as *<as-id>*
no neighbor {*<ip-address>*|*<TAG>*} [remote-as *<as-id>*]
Function: Configure the BGP neighbor. The no command is used for deleting BGP neighbors.
Parameter: *<ip-address>*: Neighbor IP address
***<TAG>*:** Name of peer group
***<as-id>*:** Neighbor AS number, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100).
Default: No neighbors
Command Mode: BGP route mode.
Usage Guide: The BGP neighbors are completely generated through command configurations. A neighbor relationship can only be really established by mutual configuring. Partner AS number should be specified in configuration. The neighbor relationship can not be established when the AS number is incorrect. The partner AS number is the same with that of local side inside the AS.
Example: Configure 2 neighbor AS as 100 and 100.200.
Switch(config)#router bgp 200
Switch(config-router)# neighbor 10.1.1.64 remote-as 100
Switch(config-router)# neighbor 10.2.1.64 remote-as 100.200

5.5.65 neighbor remove-private-AS

Command: neighbor {*<ip-address>*|*<TAG>*} remove-private-AS
no neighbor {*<ip-address>*|*<TAG>*} remove-private-AS
Function: Configures whether remove the private AS number when sending to the neighbor.The "**no neighbor {*<ip-address>*|*<TAG>*} remove-private-AS**" command cancels this configuration.
Parameter: *<ip-address>*: Neighbor IP address
***<TAG>*:** Name of peer group
Default: Not configured
Command Mode: Address-family mode.
Usage Guide: Configure this attribute to avoid assigning the internal AS number to the external AS sometimes. The internal AS number ranges between 64512-65535, which the AS number could not be sent to the INTERNET since it is not a valid external AS number. What removed here is private AS numbers of the totally private AS routes. Those who have private AS numbers while also have public AS numbers are not processed.
Example:
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 remove-private-AS

5.5.66 neighbor route-map

Command: neighbor {*<ip-address>*|*<TAG>*} route-map *<NAME>* {*<in*|*out>*}

no neighbor {*<ip-address>*|*<TAG>*} route-map *<NAME>* {*<in*|*out>*}

Function: Configure the route mapping policy when sending or receiving route. The "**no neighbor {*<ip-address>*|*<TAG>*} route-map *<NAME>* {*<in*|*out>*}**" command cancels this configuration.

Parameter: *<ip-address>*: Neighbor IP address

***<TAG>*:** Name of peer group

***<NAME>*:** Name of route mapping

***<in*|*out>*:** Direction of route mapping

Default: Not set

Command Mode: Address-family mode.

Usage Guide: First it has to configure route mapping under global mode by creating a route map with route-map command and configure the match condition and actions, then the command can be applied.

Example:

```
Switch(config)#route-map test permit 5
Switch(config-route-map)#match interface Vlan1
Switch(config-route-map)#set as-path prepend 65532
Switch(config-route-map)#exit
Switch(config)#router bgp 200
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 route-map test out
```

5.5.67 neighbor route-reflector-client

Command: neighbor {*<ip-address>*|*<TAG>*} route-reflector-client

no neighbor {*<ip-address>*|*<TAG>*} route-reflector-client

Function: Configure the route reflector client. The "**no neighbor {*<ip-address>*|*<TAG>*} route-reflector-client**" command cancels this configuration

Parameter: *<ip-address>*: Neighbor IP address

***<TAG>*:** Name of peer group

Default: Not configured.

Command Mode: Address-family mode.

Usage Guide: The route reflection is used for reducing the peers when the internal IBGP routers inside AS are too much. The client only exchanges messages with route reflector while the reflector deals with message exchange among each client and other IBGP, EBGP routers. This command configures itself as the route reflector, while specific peer group is as its client. Note: this configuration is only available inside AS.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#neighbor 10.1.1.66 remote-as 100
Switch(config-router)#neighbor 10.1.1.68 remote-as 100
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)#neighbor 10.1.1.66 route-reflector-client
```

Switch(config-bgp-ipv4)#neighbor 10.1.1.68 route-reflector-client

Related Command: bgp client-to-client reflection, no bgp client-to-client reflection, bgp cluster-id

5.5.68 neighbor route-server-client

Command: neighbor {*<ip-address>*|*<TAG>*} route-server-client

no neighbor {*<ip-address>*|*<TAG>*} route-server-client

Function: Configure the route server client. The "**no neighbor {*<ip-address>*|*<TAG>*} route-server-client**" command cancels this configuration.

Parameter: *<ip-address>*: Neighbor IP address

***<TAG>*:** Name of peer group

Default: Not configured

Command Mode: Address-family mode.

Usage Guide: The route service is for reducing the peers when the router between AS is too much under EBGP environment. The server transparently transforms the routing messages to other clients with its client exchanges messages through route server.

Example:

Three routers : 10.1.1.64（AS100） and 10.1.1.68（AS300） respectively creates neighbor relationship with the connected 10.1.1.66（AS200）, the configuration is as follows:

Switch(config)#router bgp 200

Switch(config-router)#neighbor 10.1.1.64 remote-as 100

Switch(config-router)# neighbor 10.1.1.68 remote-as 300

Switch(config-router)# address-family ipv4 unicast

Switch(config-bgp-ipv4)#neighbor 10.1.1.64 route-server-client

Switch(config-bgp-ipv4)# neighbor 10.1.1.68 route-server-client

5.5.69 neighbor send-community

Command: neighbor {*<ip-address>*|*<TAG>*} send-community [both|extended|standard]

no neighbor {*<ip-address>*|*<TAG>*} send-community [both|extended|standard]

Function: Configures whether sending the community attribute to the neighbors. The "**no neighbor {*<ip-address>*|*<TAG>*} send-community [both|extended|standard]**" command set to not sending.

Parameter: *<ip-address>*: IP address of the neighbor

***<TAG>*:** Name of peer group

[both|extended|standard]: Standard community only, extended community or both.

Default: Sending the community attributes.

Command Mode: Address-family mode.

Usage Guide: The community attributes can be sent to the outside or not. By default of our company we set to sending while the default in standard protocol is not sending. By configuring

this attribute community attributes will be carried when sending routing information's to the neighbors, or else not. Omission of the following choice will be equal to standard.

Example:

Switch(config-bgp-ipv4)#no neighbor 10.1.1.66 send-community

Switch(config-bgp-ipv4)#neighbor 10.1.1.66 send-community

5.5.70 neighbor shutdown

Command: neighbor {*<ip-address>*|*<TAG>*} shutdown

no neighbor {*<ip-address>*|*<TAG>*} shutdown

Function: Disconnect the neighbor connection. The "**no neighbor {*<ip-address>*|*<TAG>*} shutdown**" cancels this configuration

Parameter: *<ip-address>*: Neighbor IP address

***<TAG>*:** Name of peer group

Default: Not disconnecting.

Command Mode: BGP route mode.

Usage Guide: Directly disconnect/connect to a peer (group) without canceling the neighbor configuration.

Example:

Switch(config-router)#neighbor 10.1.1.64 shutdown

5.5.71 neighbor soft-reconfiguration inbound

Command: neighbor {*<ip-address>*|*<TAG>*} soft-reconfiguration inbound

no neighbor {*<ip-address>*|*<TAG>*} soft-reconfiguration inbound

Function: Configures whether perform inbound soft reconfiguration; the "**no neighbor {*<ip-address>*|*<TAG>*} soft-reconfiguration inbound**" command set to not perform the inbound soft reconfiguration.

Parameter: *<ip-address>*: Neighbor IP address

<TAG>: Name of peer group

Default: Not perform inbound soft reconfiguration.

Command Mode: Address-family mode.

Command Mode: The system saves the inbound messages in the buffer after the soft reconfiguration is set, will applies as soon as it restarts so to reduce consumptions of switching with other routers. The command is only available when the route refresh capability is not enabled

Example:

Switch(config-bgp-ipv4)#neighbor 11.1.1.120 soft-reconfiguration inbound

5.5.72 neighbor soo

Command: neighbor <ip-addr> soo <soo-val>

no neighbor <*ip-addr*> soo <*soo-val*>

Function: Configure the origin source from the neighbor route, the no command will delete the configuration.

Parameters: ***<ip-addr>*** The neighbor IP address show in dotted decimal notation.

<soo-val> is the origin source ,which the format is <AA:NN>, AA is AS number, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100), NN is a random two byte number.

Default: None.

Command Mode: VRF address family mode

Usage Guide: If the user AS connects with several ISP devices, to avoid the user route returns to itself through P area, this attribute can be set. Once this attribute is set, it spreads with route. Routes carrying SOO attributes will not be spreader to a neighbor configured with the attribute.

Example:

Switch (config)#router bgp 100

Switch(config-router)#address-family ipv4 vrf test

Switch(config-bgp-vrf)# neighbor 11.1.1.64 remote 200

Switch(config-bgp-vrf)# neighbor 11.1.1.64 soo 100.100:10

After this attribute set, the switch will no longer spreads the route with 100.100:10 rt attribute to 11.1.1.64. (what have to be mentioned here is that the soo attribute will be judged together with other rt attributes, which means if the rt is configured with the same attribute, it will be regarded as the origin neighbor even if it's not the real origin source. As a matter of fact, the normal configured soo are a single configuration which is different from rt/rd and unique within the accessible scope. In this way can only the origin concept be exactly expressed).

5.5.73 neighbor strict-capability-match

Command: neighbor {*<ip-address>*|*<TAG>*} strict-capability-match

no neighbor {*<ip-address>*|*<TAG>*} strict-capability-match

Function: Configure whether strict capability match is required when establishing connections. The "**no neighbor {*<ip-address>*|*<TAG>*} strict-capability-match**" command set to not requiring strict match.

Parameter: ***<ip-address>***: Neighbor IP address

<TAG>: Name of peer group

Default: No strict capability match configured.

Command Mode: BGP route mode.

Usage Guide: This command takes effect to MP-BGP only. With this command, neighbor can be established when MP-BGP capablilities of the both side are matched, or else it can not be establised. However, whether other capablilities are matched will not affect to establish neighbor.

Example:

Switch(config-router)#neighbor 10.1.1.64 strict-capability-match

5.5.74 neighbor timers

Command: neighbor {*<ip-address>*|*<TAG>*} timers *<0-65535> <0-65535>*

no neighbor {*<ip-address>*|*<TAG>*} timers *<0-65535> <0-65535>*

Function: Configure the KEEPALIVE interval and hold time; the "**no neighbor {*<ip-address>*|*<TAG>*} timers *<0-65535> <0-65535>***" command restores the defaults.

Parameter: *<ip-address>*Neighbor IP address

<TAG>: Name of peer group

<0-65535>: Respectively the KEEPALIVE and HOLD TIME

Default: Default KEEPALIVE time is 60s, while HOLD TIME is 240s.

Command Mode: BGP route mode.

Usage Guide: Send KEEPALIVE interval and HOLD TIME intervals sent in the peer connection. The hold time is the time period for maintain the connection when no message is received from the partner (such as KEEPALIVE). And the connection will be closed after this hold time.

Example:

Switch(config-router)#neighbor 10.1.1.64 timers 50 200

Relevant Commands: neighbor timers connect, timers bgp, no timers bgp

5.5.75 neighbor timers connect

Command: neighbor {*<ip-address>*|*<TAG>*} timers connect *<0-65535>*

no neighbor {*<ip-address>*|*<TAG>*} timers connect [*<0-65535>*]

Function: Configure the connecting retry time interval. The "**no neighbor {*<ip-address>*|*<TAG>*} timers connect [*<0-65535>*]**" command restores the default value.

Parameter: *<ip-address>*: Neighbor IP address

<TAG>: Name of peer group

<0-65535>: Retry interval

Default: 120s.

Command Mode: BGP route mode.

Usage Guide: Configure the connecting time interval when connecting a peer. The NO form restores the default value.

Example:

Switch(config-router)#neighbor 10.1.1.64 timers connect 100

Related Command: neighbor timers

5.5.76 neighbor unsuppress-map

Command: neighbor {*<ip-address>*|*<TAG>*} unsuppress-map *<WORD>*

no neighbor {*<ip-address>*|*<TAG>*} unsuppress-map *<WORD>*

Function: Configure or cancel the unsurprising to conditions meet the specified route map. The "**no neighbor {*<ip-address>*|*<TAG>*} unsuppress-map *<WORD>***" command cancels this configuration.

Parameter: *<ip-address>*: Neighbor IP address.

<TAG>: Name of peer group.

<WORD>: Name of route-map.

Default: Not set.

Command Mode: Address-family mode.

Usage Guide: This command is generally for route suppressed by the aggregated and summary-only conditions. Routes meet the route map conditions will still be send separately other than suppressed.

Example:

Switch(config-bgp-ipv4)#neighbor 10.1.1.66 unsuppress-map rmp

Switch(config)#access-list 10 permit 10.1.1.100 0.0.0.255

Switch(config)#route-map rmp permit 5

Switch(config-route-map)#match ip next-hop 10

Route with nexthop as 10.1.1.100 will not be restrained.

5.5.77 neighbor update-source

Command: neighbor {*<ip-address>*|*<TAG>*} update-source *<IFNAME>*

no neighbor {*<ip-address>*|*<TAG>*} update-source *<IFNAME>*

Function: Configure the update source. The "**no neighbor {*<ip-address>*|*<TAG>*} update-source *<IFNAME>***"cancels this configuration

Parameter: ***<ip-address>***: Neighbor IP address

<TAG>: Name of peer group

<IFNAME>: Name or IP of the interface

Default: Not configured, namely use nearest interface.

Command Mode: BGP route mode.

Usage Guide: Specified update source is allowed to connect with any available interface which normally is the loop back interface. The NO forms restores to the nearest interface update source. Improper update source use may lead to neighbor connection unavailable, while the invalid interface causes problem which is also the reasons we use loop back interfaces. Note: the loop back interface should be maintained with its address accessibility to be able to establish connections when as the update source.

Example:

Switch(config-router)#neighbor 10.1.1.66 update-source 192.168.0.1

5.5.78 neighbor version 4

Command: neighbor {*<ip-address>*|*<TAG>*} version 4

Function: Configure the BGP version of the partner.

Parameter: ***<ip-address>***: Neighbor IP address

<TAG>: Name of the peer group

4: Allowed BGP version, 4 only

Default: 4.

Command Mode: BGP route mode.

Usage Guide: Only version 4 is supported so far, so whatever the configuration is the version remains at 4.

Example:

Switch(config-router)#neighbor 10.1.1.66 version 4

Switch(config-router)#

5.5.79 neighbor weight

Command: neighbor {*<ip-address>*|*<TAG>*} weight *<0-65535>*

no neighbor {*<ip-address>*|*<TAG>*} weight [*<0-65535>*]

Function: Configure the route weight sent from the partner. The "**no neighbor {*<ip-address>*|*<TAG>*} weight [*<0-65535>*]**" command restores the default value.

Parameter: ***<ip-address>***: Neighbor IP address.

<TAG>: Name of IP address.

<0-65535>: Weight.

Default: The default weight acquired from other routers is 0. The default weight on the local static configuration is 32768.

Command Mode: BGP route mode.

Default: The default weight acquired from other routers is 0. The default weight on the local static configuration is 32768.

Usage Guide: The path selecting can be affected through the configuration of the weight. The weight is only relevant to the router which is not an attribute transmittable to outside.

Example:

Switch(config-router)#neighbor 10.1.1.66 weight 500

5.5.80 network (BGP)

Command: network *<ip-address/M>* [route-map *<WORD>*] [backdoor]

no network *<ip-address/M>* [route-map *<WORD>*] [backdoor]

Function: Configure the BGP managed network, the route map specified in network application, or set the "back door" for the network. The "**no network *<ip-address/M>* [route-map *<WORD>*] [backdoor]**" command cancels this configuration.

Parameter: ***<ip-address/M>***: Network prefix identifier

<WORD>: Name of route-map

Default: None

Command Mode: Address-family mode.

Usage Guide: As for BGP routes, specify the route through which the BGP advertisements go. With the network defined by this command, the peer will be spreaded into the route map of the neighbor even if there is no route locally. Using the attribute specified in the network application through route map, when specifying the route comes from EBGP or inside the network through back door parameters, the inside route will be the optimized route even if the external route is of shorter distance.

Example:

Switch(config-bgp-ipv4)# network 172.16.0.0/16

5.5.81 redistribute (BGP)

Command: redistribute *<ROUTES>* [route-map *<WORD>*]

no redistribute *<ROUTES>* [route-map *<WORD>*]

Function: Set the BGP to redistribute route from other modes into BGP. The "**no redistribute *<ROUTES>* [route-map *<WORD>*]**" command cancels this configuration.

Parameter: *<ROUTES>*: Route source or protocol, including: connected, ISIS, kernel, OSPF, RIP, static, etc.

***<WORD>*:** Name of route map.

Default: None.

Command Mode: Address-family mode.

Usage Guide: Route from other ways will be distributed into the BGP route table with this command and transmitted to the neighbors.

Example: The static route is introduced into BGP with this configuration and advertised to the neighbors.

Switch(config-bgp-ipv4)# redistribute static

5.5.82 redistribute ospf

Command: redistribute ospf [<*process-id*>] [route-map<*word*>]

no redistribute ospf [<*process-id*>]

Function: To redistribute routing information form OSPF to BGP. The no form of this command will remove the configuration.

Parameters: process-id is the process ID of the OSPF, limited between 1 and 65535. If no process id is specified, the default process id will be used.

route-map<*word*> is the pointer to the introduced routing map.

Default: Not redistributed by default.

Command Mode: Address-family mode.

Usage Guide: None.

Example: To redistribute routing of OSPF v2 to BGP (as number is 1).

Switch(config)#router bgp 1

Switch(config-router)#address-family ipv4 unicast

Switch(config-bgp-ipv4)#redistribute ospf 2

5.5.83 router bgp

Command: router bgp *<as-id>*

no router bgp *<as-id>*

Function: Enable BGP instance. The "**no router bgp *<as-id>***" command deletes BGP instance.

Parameter: *<as-id>*: AS number, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100).

Default: BGP not enabled.

Command Mode: Global mode

Usage Guide: Enable BGP by specified AS, and then enter the config-router state, the protocol can be configured at this prompt.
Example: Enable BGP, AS number is 4294967295 in decimal notation.
Switch(config)#router bgp 4294967295
Switch(config-router)#exit

Enable BGP, AS number is 4294967295 in delimiter method.
Switch(config)#router bgp 65535.65535
Switch(config-router)#exit

5.5.84 show ip bgp

Command: show ip bgp [*<ADDRESS-FAMILY>*] [*<ip-address>*|*<ip-address/M>* [longer-prefixes]| cidr-only]
Function: For displaying the routing messages permitted by BGP.
Parameter: ***<ADDRESS-FAMILY>***: address-family such as "ipv4 unicast"
<ip-address>: IP address
<ip-address/M>: IP address and the mask
Default: None.
Command Mode: Admin and configuration mode
Usage Guide: We can display BGP routing messages by different parameters (such as address-family or IPv4 address), or a route covered by a prefix, or only the routing message don't match the earliest IP address-family (namely the route is not A or B or C type address.)
Example:
Switch#show ip bgp
BGP table version is 147, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 12.0.0.0	10.1.1.121	0		32768	?
*> 100.1.1.0/24	10.1.1.200	0		32768	?
*> 100.1.2.0/24	10.1.1.200	0		32768	?
*> 172.0.0.0/8	0.0.0.0			32768	i

Total number of prefixes 4

5.5.85 show ip bgp attribute-info

Command: show ip bgp attribute-info
Function: Display the BGP attributes messages.
Parameter: None.
Default: None.

Command Mode: Admin and configuration mode.

Usage Guide: For displaying the attribute messages permitted by BGP.

Example:

```
Switch#sh ip bgp attribute-info
attr[1] nexthop 0.0.0.0
attr[1] nexthop 10.1.1.64
attr[3] nexthop 10.1.1.64
attr[1] nexthop 10.1.1.121
attr[2] nexthop 10.1.1.200
```

5.5.86 show ip bgp community

Command: show ip bgp [*<ADDRESS-FAMILY>*] community *<TYPE>* [exact-match]

Function: For displaying route permitted by BGP with community information.

Parameter: ***<ADDRESS-FAMILY>***: Address-family, such as "ipv4 unicast"

<TYPE>: Community attributes number show in AA:NN form or combination of local-AS, no-advertise, and no-export.

Default: None

Command Mode: Admin and configuration mode

Usage Guide: We can choose several communities at a time, exact-match shows only the perfect match entries will be displayed.

Example:

```
Switch#show ip bgp community
BGP table version is 10, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     0.0.0.0                              32768 700 800 i
*> 172.0.0.0/8      0.0.0.0                              32768 700 800 i
Total number of prefixes 2
```

5.5.87 show ip bgp community-info

Command: show ip bgp community-info

Function: For displaying the community messages permitted by BGP.

Parameter: None

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Messages in the same community multiply closable at the same time.

Example:

```
Switch#show ip bgp community-info
```

Address Refcnt Community
[0x3312558] (3) 100:50

5.5.88 show ip bgp community-list

Command: show ip bgp [*<ADDRESS-FAMILY>*] community-list *<NAME>* [exact-match]

Function: For displaying the routes containing the community list messages and permitted by BGP

Parameter: ***<ADDRESS-FAMILY>***: Address-family such as “ipv4 unicast”

<NAME>: Community list

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Configure the community list with ip community-list command and the contained community as well. When displayed with its name, communities included in all the lists are contained.

Example:

```
Switch(config)#ip community-list commu per 100:50
Switch#sh ip bgp community-list commu
BGP table version is 25, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     0.0.0.0                                  32768 700 800 i
*> 172.0.0.0/8      0.0.0.0                                  32768 700 800 i
```

Related Command: ip community-list

5.5.89 show ip bgp dampening

Command: show ip bgp [<ADDRESS-FAMILY>] dampening {<dampened-paths>|<flap-statistics>|<parameters>}

Function: Display the routes permitted by BGP and relevant to the route dampening.

Parameter: ***<ADDRESS-FAMILY>***: Address-family, such as “ipv4 unicast”.

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Only the surged routes will be displayed. The Parameters shows the display configuration other than specific routes. The other two options will respectively show the restrained route and the dampening (recently recovered from invalid) routing messages.

Example:

```
Switch#sh ip bgp dampening dampened-paths
BGP table version is 12, local router ID is 10.1.1.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	From	Reuse	Path
*d 100.1.3.0/24	10.1.1.64	00:27:40	100 ?

Total number of prefixes 1

Switch#sh ip bgp dampening flap-statistics
BGP table version is 13, local router ID is 10.1.1.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	From	Flaps	Duration	Reuse	Path
*d 100.1.3.0/24	10.1.1.64	3	00:06:05	00:27:00	100 ?

Switch#sh ip bgp dampening parameters

dampening 15 750 2000 60 15 (route-map rmp)
Reach ability Half-Life time : 15 min
Reuse penalty : 750
Suppress penalty : 2000
Max suppress time : 60 min
Un-reach ability Half-Life time : 15 min
Max penalty (ceil) : 11999
Min penalty (floor) : 375
Total number of prefixes 1
Related Command: bgp dampening

5.5.90 show ip bgp filter-list

Command: show ip bgp [*<ADDRESS-FAMILY>*] filter-list [*<WORD >*]
Function: For displaying the routes in BGP meeting the specific AS filter list.
Parameter: ***<ADDRESS-FAMILY>***: address-family such as “ipv4 unicast”
< WORD >: AS-PATH access-list name
Default: None
Command Mode: Admin and configuration mode
Usage Guide: Configure AS access-list with ip as-path access-list command. This command can show the routes passed the access-list.
Example:
Switch#SH IP BGP filter-list FL
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 100.1.1.0/24	10.1.1.64	0		0	100 ?

Total number of prefixes 1

Related Command: neighbor filter-list, ip as-path access-list

5.5.91 show ip bgp inconsistent-as

Command: show ip bgp [*<ADDRESS-FAMILY>*] inconsistent-as

Function: For displaying routes with inconsistent BGP AS.

Parameter: ***<ADDRESS-FAMILY>***: address family such as “ipv4 unicast”.

Default: None

Command Mode: Admin and configuration mode

Usage Guide: If same prefix comes from different origin AS, the AS will be regarded as inconsistent. This command is for displaying this kind of routes.

Example:

Switch#sh ip bgp inconsistent-as
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	100.1.1.0/24	10.1.1.68	0		0	300 ?
*>		10.1.1.64	0		0	100 ?

Total number of prefixes 1

5.5.92 show ip bgp neighbors

Command: show ip bgp [*<ADDRESS-FAMILY>*] neighbors [IP-ADDRESS] [advertised-routes|received {prefix-filter|routes}|routes]

Function: For displaying the BGP neighbor related messages.

Parameter: ***<ADDRESS-FAMILY>***: Address-family, such as “ipv4 unicast”

<ip-address>: Neighbor IP address

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Display detailed messages of all neighbors by this command without parameters. Specifying IP address will show the detailed information of the neighbors with specified IP address. The advertised-routes、received prefix-filter、received routes、routes parameters will respectively displays the routes broadcast on local side, the received prefix filter, received routes (soft reconfiguration enabled) and the routing message from specific neighbor.

Example:

```
Switch#sh ip bgp neighbor
BGP neighbor is 10.1.1.66, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 11.1.1.100
  BGP state = Established, up for 00:13:43
  Last read 00:13:43, hold time is 240, keep alive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 17 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes
 Connections established 7; dropped 6
```

5.5.93 show ip bgp paths

Command: show ip bgp [*<ADDRESS-FAMILY>*] paths

Function: Display the path message permitted by BGP.

Parameter: ***<ADDRESS-FAMILY>***: Address-family such as “ipv4 unicast”.

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Display the BGP path message includes the utilization state.

Example:

```
Switch#sh ip bgp paths
Address          Refcnt Path
[0x331dad0:0] (1)
[0x331d850:93] (1) 600
[0x331d8d8:249] (2) 200 300
```

5.5.94 show ip bgp prefix-list

Command: show ip bgp [*<ADDRESS-FAMILY>*] prefix-list [*<NAME>*]

Function: For displaying the route meet the specific prefix-list in BGP.

Parameter: ***<ADDRESS-FAMILY>***: Address family such as “ipv4 unicast”

<NAME>: Name of prefix-list

Default: None

Command Mode: Admin and configuration mode

Usage Guide: We can select the required BGP route by regular expression.

Example:

```
Switch(config)#ip prefix-list PL permit any
Switch(config)#
Switch#sh ip bgp prefix-list PL
BGP table version is 1, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
*   100.1.1.0/24     10.1.1.66                                0 200 300 ?
*>                   10.1.1.100               0             32768 ?
Total number of prefixes 1
```

5.5.95 show ip bgp quote-regexp

Command: show ip bgp [<*ADDRESS-FAMILY*>] quote-regexp [<WORD>]

Function: For displaying the BGP route meets the specific AS related regular expression.

Parameter: <ADDRESS-FAMILY>: **>**: address-family such as “ipv4 unicast”

<WORD>: Regular expression

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Selecting the required route through regular expressions.

Example:

```
Switch#sh ip bgp quote-regexp ^300$
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
*> 100.1.1.0/24     10.1.1.68              0                0 300 ?
Total number of prefixes 1
Switch#sh ip bgp quote-regexp 100
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
```

*	100.1.1.0/24	10.1.1.64	0	0 500 100 600 ?

Total number of prefixes 1

5.5.96 show ip bgp redistribute

This command is not supported by the switch.

5.5.97 show ip bgp neighbors

This command is not supported by the switch.

5.5.98 show ip bgp regexp

Command: show ip bgp [*<ADDRESS-FAMILY>*] regexp [*<LINE>*]

Function: For displaying the BGP routes meets specific AS related normal expressions.

Parameter: ***<ADDRESS-FAMILY>***: ***>***: address-family such as “ipv4 unicast”

<LINE>: Regular expression

Default: None

Command Mode: Admin and configuration mode

Usage Guide: We can select BGP route of the required AS with normal expression.

Example:

Switch#sh ip bgp regexp 100

BGP table version is 2, local router ID is 11.1.1.100

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric LocPrf Weight Path	
*	100.1.1.0/24	10.1.1.64	0	0 500 100 600 ?

Total number of prefixes 1

5.5.99 show ip bgp route-map

Command: show ip bgp [*<ADDRESS-FAMILY>*] route-map [*<NAME>*]

Function: For displaying the BGP routes meets the specific related route map.

Parameter: ***<ADDRESS-FAMILY>***: such as “ipv4 unicast”

<NAME>: Name of route map

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Configure the route map with the route-map command, through which it can be displayed that process routes with route map. The command will display the routes meet specific route map.

Example:

Switch#sh ip bgp route-map rmp

BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	100.1.1.0/24	10.1.1.64	0		0	500 100 600 ?
*>		10.1.1.68	0		0	300 ?

Total number of prefixes 1

5.5.100 show ip bgp scan

Command: show ip bgp scan
Function: For displaying BGP scan messages.
Parameter: None
Default: None
Command Mode: Admin and configuration mode
Usage Guide: Scan regularly the nexthop messages. The command can show the current interval and related routes.
Example:
Switch#show ip bgp scan
BGP Instance: (Default) AS 200, router-id 11.1.1.100
BGP scan interval is 60
Current BGP nexthop cache:
Related Command: bgp scan-time

5.5.101 show ip bgp summary

Command: show ip bgp [*<ADDRESS-FAMILY>*] summary
Function: For displaying the BGP summary information.
Parameter: ***<ADDRESS-FAMILY>***: Address-family such as “ipv4 unicast”.
Default: None.
Command Mode: Admin and configuration mode
Usage Guide: Display some basic summary information of BGP.
Example:
Switch#show ip bgp summary
BGP router identifier 10.1.1.66, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.1.68	4	300	0	0	0	0	0	never	Active

Total number of neighbors 1

Display Contents	Explanation
identifier	Local identifier
local AS number	The number of AS of local router
table version	the version number of BGP interior database
AS-PATH entries	The tabulation of the AS-PATH entries
community entries	The property of the community entries
Neighbor	Neighbor address
V	The BGP version of neighbor running
AS	The AS number of neighbor what is affiliated with
MsgRcvd	The amount of message received from neighbor
MsgSent	The amount of message sent to the neighbor
TblVer	the version of route table
Up/Down	It will display the conversation time length if the state with neighbor was established, otherwise display the present status.
State/PfxRcd	If the state is established, display the amount of the prefix received of the router.otherwise,display the state of the neighbor at present.

5.5.102 show ip bgp view

Command: show ip bgp view [*<NAME>*] [*<ip-address>* | *<ip-address/M>* | [*<ADDRESS-FAMILY>*] summary]

Function: For displaying the messages of specified BGP instance.

Parameter: ***<NAME>***: Name of BGP instance

<ip-address>: IP address

<ip-address/M>: IP address and mask

<ADDRESS-FAMILY>: Address-family such as “ipv4 unicast”

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Display messages of specified BGP instance.

Example:

Switch#show ip bgp view as300 100.1.1.0/24

Related Command: router bgp

5.5.103 show ip bgp view neighbors

Command: show ip bgp view [*<NAME>*] neighbors [*<ip-address>*]

Function: Display neighbor messages of specified BGP instance.

Parameter: ***<NAME>***: Name of BGP instance

<ip-address>: neighbor IP address

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Display neighbor messages of specified BGP instance.

Example:

Switch#show ip bgp view as300 neighbors

5.5.104 show ip bgp vrf

Command: show ip bgp vrf [NAME] {summary | A.B.C.D | A.B.C.D/M}

Function: For displaying the routing messages and the neighbors permitted by BGP.

Parameter: <NAME>: The name of the VRF instance

summary: Display the summary information of the BGP neighbor

A.B.C.D: IP address

A.B.C.D/M: IP address and the mask

Default: None.

Command Mode: Admin and configuration mode

Usage Guide: Display BGP routing messages by different parameters (such as IPv4 address or IPv4 address/mask), or a route covered by a prefix, or only the routing information don't match the earliest IP address (namely the route is not A or B or C type address.)

Example:

1) Display the bgp neighbor information:

S2#show ip bgp vrf 1 summary

BGP router identifier 30.1.1.2, local AS number 200

BGP table version is 8

1 BGP AS-PATH entries

0 BGP community entries

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
30.1.1.1	4	100	57	51	8	0	0	00:41:44	31

Total number of neighbors 1

The explanation of the displayed contents:

Displayed Content	Explanation
identifier	The local identifier
local	AS
table	version
AS-PATH	entries
community	entries
Neighbor	Neighbor address
V	Neighbor runs BGP
AS	Neighbor belongs to AS
MsgRcvd	The information number received from the neighbor
MsgSent	The information number is sent to the neighbor

TblVer	Route table version
Up/Down	If the state is established with the neighbor, display the dialog time, or display the current state
State/PfxRcd	If the state is established with the neighbor, display the prefix number of the received route, or display the current state

2) Display the BGP route information:

```
S2#show ip bgp vrf 1
BGP routing table entry for 44.1.1.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
BGP routing table entry for 44.1.2.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
BGP routing table entry for 44.1.3.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
BGP routing table entry for 44.1.4.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
```

5.5.105 show ip bgp vpnv4

Command：show ip bgp vpnv4 {all | rd <rd-val> }

Function： This command is used to display detailed information about all VPNv4 peers or BGP neighbor connections with a specified route identifier under this switch

Parameter：all： All VPNv4 peers；

rd-val： Representing a routing identifier, usually in the form of (AS number or IP address): a number, such as 100:10；

Default： None.

Command Mode： all config mode。

Usage Guide： Can display for specified RD。

Example：

```
switch(config)#show ip bgp vpnv4 all neighbors
BGP neighbor is 11.1.1.2, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 0.0.0.0
  Neighbor under common administration
  BGP state = Active
  Last read          , hold time is 240, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 0; dropped 0
Next connect timer due in 83 seconds
```

5.5.106 timers bgp

Command: timers bgp *<0-65535> <0-65535>*

no timers bgp [*<0-65535> <0-65535>*]

Function: Configure all neighbor time in BGP. The "**no timers bgp [*<0-65535> <0-65535>*]**" command restores these times to default value.

Parameter: *<0-65535>* Respectively the KEEPALIVE interval and the hold time.

Default: KEEPALIVE is 60s, HOLD TIME is 240s.

Command Mode: Admin and Configuration Mode.

Usage Guide: Similar to neighbor time configuration which just performed on all neighbors

Example:

```
Switch(config-router)# timers bgp 50 200
```

Relevant Commands: neighbor timers, no neighbor timers

5.6 IPv4 Black Hole Routing

5.6.1 ip route null0

Command: ip route {<*ip-prefix*> <*mask*>|<*ip-prefix*>|<*prefix-length*>} null0 [<*distance*>]
no ip route {<*ip-prefix*> <*mask*>|<*ip-prefix*>|<*prefix-length*>} null0

Function: To configure routing destined to the specified network to the interface of null0.

Parameters: **<*ip-prefix*>** and **<*mask*>** are the IP address and network address mask of the destination, in dotted decimal format: **<*ip-prefix*>** and **<*prefix-length*>** are the IP address of the destination and the length of the prefix respectively; **null0** is the output interface for the black hole routing; **<*distance*>** is the management distance of the routing entry with limitation between 1 and 255.

Default: None.

Command Mode: Global Configuration Mode.

Usage Guide: Null0 should be used as the output interface for IPv4 Black Hole Routing.

Example: To configure the routing to 192.168.188.0/24 as a Black Hole Routing.

Switch (config)# ip route 192.168.188.0/24 null0 20

5.7 GRE

5.7.1 debug gre

Command: debug gre {packet | events | all}
no debug gre {packet | events | all}

Function: Open the corresponding debug switch of the GRE tunnel.

Parameter: all: Open the display function of all debug information for GRE tunnel.

packet: Open the display function of the receiving/sending packets information for GRE tunnel.

events: Open the display function of the event information for GRE tunnel.

Command mode: Admin mode

Default: None.

Example: Open the corresponding debug switch of the GRE tunnel, all the information of processing, encapsulating and forwarding of the GRE tunnel will be shown.

Switch# debug gre all

GRE Tunnel PACKET: sent, src <1.1.1.1>, dst <1.1.1.2>, size <140>, proto <0x0800>, to <tunnel1>

GRE Tunnel PACKET: recv, src <1.1.1.2>, dst <1.1.1.1>, size <140>, proto <0x0800>, from <tunnel1>

5.7.2 ip address

Command: ip address *<ipv4-address> <mask>*

no ip address *<ipv4-address> <mask>*

Function: Configure the IPv4 address of GRE tunnel interface.

Parameter: *<ipv4-address>* is IPv4 address, ***<mask>*** is the sub-net mask.

Command mode: Tunnel interface configuration mode.

Default: None.

Usage Guide: When configuring the interface address is IPv4 address for GRE tunnel, only one primary address can be set, but secondary address can not be set. This limitation will also be used to other tunnels, such as configure tunnel, 6to4, isatap.

Notice: the tunnel must stays in active state when configuring IPv4 address, so it is different to IPv6 address.

Example: Configure the interface address is IPv4 address for GRE tunnel.

Switch(config)# interface tunnel 1

Switch(config-if-tunnel1)#ip address 11.0.0.1 255.255.255.0

5.7.3 ip route

Command: ip route *<ipv4-address/mask>* tunnel *<ID>*

no ip route *<ipv4-address/mask>* tunnel *<ID>*

Function: Configure the output interface of IPv4 static route as GRE tunnel.

Parameter: *<ipv4-address >* is the IPv4 address, ***<mask>*** is the sub-net mask, ***<ID>*** is GRE tunnel ID.

Command mode: Global mode.

Default: None.

Usage Guide: Configure the output interface of IPv4 static route as GRE tunnel.

Example: Configure the output interface of IPv4 static route as GRE tunnel.

Switch(config)# interface tunnel 1

Switch(config)#ip route 101.0.0.0/24 tunnel 1

5.7.4 ipv6 address

Command: ipv6 address *<ipv6-address/prefix>*

no ipv6 address *<ipv6-address/prefix>*

Function: Configure the IPv6 address for the GRE tunnel interface.

Parameter: *<ipv6-address>* is the IPv6 address, ***<prefix>*** is prefix length.

Command mode: Tunnel interface configuration mode.

Default: None.

Usage Guide: When configuring the interface IPv6 address for GRE tunnel, and only one IPv6 address can be configured. This limitation will also be used to other tunnels, such as configure tunnel, 6to4, isatap.

Notice: 6to4 tunnel will generate an IPv6 address automatically. When configuring IPv6 address,

the tunnel may stay in active state, so it is different to IPv4 address.

Example: Configure the interface IPv6 address for GRE tunnel.

Switch(config)# interface tunnel 1

Switch(config-if-tunnel1)#ipv6 address 2011::1/64

5.7.5 ipv6 route

Command: ipv6 route *<ipv6-address/prefix>* tunnel *<ID>*

no ipv6 route *<ipv6-address/prefix>* tunnel *<ID>*

Function: Configure the output interface of IPv6 static route as GRE tunnel.

Parameter: *<ipv6-address >* is the IPv6 address, ***<prefix>*** is the prefix length, ***<ID>*** is the GRE tunnel ID.

Command mode: Global mode.

Default: None.

Usage Guide: Configure the output interface of IPv6 static route as GRE tunnel.

Example: Configure the output interface of IPv6 static route as GRE tunnel.

Switch(config)# interface tunnel 1

Switch(config)# ipv6 route 2080::/64 tunnel 1

5.7.6 loopback-group (Global)

Command: loopback-group *<id>*

no loopback-group *<id>*

Function: Create loopback-group.

Parameter: *<id>* is the loopback-group ID, the ranging from 1 to 128.

Command mode: Global Mode.

Default: None.

Usage Guide: Create loopback-group.

Example: Create loopback-group 1.

Switch(config)#loopback-group 1

5.7.7 loopback-group (Port)

Command: loopback-group *<id>*

no loopback-group *<id>*

Function: Join layer 2 Ethernet port in the specified loopback-group.

Parameter: *<id>* is the loopback-group ID, the ranging from 1 to 128.

Command mode: Port Mode.

Default: None.

Usage Guide: There is no configuration for a specified port before join it in a loopback-group.

Example: Join port 1/1/1 in loopback-group 1.

Switch (config-if-ethernet1/1/1)#loopback-group 1

5.7.8 loopback-group (Tunnel Interface)

Command: loopback-group *<id>*

no loopback-group *<id>*

Function: The specified tunnel quotes a specified loopback group.

Parameter: *<id>* is the loopback-group ID, the ranging from 1 to 128.

Command mode: Tunnel Interface Mode.

Default: None.

Usage Guide: The specified tunnel quotes a loopback group. At present only GRE tunnel and ISATAP tunnel can be supported by this function, but ISATAP tunnel quotes loopback group is mutually exclusive to nexthop configuration.

Example: The specified tunnel 1 quotes loopback group 1.

Switch (config-if-tunnel1)#loopback-group 1

5.7.9 show gre tunnel

Command: show gre tunnel {<1-50 |>}

Function: Display the configuration information of GRE tunnel.

Parameter: <1-50>: The tunnel ID.

Command mode: Admin mode and configuration mode.

Default: None.

Example: Display the configuration information of GRE tunnel.

```
Switch# show gre tunnel
name          mode          source          destination
Tunnel1       gre ip        192.168.1.1     192.168.1.2
Tunnel2       gre ipv6      2001::1         2001::2
```

Displayed Information	Explanation
name	The tunnel name
mode	The tunnel type
source	The tunnel source address （IPv4 or IPv6）
destination	The tunnel destination address（IPv4 or IPv6）

5.7.10 show interface tunnel

Command: show interface tunnel *<1-50>*

Function: Display the relative information of the tunnel interface.

Parameter: <1-50>: The tunnel ID.

Default: None.

Command mode: Admin mode and configuration mode.

Example: Display the relative information of the specific tunnel interface. If the specific tunnel is GRE tunnel, then display the relative information of the specific GRE tunnel interface.

Switch# show interface tunnel 1

```
Tunnel1 is up, line protocol is up, dev index is 8001
   Device flag 0x81(UP NOARP)
   IPv4 address is:
      (NULL)
   VRF Bind: Not Bind
```

5.7.11 tunnel destination

Command: tunnel destination <ipv4-address>

no tunnel destination

Function: Configure the IPv4 address as the destination address for GRE tunnel.

Parameter: <*ipv4-address*> is the IPv4 address.

Command mode: Tunnel interface configuration mode.

Default: None.

Usage Guide: Configure the IPv4 address as the destination address for GRE tunnel.

Example: Configure the IPv4 address as the destination address for GRE tunnel.

```
Switch(config)# interface tunnel 1
Switch(config-if-tunnel1)#tunnel destination 60.0.0.3
```

5.7.12 tunnel mode gre ip

Command: tunnel mode gre ip

no tunnel mode

Function: Configure the tunnel mode as GREv4, after data packets are encapsulated with GREv4, it has an IPv4 packet head and pass the IPv4 network.

Parameter: None.

Command mode: Tunnel interface configuration mode.

Default: None.

Usage Guide: Configure the GREv4 tunnel mode, the data packets are encapsulated with GREv4 to be forwarded.

Example: Configure the data packets to process the encapsulation of the GREv4 to be forwarded.

```
Switch(config)# interface tunnel 1
Switch(config-if-tunnel1)# tunnel mode gre ip
```

5.7.13 tunnel mode gre ipv6

This command is not supported by switch.

5.7.14 tunnel source

Command: tunnel source <ipv4-address>

no tunnel source

Function: Configure the IPv4 address as the source address for GRE tunnel.
Parameter: <*ipv4-address*> is the IPv4 address.
Command mode: Tunnel interface configuration mode.
Default: None.
Usage Guide: Configure the IPv4 address as the source address for GRE tunnel.
Example: Configure the IPv4 address as the source address for GRE tunnel.
Switch(config)# interface tunnel 1
Switch(config-if-tunnel1)#tunnel source 10.1.1.3

5.8 ECMP

5.8.1 load-balance

Command: load-balance {dst-src-mac | dst-src-ip | dst-src-mac-ip}
Function: Set load-balance mode for switch, it takes effect for port-group and ECMP at the same time.
Parameter: dst-src-mac performs load-balance according to the source and destination MAC
dst-src-ip performs load-balance according to the destination and source IP
dst-src-mac-ip performs load-balance according to the destination and source MAC, the destination and source IP
Command mode: Global mode.
Default: Perform load-balance according to the source and destination MAC.
Usage Guide: Use port-channel or ECMP to implement load-balance, user can configure the load-balance mode according to the requirements. If the specific load-balance mode of the command line is different with the current load-balance mode, then modify the load-balance as the specific load-balance of command line; otherwise return a message to notice that the current mode is already configured.
Example: Set load-balance mode.
Switch(config)#load-balance src-mac-ip

5.8.2 maximum-paths

Command: maximum-paths <1-8>
no maximum-paths
Function: This command is used to configure the maximum-paths which support the equivalence multi-paths. The no command restores the default configuration.
Parameter: <1-8>: At present, users can configure the multi-paths number from 1 to 8. When configure 1, it is equal to disable ECMP function.
Command mode: Global Mode.

Default: The default number is 4.

Usage Guide: None.

Example: Configure the maximum-paths of the equivalence multi-paths as 8.

Switch(config)# maximum-paths 8

5.8.3 load-balance hash-shift

Command：load-balance hash-shift { dstmac| srcmac | srcport | vlan | dstip | srcip | l4-srcport | l4-dstport | flow-label | proto} value < num >

Function： Set the hash-shift field of the switch to participate in the load balancing algorithm.

Parameter： dstmac： Use the shift of the dstmac to participate in the calculation；

srcmac： Use the shift of the srcmac to participate in the calculation；

srcport： Use the shift of the srcport to participate in the calculation；

vlan： Use the shift of the vlan to participate in the calculation；

dstip： Use the shift of the dstip to participate in the calculation；

srcip： Use the shift of the srcip to participate in the calculation；

l4-srcport： Use the shift of the l4-srcport to participate in the calculation；

l4-dstport： Use the shift of the l4-dstport to participate in the calculation；

flow-label： Use the shift of the flow-label to participate in the calculation；

proto： Use the shift of the proto to participate in the calculation；

num： ranging from <0-5>

Command Mode： Global Mode

Default：not set

Usage Guide： Set the field offset to evenly distribute the traffic of aggregate port members. This command aims to assist in debugging scenarios with unbalanced loads.

Example： set dstip shift 5

Switch(config)# load-balance hash-shift dstip value 5

5.9 BFD

5.9.1 bfd authentication key

Command: bfd authentication key <*1-255*>

no bfd authentication key

Function: Enable BFD authentication and configure key for interface, no command disables BFD authentication.

Parameter: <*1-255*>- key ID.

Default: Do not enable BFD authentication for interface.

Command Mode: interface configuration mode

Usage Guide: Configure key ID of BFD interface, different interfaces can use different way to encrypt and authenticate. Output: the specific BFD interface use encryption authentication.

Example: Enable BFD authentication on interface, key ID is 1.

s5(config-if-vlan50)#bfd authentication key 1

5.9.2 bfd authentication key md5|sm3

Command: bfd authentication key <*1-255*> md5|sm3 <*WORD*>

no bfd authentication key <*1-255*>

Function: Configure key and authentication character string encrypted with md5 method for BFD, no command deletes the configured key.

Parameter: <*1-255*> key ID, **<*WORD*>** key string, length from 1 to 16 bytes

Default: No key and character string are configured.

Command Mode: Global configuration mode

Usage Guide: Configure md5 mode and authentication character string for BFD authentication, BFD authentication will be processed by optional fields of packets after this command is configured. BFD will establish neighbor in case that keys in two peers are same.

Example: Use md5 to encrypt, key ID is 1, authentication character string is 123456.

s5(config)#in vlan 50

s5(config)#bfd authentication key 1 md5 123456

5.9.3 bfd authentication key text

Command: bfd authentication key <*1-255*> text <*WORD*>

no bfd authentication key <*1-255*>

Function: Configure key and authentication character string encrypted with text method for BFD, no command deletes the configured key.

Parameter: <*1-255*> key ID, **<*WORD*>** key string, length from 1 to 16 bytes

Default: No key and character string are configured.

Command Mode: Global configuration mode

Usage Guide: Configure mode and authentication character string for BFD authentication, BFD authentication will be processed by optional fields of packets after this command is configured. BFD will establish neighbor in case that keys in two peers are same.

Example: Use text to encrypt, key ID is 1, authentication character string is 123456.

s5(config)#bfd authentication key 1 text 123456

5.9.4 bfd echo

Command: bfd echo

no bfd echo

Function: Enable bfd echo, no command deletes bfd echo.

Parameter: None

Default: echo is disabled on interface.

Command Mode: Interface configuration mode

Usage Guide: Enable bfd echo, session in up mode sends echo packets to reduce frequency of control packets.

Example: Enable echo on interface.

s5(config)#in vlan 50

s5(config-if-vlan50)#bfd echo

5.9.5 bfd echo-source-ip

Command: bfd echo-source-ip *<ipv4-address>*

no bfd echo-source-ip

Function: Detect link fault by configuring source address of echo packets, no command deletes the configured source address of echo packets.

Parameter: *<ipv4-address>* is IPv4 address, the validity of parameter should be ensured by users and do not check the validity of address.

Default: No source address of echo packets is configured.

Command mode: Global mode

Usage Guide: It needs to configure source address of Echo packets when BFD echo detects IPv4 link fault. The configuration for source address is optional, it just avoids ICMP redirect packets to be sent. The destination address of packets is an interface address to ensure that packets can be returned along the original paths. There is no special request for UDP data.

Example: Configure source address of bfd echo packets to 192.168.1.1.

s5(config)#bfd echo-source-ip 192.168.1.1

5.9.6 bfd echo-source-ipv6

Command: bfd echo-source-ipv6 <*ipv6-address*>

no bfd echo-source-ipv6

Function: Detect link fault by configuring source address of echo packets, no command deletes the configured source address of echo packets.

Parameter: *<ipv6-address>* is IPv6 address, the validity of parameter should be ensured by users and do not check the validity of address.

Default: No source address of echo packets is configured.

Command mode: Global mode

Usage Guide: It needs to configure source address of Echo packets when BFD echo detects IPv6 link fault. The configuration for source address is optional, it just avoids ICMPv6 redirect packets to be sent. The destination address of packets is an interface address to ensure that packets can be returned along the original paths. There is no special request for UDP data.

Example: Configure source address of bfd echo packets to 2000::1.

s5(config)#bfd echo-source-ipv6 2000::1

5.9.7 bfd enable

Command: bfd enable

no bfd enable

Function: Enable BFD for VRRP(v3) protocol and enable BFD detection on the group, no command disables BFD for VRRP(v3) protocol.

Parameter: None.

Default: BFD is not enabled for VRRP(v3).

Command Mode: VRRP(v3) group configuration mode

Usage Guide: After enable BFD detection on the group, if the group receives hello packets when processing backup, it will inform BFD to establish the relevant session. Local ip and remote ip are IP of the interfaces at two peers.

Example: Enable BFD on VRRP group1.

s5(config)#router vrrp 1
s5(config-router)#virtual-ip 50.1.1.10
s5(config-router)#interface vlan 50
s5(config-router)#bfd enable
s5(config-router)#enable

Enable BFD on VRRPv3 group1.

s5(config)#router ipv6 vrrp 1
s5(config-router)#virtual-ipv6 fe80::1 interface vlan 50
s5(config-router)#bfd enable
s5(config-router)#enable

5.9.8 bfd interval

Command: bfd interval <*value1*> min_rx <*value2*> multiplier <*value3*>

no bfd interval

Function: Configure the minimum transmission interval and the multiplier of session detection for BFD control packets, no command restores the default detection multiplier.

Parameter: *<value1>*- minimum transmission interval, unit is ms, range from 200 to 1000, it may be different for different devices.

<value2>-minimum receiving interval, unit is ms, range from 200 to 1000, it may be different for different devices.

<*value3*>- multiplier of session detection, range from 3 to 50.

Default: minimum transmission interval is 400ms, minimum receiving interval is 400ms, detection multiplier is 5.

Command Mode: Interface configuration mode

Usage Guide: Configure the minimum transmission interval and the multiplier of session detection for BFD control packets. The default minimum interval is 400ms and detection multiplier is 5.

Example: Set the minimum transmission interval and the minimum receiving interval of BFD are 800ms, detection multiplier is 50 on interface.

s5(config)#in vlan 50

s5(config-if-vlan50)#bfd interval 800 min-rx 800 multiplier 50

s5(config-if-vlan50)#

5.9.9 bfd min-echo-recv-interval

Command: bfd min-echo-receive-interval <*value*>

no bfd min-echo-receive-interval

Function: Configure the minimum receiving interval for BFD control packets, no command restores its default value.

Parameter: *<value>*- minimum receiving interval, unit is ms, range from 200 to 1000, it may be different for different devices.

Default: minimum receiving interval is 400ms.

Command Mode: Interface configuration mode

Usage Guide: *<value>* is minimum receiving interval, unit is ms, range from 200 to 1000, it may be different for different devices. The default minimum receiving interval is 400ms.

Example: Configure the minimum receiving interval is 800ms for bfd echo packets.

s5(config)#in vlan 50

s5(config-if-vlan50)#bfd min-echo-recv-interval 800

5.9.10 bfd mode

Command: bfd mode {active | passive}

no bfd mode

Function: Configure BFD working mode before the session is established, the default mode is active mode. No command restores active mode.

Parameter: active-active mode, passive-passive mode.

Default: active mode

Command Mode: Global mode

Usage Guide: Configure BFD working mode before the session is established, the default mode is active mode. BFD control packets will be sent forwardly whether they are received or not.

Example: Configure BFD working mode as passive mode globally.

s1(config)#bfd mode passive

5.9.11 debug bfd

Command: debug bfd {packet | event | all | fsm | error | timer | notify}

Function: Enable the relevant debugging for BFD.

Parameter: all：Enable all debugging for BFD

packet：Enable the debugging of sending and receiving packets for BFD

event：Enable the debugging of events for BFD

fsm： Enable the display of state machine for BFD
error: Enable the display of error events for BFD
timer: Enable the display of timeout events for BFD
Notify: Enable the notify of infomation for BFD

Default: None.
Command Mode: Admin mode
Usage Guide: Enable the relevant debugging of BFD.
Example: Enable the debugging of BFD.
s5#debug bfd all

5.9.12 ip ospf bfd enable

Command: ip ospf bfd enable
no ip ospf bfd enable
Function: Enable BFD for OSPF protocol on the specific interface, no command disables BFD for OSPF protocol.
Parameter: None.
Default: BFD is not enabled for OSPF protocol.
Command Mode: Interface configuration mode
Usage Guide: Configure BFD for OSPF protocol enabled by the specific interface, BFD will inform OSPF after detect link fault and OSPF will deal with it in best times.
Example: Enable BFD for OSPF on interface.
s5(config-if-vlan50)#ip ospf bfd enable

5.9.13 ip route bfd

Command: ip route {vrf <*name*> <*ipv4-address*> | <*ipv4-address*>} mask <*nexthop*> bfd
no ip route {vrf <*name*> <*ipv4-address*> | <*ipv4-address*>} mask <*nexthop*> bfd
Function: Configure BFD for the static route, no command cancels the configuration.
Parameter: *<name>* is vrf name, *<ipv4-address>* is destination address, mask is the subnet mask, nexthop is nexthop address
Command Mode: Global mode
Default: BFD is not configured for the static route.
Usage Guide: Configure BFD for the route and specify the detection mode.
Example: Configure BFD for the static route.
s3(config)#ip route 10.1.1.0/24 20.1.1.2 bfd

5.9.14 ipv6 ospf bfd enable

Command: ipv6 ospf bfd enable
no ipv6 ospf bfd enable
Function: Configure BFD for OSPFv3 protocol on the specific interface, no command cancels the configuration.

Parameter: None.

Default: BFD is no enabled for OSPFv3.

Command Mode: Interface configuration mode

Usage Guide: Configure BFD for OSPFv3 protocol enabled by the specific interface, BFD will inform OSPFv3 after detect link fault and OSPFv3 will deal with it in best times.

Example: Enable BFD for OSPFv3 on interface.

s5(config-if-vlan50)#ipv ospf bfd enable

5.9.15 ipv6 ospf bfd enable instance-id

Command: ipv6 ospf bfd enable instance-id *<0-255>*

no ipv6 ospf bfd enable

Function: Configure BFD for OSPFv3 instance on the specific interface, no command cancels the configuration.

Parameter: None.

Default: BFD is no enabled for OSPFv3 instance.

Command Mode: Interface configuration mode

Usage Guide: Configure BFD for OSPFv3 instance on the specific interface which enable OSPFv3 protocol, BFD will inform OSPFv3 after detect link fault and OSPFv3 will deal with it in best times.

Example: Enable BFD for OSPFv3 on interface.

s5(config-if-vlan50)#ipv ospf bfd enable instance-id 254

5.9.16 ipv6 rip bfd enable

Command: ipv6 rip bfd enable

no ipv6 rip bfd enable

Function: Configure BFD for RIPng protocol on the specific interface, no command cancels the configuration.

Parameter: None.

Default: BFD is not enabled for RIPng.

Command Mode: Interface configuration mode

Usage Guide: Enable BFD for RIPng protocol, after that, if this interface has received RIPng packets, RIPng will inform BFD to set remote ip as session and detect the state in order to inform RIPng in time.

Example: Enable BFD for RIPng.

s5(config-if-vlan50)#ipv6 rip bfd enable

5.9.17 ipv6 route bfd

Command: ipv6 route {vrf <*name*> <*ipv6-address*> | <*ipv6-address*>} prefix <*nexthop*> bfd

no ipv6 route {vrf <name> <ipv6-address>|<ipv6-address>} prefix <*nexthop*> bfd

Function: Configure BFD for the static IPv6 route, no command cancels the configuration.

Parameter: *<name>* is vrf name, *<ipv6-address>* is destination address, prefix is prefix length, vlanid is output interface, nexthop is nexthop address.

Default: BFD is not configured for the static IPv6 route.

Command Mode: Global mode

Usage Guide: Configure BFD for the route and specify the detection mode.

Example: Configure BFD for the static IPv6 route.

s3(config)#ipv6 route 3000::/64 2010::1 bfd

5.9.18 neighbor

Command: neighbor {*<ipv6-address>* | *<ipv4-address>*} bfd

no neighbor {*<ipv6-address>* | *<ipv4-address>*}bfd

Function: Enable link detection offered by BFD on the peer neighbor of BGP(4+), no command cancels the configuration.

Parameter: *<ipv4-address>* is IPv4 address

<ipv6-address> is IPv6 address

The validity of parameter should be ensured by users and do not check the validity of address.

Default: BFD is not enabled for BGP(4+).

Command Mode: BGP(4+) route configuration mode

Usage Guide: Enable link detection offered by BFD on the peer neighbor of BGP(4+), BFD will inform BGP(4+) protocol after detect the neighbor's link fault.

Example:

Enable link detection offered by BFD on the peer neighbor of BGP.

s5(config)#router bgp 1

s5(config-router)#neighbor 1.1.1.1 bfd

Enable link detection offered by BFD on the peer neighbor of BGP4+.

s5(config-router)#router bgp 1

s5(config-router)#neighbor 2001::2 remote-as 200

s5(config-router)#neighbor 2001::2 bfd

5.9.19 rip bfd enable

Command: rip bfd enable

no rip bfd enable

Function: Configure BFD for RIP protocol on the specific interface, no command disables BFD for RIP protocol.

Parameter: None.

Default: BFD is not enabled for RIP.

Command Mode: Interface configuration mode

Usage Guide: Enable BFD for RIP protocol, after that, if this interface has received RIP packets,

RIP will inform BFD to set remote ip as session and detect the state in order to inform RIP.
Example: Enable BFD for RIP on interface.
s5(config-if-vlan50)#rip bfd enable

5.9.20 show bfd neighbor

Command: show bfd neighbor [[*<ipv6-address>*|*<ipv4-address*>] [details]]
Function: Show BFD neighbor in switch.
Parameter: *<ipv6-address>* specifies the shown neighbor shown of IPv6 address, *<ipv4-address>* specifies the shown neighbor of IPv4 address, IP address refers to remote IP address, details shows the detail information of neighbor.
Default: None.
Command Mode: Admin mode and configuration mode
Usage Guide: Show BFD neighbor in switch.
Example: Check the relevant information of BFD neighbor.
s5#show bfd neighbor 50.1.1.1 details

OurAddr	NeighAddr	LD/RD	Detec Int(ms)	State	Interface
50.1.1.5	50.1.1.1	1/1	2000	Up	3050

Local Diag: 0, Poll bit: 0
MinTx Int: 400(ms), MinRx Int: 400(ms), Multiplier: 5
Received MinRxInt: 400(ms), Received MinTxInt: 400(ms), Received Multiplier: 5
Local Act Trans Int: 400(ms), Remote Act Trans Int: 400(ms)
Local Act Detec Int: 2000(ms)
Registered protocols: RIP
Echo state: Disable, Echo Detec Int(ms): 2000
Multi Hop: No, Vrf Id: 0
Recv Ctl Pkt Num: 631, Send Ctl Pkt Num: 630
Recv Echo Pkt Num: 0, Send Echo Pkt Num: 0
Last packet: Version: 1 - Diagnostic: 0
Poll bit: 0 - Final bit: 0
Multiplier: 5 - Length: 24
My Discr: 1 - Your Discr: 1
Min tx interval: 400(ms) - Min rx interval: 400(ms)
Min Echo interval: 400(ms)

5.10 BGP GR

5.10.1 bgp graceful-restart

Command: bgp graceful-restart

no bgp graceful-restart

Function: Enable BGP to support GR and set restart-time and stale-path-time as the default value, no command disables GR.

Parameter: None.

Command Mode: BGP router configuration mode

Default: Do not enable BGP to support GR.

Usage Guide: None

Example: Configure GR.

Switch(config-router)# bgp graceful-restart

5.10.2 bgp graceful-restart restart-time

Command: bgp graceful-restart restart-time <1-3600>

no bgp graceful-restart restart-time <1-3600>

Function: Configure BGP GR's restart-time (Receiving Speaker enables a timeout timer for a neighbor, it uses the restart-time as the timeout). A restart-time specifies the longest waiting time from Receiving Speaker finds restarting to the received OPEN messages. If Receiving Speaker does not receive OPEN messages after exceed the time, it can delete SATLE route saved by neighbor. No command restores restart-time as the default value of 120 seconds.

Parameter: <1-3600>：time in seconds.

Command Mode: BGP route configuration mode

Default: restart-time uses the default value of 120s.

Usage Guide: None

Example: Configure restart-time as 60s for BGP GR

Switch(config-router)# bgp graceful-restart restart-time 60

5.10.3 bgp graceful-restart stale-path-time

Command: bgp graceful-restart stale-path-time <1-3600>

no bgp graceful-restart stale-path-time <1-3600>

Function: Configure stale-path-time for BGP GR. Specify the longest waiting time that delete stale route from the received OPEN messages to the received EOR for Receiving Speaker. No command restores stale-path-time as the default value of 360 seconds.

Parameter: <1-3600>：time in seconds

Command Mode: BGP route configuration mode

Default: stale-path-time uses the default value of 360s.

Usage Guide: None.

Example: Configure stale-path-time as 460s for BGP GR.

Switch(config-router)# bgp graceful-restart stale-path-time 460

5.10.4 bgp selection-deferral-time

Command: bgp selection-deferral-time <1-3600>

no bgp selection-deferral-time <1-3600>

Function: Configure selection-deferral-time for BGP GR. Specify the longest waiting time that start to count selection route from the received OPEN messages to the received EOR for Restarting Speaker. If Restarting Speaker does not receive EOR after exceed the time, it can count selection route. No command restores selection-deferral-time as the default value of 120 seconds.

Parameter: <1-3600>：time in seconds

Command Mode: BGP route configuration mode

Default: selection-deferral-time uses the default value of 120s.

Usage Guide: None.

Example: Configure selection-deferral-time as 240s for BGP GR.

Switch(config-router)# bgp selection-deferral-time 240

5.10.5 neighbor capability graceful-restart

Command: neighbor (A.B.C.D | X:X::X:X | WORD) capability graceful-restart

no neighbor (A.B.C.D | X:X::X:X | WORD) capability graceful-restart

Function: Configure whether neighbor supports GR capability, no command does not support GR capability.

Parameter: (A.B.C.D|X:X::X:X|WORD)： name of neighbor address or neighbor group for BGP

Command Mode: BGP protocol unicast address family mode and VRF address family mode.

Default: Do not configure GR.

Usage Guide: None

Example: Configure that GR capability is sent to neighbor 1.1.1.1.

Switch(config-router)#neighbor 1.1.1.1 capability graceful-restart

5.11 OSPF GR

5.11.1 capability restart graceful

Command: capability restart graceful

no capability restart

Function: Enable GR of specified OSPF process, no command disables this function.

Parameter: None.

Command mode: OSPF protocol configuration mode

Default: Enable OSRF GR function.

Usage Guide: When a switch is using OSPF GR, it will quit GR directly if disable GR.

Example: Enable OSPF GR function.

Switch(config)#router ospf

Switch(config-router)#capability restart graceful

5.11.2 debug ospf events gr

Command: debug ospf events gr

no debug ospf events gr

Function: Enable the debugging for displaying relevant event of OSPF GR, no command disables the debugging.

Parameter: None.

Command mode: Admin mode

Default: Disable.

Usage Guide: None.

Example: Enable the debugging for displaying relevant event of OSPF GR.

Switch#debug ospf events gr

5.11.3 ospf graceful-restart grace-period

Command: ospf graceful-restart grace-period <integer>

no ospf restart grace-period

Function: Configure grace period of GR restarter, no command restores grace period to default value.

Parameter: <*integer*>: value of grace period, unit is second and ranging from 1 to 1800.

Command mode: Global configuration mode

Default: 60s.

Usage Guide: Configure grace period of GR restarter (The switch processes switchover or restart protocol). GR process should be completed during a grace period. If it does not complete GR process in time, it should quit GR forcibly and restart OSPF normally.

Example: Configure grace period of GR restarter to 100s.

Switch(config)#ospf graceful-restart grace-period 100

5.11.4 ospf graceful-restart helper max-grace-period

Command: ospf graceful-restart helper max-grace-period <*integer*>

no ospf graceful-restart helper

Function: One of GR helper policies. Configure the maximum grace period supported by helper. The no command deletes all configured helper policies.

Parameter: <*integer*>: value of grace period, unit is second and ranging from 1 to 1800.

Command mode: Global configuration mode

Default: Do not limit grace period supported by helper.

Usage Guide: If grace period set by GR restarter is bigger than max-grace period configured by helper, helper will not help restarter to complete GR. The no command deletes all helper policies.

Example: Configure the maximum grace period allowed by GR helper to 100s.

Switch(config)#ospf graceful-restart helper max-grace-period 100

5.11.5 ospf graceful-restart helper never

Command: ospf graceful-restart helper never

no ospf graceful-restart helper

Function: One of GR helper policies. Configured the switch can not work as OSPF GR helper. The no command deletes all configured helper policies.

Parameter: None.

Command mode: Global configuration mode

Default: Switch can work as GR helper.

Usage Guide: After configure the policy, switch can only work as GR restarter (a switch processes switchover and restart protocol), not GR helper (a switch helps restarter to complete GR).

Example: Configure that switch cannot work as OSPF helper.

Switch(config)#ospf graceful-restart helper never

5.11.6 show ip ospf

Command: show ip ospf [<process-id>]

Function: Show main information of OSPF, including whether it supports GR and it can works as GR helper, the configured grace period and so on.

Parameter: <*process-id*>: Process ID, ranging from 0 to 65535. It means that show main OSPF information of all processes when there is no parameter configured.

Command Mode: Admin mode

Default: None.

Usage Guide: None.

Example: Show main OSPF information of all processes.

```
Switch#show ip ospf
Routing Process "ospf 0" with ID 192.168.40.69
  Process bound to VRF default
  Process uptime is 52 minutes
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Graceful Restart
  Supports helper mode for Graceful Restart
  Grace period for Graceful Restart 100 secs
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Refresh timer 10 secs
  Number of external LSA 0. Checksum Sum 0x000000
  Number of opaque AS LSA 0. Checksum Sum 0x000000
  Number of non-default external LSA 0
  External LSA database is unlimited.
  Number of LSA originated 0
```

Number of LSA received 0
Number of areas attached to this router: 0

Display	Description
Supports Graceful Restart	Switch supports OSPF GR
Supports helper mode for Graceful Restart	Switch supports helper mode of OSPF GR
Grace period for Graceful Restart 100 secs	Switch configures OSPF GR Grace Period to 100s

5.11.7 show ip ospf graceful-restart

Command: show ip ospf [<process-id>] graceful-restart
Function: Show the state of OSPF GR, including whether it is processing GR at helper mode, GR remaining time.
Parameter: <*process-id*>: Process ID, ranging from 0 to 65535. It means that GR state of all processes shown when there is no parameter configured.
Command Mode: Admin mode
Default: None.
Usage Guide: None.
Example: Show GR state of all processes on GR restarter.
Switch#show ip ospf graceful-restart
OSPF process 0 graceful-restart information：
GR status :GR in progress
GR remaining time : 50

Display	Description
OSPF process 0 graceful-restart information	OSPF GR state in process 0.
GR status	GR state of GR, GR in progress means switch is processing GR
GR remaining time	Remaining time of GR

Show GR state of all processes on GR helper:
Switch#show ip ospf graceful-restart
OSPF process 0 graceful-restart information:
GR status :Helper

Neighbor ID	Interface	Remaining time
1.1.1.1	Vlan1	100
2.2.2.2	Vlan1	200

Display	Description

OSPF process 0 graceful-restart information	OSPF GR state of process 0.
GR status	GR state, Helper means switch is in helper mode
Neighbor ID	The router-id of restarter helped
Interface	The layer 3 interface connected with restarter
Remaining time	Remaining time of GR

Chapter 6 Commands for Multicast Protocol

6.1 Multicast

6.1.1 show ip mroute

Command: show ip mroute [<GroupAddr> [<SourceAddr>]]

Function: show IPv4 software multicast route table.

Parameter: GroupAddr: show the multicast entries relative to this Group address.

SourceAddr: show the multicast route entries relative to this source address.

Default: None

Command Mode: Admin mode and global mode

Usage Guide:

Example: show all entries of multicast route table.

Switch(config)#show ip mroute

Name: Loopback, Index: 2002, State:49

Name: null0, Index: 2003, State:49

Name: sit0, Index: 2004, State:80

Name: Vlan1, Index: 2005, State:1043

Name: Vlan2, Index: 2006, State:1002

Name: pimreg, Index: 2007, State:c1

The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0

Group	Origin	Iif	Wrong	Oif:TTL
225.1.1.1	192.168.1.136	vlan1	0	2006:1

Displayed information	Explanation
Name	the name of interface
Index	the index number of interface
State	the state of interface
The total matched ipmr active mfc entries	The total matched active IP multicast route mfc （multicast forwarding cache） entries
unresolved ipmr entries	unresolved ip multicast route entries
Group	the destination address of the entries
Origin	the source address of the entries
Iif	ingress interface of the entries
Wrong	packets received from the wrong interface
Oif	egress interface of the entries
TTL	the value of TTL

6.2 PIM-DM

6.2.1 debug pim timer sat

Command: debug pim timer sat

no debug pim timer sat

Function: Enable debug switch of PIM-DM source activity timer information in detail; the "**no debug pim timer sat**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example:

Switch # debug ip pim timer sat

Remark: Other debug switches in PIM-DM are common in PIM-SM, including debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim timer, debug pim state, refer to PIM-SM handbook.

6.2.2 debug pim timer srt

Command: debug pim timer srt

no debug pim timer srt

Function: Enable debug switch of PIM-DM state-refresh timer information in detail; the "**no debug pim timer srt**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: Enable the switch, and display PIM-DM state-refresh timer information in detail.

Example: Switch #debug ip pim timer srt

Remark: Other debug switches in PIM-DM are common in PIM-SM, including debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim timer, debug pim state, refer to PIM-SM manual section.

6.2.3 ip mroute

Command: ip mroute <*A.B.C.D*> <*A.B.C.D*> <*ifname*> <*.ifname*>

no ip mroute <*A.B.C.D*> <*A.B.C.D*> [<*ifname*> <*.ifname*>]

Function: To configure static multicast entry. The no command will delete some static multicast entries or some egress interfaces.

Parameter: ***<A.B.C.D> <A.B.C.D>*** are the source address and group address of multicast.

<ifname> <.ifname>, the first one is ingress interface, follow is egress interface.

Default: To delete this static multicast entry, if the command isn't included interface parameter.

Command Mode: Global Mode.

Usage Guide: The ***<ifname>*** should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.

Example:

Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

6.2.4 ip pim bsr-border

Command: ip pim bsr-border

no ip pim bsr-border

Function: To configure or delete PIM BSR-BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

Switch(Config-if-Vlan1)#no ip pim bsr-border

6.2.5 ip pim dense-mode

Command: ip pim dense-mode

no ip pim dense-mode

Function: Enable PIM-DM protocol on interface; the "**no ip pim dense-mode**" command disenables PIM-DM protocol on interface.

Parameter: None.

Default: Disable PIM-DM protocol.

Command Mode: Interface Configure Mode

Usage Guide: The command will be taken effect, executing ip multicast-routing in Global Mode. Don't support multicast protocol mutual operation, namely can't synchronously enable dense mode and sparse mode in one swtich.

Example: Enable PIM-DM protocol on interface vlan1.

Switch (config)#ip pim multicast-routing

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip pim dense-mode

6.2.6 ip pim dr-priority

Command: ip pim dr-priority <*priority*>

no ip pim dr-priority

Function: Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ip pim dr-priority"** command restores the default value.

Parameter: <*priority*> is priority

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority.

Example: Configure VLAN's DR priority to 100

Switch (config)# interface vlan 1

Switch(Config-if-Vlan1)ip pim dr-priority 100

Switch (Config -if-Vlan1)#

6.2.7 ip pim exclude-genid

Command: ip pim exclude-genid

no ip pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option. The "**no ipv6 pim exclude-genid**" command restores the default value

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the Hello packets sent by the switch do not include GenId option.

Switch (Config-if-Vlan1)#ip pim exclude-genid

Switch (Config-if-Vlan1)#

6.2.8 ip pim hello-holdtime

Command: ip pim hello-holdtime <*value*>

no ip pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbore holdtime, if the switch hasn't received the neighbore hello packets when the holdtime is over, this neighbore is deleted. The "**no ip pim hello-holdtime**" command cancels configured holdtime value and restores default value.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s, so Holdtime's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval, this configuration is denyed. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If

hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval, hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.

Example: Configure vlan1's Hello Holdtime

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ip pim hello-holdtime 10

Switch (Config -if-Vlan1)#

6.2.9 ip pim hello-interval

Command: ip pim hello-interval < *interval*>

no ip pim hello-interval

Function: Configure interface PIM-DM hello message interval; the "**no ip pim hello-interval**" restores default value.

Parameter: < *interval*> is interval of periodically transmitted PIM-DM hello message, value range from 1s to 18724s.

Default: Default interval of periodically transmitted PIM-DM hello message as 30s.

Command Mode: Interface Configuration Mode.

Usage Guide: Hello message makes PIM-DM switch mutual location, and ensures neighborship. PIM-DM switch announces existence itself by periodically transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime.

Example: Configure PIM-DM hello interval on interface vlan1.

Switch (config)#interface vlan1

Switch(Config-if-Vlan1)#ip pim hello-interval 20

6.2.10 ip pim multicast-routing

Command: ip pim multicast-routing

no ip pim multicast-routing

Function: Enable PIM-SM globally. The "**no ip pim multicast-routing**" command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM

Command Mode: Global Mode

Usage Guide: Enable PIM-SM globally. The interface must enable PIM-SM to have PIM-SM work

Example: Enable PIM-SM globally.

Switch (config)#ip pim multicast-routing

6.2.11 ip pim neighbor-filter

Command: ip pim neighbor-filter <*list-number*>

no ip pim neighbor-filter <*list-number*>

Function: Configure the neighbore access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this conncetion can't be created.

Parameter: <*list-number*>: <*list-number*> is the simple access-list number, it ranges from 1 to 99

Default: No neighbor filter configuration.

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1,access-list 1's default is deny. In the following example, if "permit any-source" is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any-source.

Example: Configure VLAN's filtering rules of pim neighbors.

```
Switch #show ip pim neighbor
Neighbor          Interface          Uptime/Expires      Ver   DR
Address                                                        Priority/Mode
10.1.4.10         Vlan1              02:30:30/00:01:41 v2     4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any-source
Switch (config)#show ip pim neighbor
Switch (config)#
```

6.2.12 ip pim scope-border

Command: ip pim scope-border [<*1-99* >|<*acl_name*>]

no ip pim scope-border

Function: To configure or delete management border of PIM.

Parameters: <*1-99* >: is the ACL number for the management border.

<*acl_name*>: is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

```
Switch(Config-if-Vlan2)#ip pim scope-border 3
```

6.2.13 ip pim state-refresh origination-interval

Command: ip pim state-refresh origination-interval *<interval>*

no ip pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message. The "**no ip pim state-refresh origination-interval**" command restores default value.

Parameter: <*interval*> packet transmission interval value is from 4s to 100s.

Default: 60s

Command Mode: Global Mode

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list items of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval.

Example: Configure transmission interval of state-refresh message to 90s.

Switch (config)#ip pim state-refresh origination-interval 90

6.2.14 show ip pim interface

Command: show ip pim interface

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display PIM interface information

Example: Switch(config)#show ip pim interface

Address	Interface	VIFindex	Ver/ Mode	Nbr Count	DR Prior	DR
10.1.4.3	Vlan1	0	v2/S	1	1	10.1.4.3
10.1.7.1	Vlan2	2	v2/S	0	1	10.1.7.1

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

6.2.15 show ip pim mroute dense-mode

Command: show ip pim mroute dense-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]

Function: Display PIM-DM message forwarding items.

Parameter: group <A.B.C.D>: displays forwarding items relevant to this multicast address.

source <A.B.C.D>: displays forwarding items relevant to this source.

Default: Do not display (Off).

Command Mode: Admin Mode

Usage Guide: The command shows PIM-DM multicast forwarding items, namely forwarding items of forward multicast packet in system FIB table.

Example: Display all of PIM-DM message forwarding items.

Switch(config)#show ip pim mroute dense-mode

IP Multicast Routing Table

(*,G) Entries: 1
(S,G) Entries: 1

(*, 226.0.0.1)
  Local   ..l.....

(192.168.1.12, 226.0.0.1)
RPF nbr: 0.0.0.0
RPF idx: Vlan2
Upstream State: FORWARDING
Origin State: ORIGINATOR
  Local   .....
  Pruned   .....
  Asserted   .....
  Outgoing   ..o.....

Switch#

Displayed Information	Explanations
(*,226.0.0.1)	(*,G) Forwaridng item
(192.168.1.12, 226.0.0.1)	(S,G) Forwarding item
RPF nbr	Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop.
RPF idx	Interface located in RPF neighbor
Upstream State	Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream response, forwarding upstream data)
Origin State	The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)
Local	Local position joins interface, the interface receives IGMP Join
Pruned	PIM prunes interface, the interface receives Prune messages
Asserted	Asserted state
Outgoing	Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

6.2.16 show ip pim neighbor

Command: show ip pim neighbor

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example: Switch (config)#show ip pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.1.6.1	Vlan1	00:00:10/00:01:35	v2	1 /
10.1.6.2	Vlan1	00:00:13/00:01:32	v2	1 /
10.1.4.2	Vlan3	00:00:18/00:01:30	v2	1 /
10.1.4.3	Vlan3	00:00:17/00:01:29	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.

6.2.17 show ip pim nexthop

Command: show ip pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

Switch(config)#show ip pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable

Destination	Type	Nexthop Num	Nexthop Addr	Nexthop Ifindex	Nexthop Name	Metric	Pref	Refcnt
192.168.1.1	N...	1	0.0.0.0	2006		0	0	1
192.168.1.9	..S.	1	0.0.0.0	2006		0	0	1

Displayed Information	Explanations
Destination	Destination of next item

Type	N: created nexthop, RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

6.3 PIM-SM

6.3.1 clear ip pim bsr rp-set

Command: clear ip pim bsr rp-set *

Function: Clear all RP.

Parameters: None.

Command Mode: Admin Configuration Mode

Usage Guide: Clear all RP rapidly.

Example: Clear all RP.

Switch# clear ip pim bsr rp-set *

Relative Command: show ip pim bsr-router

6.3.2 debug pim event

Command: debug pim event

no debug pim event

Function: Enable or Disable pim event debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable pim event debug switch and display events information about pim operation.

Example:

Switch# debug ip pim event

Switch#

6.3.3 debug pim mfc

Command: debug pim mfc

no debug pim mfc

Function: Enable or Disable pim mfc debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable pim mfc debug switch and display generated and transmitted multicast id's information.

Example: Switch# debug ip pim mfc

6.3.4 debug pim mib

Command: debug pim mib

no debug pim mib

Function: Enable or Disable PIM MIB debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM MIB information by PIM MIB debug switch. It's not available now and it's for the future extension.

Example: Switch# debug ip pim mib

6.3.5 debug pim nexthop

Command: debug pim nexthop

no debug pim nexthop

Function: Enable or Disable pim nexthop debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM NEXTHOP changing information by the pim nexthop switch.

Example: Switch# debug ip pim nexthop

6.3.6 debug pim nsm

Command: debug pim nsm

no debug pim nsm

Function: Enable or Disable pim debug switch communicating with Network Services

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the communicating information between PIM and Network Services by this switch.

Example: Switch# debug ip pim nsm

6.3.7 debug pim packet

Command: debug pim packet
debug pim packet in
debug pim packet out
no debug pim packet
no debug pim packet in
no debug pim packet out
Function: Enable or Disable pim debug switch
Parameter: in display only received pim packets
out display only transmitted pim packets
none display both
Default: Disabled
Command Mode: Admin Mode.
Usage Guide: Inspect the received and transmitted pim packets by this switch.
Example: Switch# debug ip pim packet in

6.3.8 debug pim state

Command: debug pim state
no debug pim state
Function: Enable or Disable pim debug switch
Parameter: None
Default: Disabled
Command Mode: Admin Mode.
Usage Guide: Inspect the changing information about pim state by this switch.
Example: Switch# debug ip pim state

6.3.9 debug pim timer

Command: debug pim timer
debug pim timer assert
debug pim timer assert at
debug pim timer bsr bst
debug pim timer bsr crp
debug pim timer bsr
debug pim timer hello ht
debug pim timer hello nlt
debug pim timer hello tht
debug pim timer hello
debug pim timer joinprune et

debug pim timer joinprune jt
debug pim timer joinprune kat
debug pim timer joinprune ot
debug pim timer joinprune plt
debug pim timer joinprune ppt
debug pim timer joinprune pt
debug pim timer joinprune
debug pim timer register rst
debug pim timer register
no debug pim timer
no debug pim timer assert
no debug pim timer assert at
no debug pim timer bsr bst
no debug pim timer bsr crp
no debug pim timer bsr
no debug pim timer hello ht
no debug pim timer hello nlt
no debug pim timer hello tht
no debug pim timer hello
no debug pim timer joinprune et
no debug pim timer joinprune jt
no debug pim timer joinprune kat
no debug pim timer joinprune ot
no debug pim timer joinprune plt
no debug pim timer joinprune ppt
no debug pim timer joinprune pt
no debug pim timer joinprune
no debug pim timer register rst
no debug pim timer register

Function: Enable or Disable each pim timer

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable the specified timer's debug information.

Example:

Switch# debug pim timer assert
Switch#

6.3.10 ip mroute

Command: ip mroute <*A.B.C.D*> <*A.B.C.D*> <*ifname*> <.*ifname*>

no ip mroute <*A.B.C.D*> <*A.B.C.D*> [<*ifname*> <.*ifname*>]

Function: To configure static multicast entry. The no command will delete some static multicast

entries or some egress interfaces.

Parameter: ***<A.B.C.D> <A.B.C.D>*** are the source address and group address of multicast.

<ifname> <.ifname>, the first one is ingress interface, follow is egress interface.

Default: To delete this static multicast entry, if the command isn't included interface parameter.

Command Mode: Global Mode.

Usage Guide: The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.

Example:

Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

6.3.11 ip multicast unresolved-cache aging-time

Command: ip multicast unresolved-cache aging-time <value>

no ip multicast unresolved-cache aging-time

Function: Configure the cache time of the kernel multicast route, the no command restores the default value.

Parameter: < value> is the configured cache time, ranging between 1 and 20s.

Default: 10s.

Command Mode: Global Configuration Mode.

Usage Guide: Configure the cache time of multicast route entry in kernel.

Example:

Switch(config)# ip multicast unresolved-cache aging-time 18

6.3.12 ip pim accept-register

Command: ip pim accept-register list <*list-number*>

no ip pim accept-register

Function: Filter the specified multicast group and multicast address.

Parameter: <***list-number***>: **<*list-number*>** is the access-list number, it ranges is 1-99 or 100-199, where 1-99 is the standard access list number and 100-199 is the extended access list number.

Default: Permit the multicast registers from any sources to any groups.

Command Mode: Global Mode

Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets.The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY, PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets. Unlike other access-list, when the access-list is configured, the default value is PERMIT.

Example: Configure the filtered register message's rule to myfilter.

Switch(config)#ip pim accept-register list 120

Switch (config)#access-list 120 deny ip 10.1.0.2 0.0.0.255 239.192.1.10 0.0.0.255
Switch (config)#

6.3.13 ip pim bsr-border

Command: ip pim bsr-border

no ip pim bsr-border

Function: To configure or delete PIM BSR-BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

Switch(Config-if-Vlan1)#no ip pim bsr-border

6.3.14 ip pim bsr-candidate

Command: ip pim bsr-candidate {vlan <*vlan-id*>| <*ifname*>} [*hash-mask-length*] [*priority*]

no ip pim bsr-candidate

Function: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete with other candidate BSRs for the BSR router. The command **"no ip pim bsr-candidate"** disables the candidate BSR.

Parameter: ***Ifname*** is the specified interface's name;

[*hash-mask-length*] is the specified hash mask length. It's used for the RP enable selection and ranges from 0 to 32;

[*priority*] is the candidate BSR priority and ranges from 0 to 255. If this parameter is not configured, the default priority value is 0.

Default: This switch is not a candidate BSR router.

Command Mode: Global Mode

Usage Guide: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete with other candidate BSRs for the BSR router. Only this command is configured, this switch is the BSR candidate router.

Example: Globally configure the interface vlan1 as the candidate BSR-message transmitting interface.

Switch (config)# ip pim bsr-candidate vlan1 30 10

6.3.15 ip pim cisco-register-checksum

Command: ip pim cisco-register-checksum [group-list <*simple-acl*>]

no ip pim cisco-register-checksum [group-list <*simple-acl*>]

Function: Configure the register packet's checksum of the group specified by myfilter to use the

whole packet's length.
Default: Compute the checksum according to the register packet's head length, default: 8
Parameter: <*simple-acl*>: <1-99> Simple access-list **<*simple-acl*>:** <1-99> Simple access-list
Command Mode: Global Mode
Usage Guide: This command is used to interact with older Cisco IOS version.
Example: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.
Switch (config)#ip pim cisco-register-checksum group-list 23

6.3.16 ip pim dr-priority

Command: ip pim dr-priority <*priority*>
no ip pim dr-priority
Function: Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ip pim dr-priority**" command restores the default value.
Parameter: *<priority>* is priority
Default: 1
Command Mode: Interface Configuration Mode
Usage Guide: Range from 0 to 4294967294, the higher value has more priority.
Example: Configure VLAN's DR priority to 100
Switch (config)# interface vlan 1
Switch(Config-if-Vlan1)ip pim dr-priority 100
Switch (Config -if-Vlan1)#

6.3.17 ip pim exclude-genid

Command: ip pim exclude-genid
no ip pim exclude-genid
Function: This command makes the Hello packets sent by PIM SM do not include GenId option. The "**no ipv6 pim exclude-genid**" command restores the default value
Parameter: None
Default: The Hello packets include GenId option.
Command Mode: Interface Configuration Mode
Usage Guide: This command is used to interact with older Cisco IOS version.
Example: Configure the Hello packets sent by the switch do not include GenId option.
Switch (Config-if-Vlan1)#ip pim exclude-genid
Switch (Config-if-Vlan1)#

6.3.18 ip pim hello-holdtime

Command: ip pim hello-holdtime <*value*>
no ip pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbor holdtime,if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor is deleted. The "**no ip pim hello-holdtime**" command cancels configured holdtime value and restores default value.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s, so Hold time's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval, this configuration is denied. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval, hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.

Example: Configure vlan1's Hello Holdtime

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ip pim hello-holdtime 10

Switch (Config -if-Vlan1)#

6.3.19 ip pim hello-interval

Command: ip pim hello-interval <*interval*>

no ip pim hello-interval

Function: Configure the interface's hello_interval of pim hello packets. The "**no ip pim hello-interval**" command restores the default value.

Parameter: <*interval*> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s.

Default: The default periodically transmitted pim hello packets' hello_interval is30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello messages make pim switches oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor overtime.

Example: Configure VLAN's pim-sm hello interval

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip pim hello-interval 20

Switch(Config-if-Vlan1)#

6.3.20 ip pim ignore-rp-set-priority

Command: ip pim ignore-rp-set-priority

no ip pim ignore-rp-set-priority

Function: When RP selection is carried out, this command configures the switch to enable

Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.

Default: Disabled

Parameter: None

Command Mode: Global Mode

Usage Guide: When selecting RP, Pim usually will select according to RP priority. When this command is configured, pim will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.

Example: Switch (config)#ip pim ignore-rp-set-priority

6.3.21 ip pim jp-timer

Command: ip pim jp-timer <*value*>

no ip pim jp-timer

Function: Configure to add JP timer. The "**no ip pim jp-timer**" command restores the default value.

Parameter: **<*value*>** ranges from 10 to 65535s

Default: 60s

Command Mode: Global Mode

Usage Guide: Configure the interval of JOIN-PRUNE packets sent by PIM periodically, the default value is 60s. The default value is recommended if no special reasons.

Example: Configure the interval of timer

Switch (config)#ip pim jp-timer 59

6.3.22 ip pim multicast-routing

Command: ip pim multicast-routing

no ip pim multicast-routing

Function: Enable PIM-SM globally. The "**no ip pim multicast-routing**" command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM

Command Mode: Global Mode

Usage Guide: Enable PIM-SM globally. The interface must enable PIM-SM to have PIM-SM work

Example: Enable PIM-SM globally.

Switch (config)#ip pim multicast-routing

Switch (config)#

6.3.23 ip pim neighbor-filter

Command: ip pim neighbor-filter <*list-number*>

no ip pim neighbor-filter <*list-number*>

Function: Configure the neighbor access-list. If filtered by the lists and connections with

neighbors are created, this connections are cut off immediately. If no connection is created, this connection can't be created.

Parameter: <*list-number*>: <*list-number*> is the simple access-list number, it ranges from 1 to 99

Default: No neighbor filter configuration.

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1, access-list 1's default is deny. In the following example, if "permit any" is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any.

Example: Configure VLAN's filtering rules of pim neighbors.

```
Switch #show ip pim neighbor
Neighbor          Interface          Uptime/Expires      Ver   DR
Address                                                        Priority/Mode
10.1.4.10         Vlan1              02:30:30/00:01:41 v2     4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any
Switch (config)#show ip pim neighbor
```

6.3.24 ip pim register-rate-limit

Command: ip pim register-rate-limit <*limit*>

no ip pim register-rate-limit

Function: This command is used to configure the speedrate of DR sending register packets; the unit is packet/second. The "**no ip pim Register-rate-limit**" command restores the default value. This configured speedrate is each（S, G）state's ,not the whole system's.

Parameter: *<limit>* ranges from 1 to 65535.

Default: No limit for sending speed

Command Mode: Global Mode

Usage Guide: This configuration is to prevent the attack to DR, limiting sending REGISTER packets.

Example: Configure the speedrate of DR sending register packets to 59p/s.

```
Switch (config)#ip pim register-rate-limit 59
Switch (config)#
```

6.3.25 ip pim register-rp-reachability

Command: ip pim register-rp-reachability

no ip pim register-rp-reachability

Function: This command makes DR check the RP reachability in the process of registration.

Parameter: None

Default: Do not check

Command Mode: Global Mode

Usage Guide: This command configures DR whether or not to check the RP reachability.

Example: Configure DR to check the RP reachability.
Switch (config)#ip pim register-rp-reachability
Switch (config)#

6.3.26 ip pim register-source

Command: ip pim register-source {<*A.B.C.D*> | <*ifname*>| vlan <*vlan-id*>}
no ip pim register-source

Function: This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is usually the RPF neighbor of source host direction.

Parameter: <*ifname*> is the interface name,
<*vlan-id*> is VLAN ID;
<*A.B.C.D*> is the configured source IP addresses.

Default: Do not check

Command Mode: Global Mode

Usage Guide: The "**no ip pim register-source**" command restores the default value, no more parameter is needed. Configured address must be reachable to Register-Stop messages sent by RP. It's usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.

Example: Configure the source address sent by DR.
Switch (config)#ip pim register-source 10.1.1.1

6.3.27 ip pim register-suppression

Command: ip pim register-suppression <*value*>
no ip pim register-suppression

Function: This command is to configure the value of register suppression timer, the unit is second. The "**no ip pim register-suppression**" command restores the default value.

Parameter: <*value*> is the timer's value; it ranges from 10 to 65535s.

Default: 60s

Command Mode: Global Mode

Usage Guide: If this value is configured at DR, it's the value of register suppression timer; the bigger one of the default register keep-alive time of RP (210s) and the sum of triple register suppression time and 5. If configure this value on RP without the command "ip pim rp-register-kat", this command may modify the RP register keep-alive time.

Example: Configure the value of register suppression timer to 10s.
Switch (config)#ip pim register- suppression 10
Switch (config)#

6.3.28 ip pim rp-address

Command: ip pim rp- address <*A.B.C.D*> <*A.B.C.D/M*>

no ip pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>|<*all*>]

Function: This command is to configure static RP globally or in a multicast address range.The **"no ipv6 pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>|<*all*>]**" command cancels static RP.

Parameter: <*A.B.C.D*> is the RP address

<*A.B.C.D/M*> the scope of the specified RP address

<*all*> is all the range

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is to configure static RP globally or in a multicast address range and configure PIM-SM static RP information. Attention, when computing rp, BSR RP is selected first. If it doesn't succeed, static RP is selected.

Example: Configure vlan1 as candidate RP announcing sending interface globally.

Switch (config)# ip pim rp-address 10.1.1.1 238.0.0.0/8

Switch (config)#

6.3.29 ip pim rp-candidate

Command: ip pim rp-candidate {vlan < *vlan-id* > | <*ifname*>} [<*A.B.C.D/M*>] [<priority>]

no ip pim rp-candiate

Function: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. The "**no ip pim rp-candiate**" command cancels the candidate RP.

Parameter: *vlan-id* isVlan ID;

ifname is the name of the specified interface;

A.B.C.D/M is the ip prefix and mask;

<priority> is the RP selection priority, it ranges from 0 to 255, the default value is 192, the lower value has more priority.

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs.Only this command is configured, this switch is the RP candidate router.

Example: Configure vlan1 as the sending interface of candidate RP announcing sending messages

Switch (config)# ip pim rp-candidate vlan1 100

6.3.30 ip pim rp-register-kat

Command: ip pim rp-register-kat <*vaule*>

no ip pim rp-register-kat

Function: This command is to configure the KAT (KeepAlive Timer) value of the RP (S, G) items, the unit is second. The "**no ip pim rp-register-kat**" command restores the default value.

Parameter: <*vaule*> is the timer value; it ranges from 1 to 65535s.

Default: 185s

Command Mode: Global Mode

Usage Guide: This command is to configure the RP's keep alive time, during the keep alive time RP's (S, G) item will not be deleted because it hasn't received REGISTER packets. If no new REGISTER packet is received when the keep alive time is over, this item will be obsolete.

Example: Configure the kat value of RP's (S, G) item to 180s

Switch (config)#ip pim rp-register- kat 180

Switch (config)#

6.3.31 ip pim scope-border

Command: ip pim scope-border [<*1-99* >|<*acl_name*>]

no ip pim scope-border

Function: To configure or delete management border of PIM.

Parameters: <*1-99* >: is the ACL number for the management border.

<*acl_name*>: is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

Switch(Config-if-Vlan2)#ip pim scope-border 3

6.3.32 ip pim sparse-mode

Command: ip pim sparse-mode [passive]

no ip pim sparse-mode [passive]

Function: Enable PIM-SM on the interface; the "**no ip pim sparse-mode [passive]**" command disables PIM-SM.

Parameter: [*passive*] means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable IGMP (reveice and transmit IGMP packets).

Default: Do not enable PIM-SM

Command Mode: Interface Configuration Mode

Usage Guide: Enable PIM-SM on the interface.

Example: Enable PIM-SM on the interface vlan1.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip pim sparse-mode

Switch(Config-if-Vlan1)#

6.3.33 show ip pim bsr-router

Command: show ip pim bsr-router

Function: Display BSR address

Parameter: None

Default: None

Command Mode: Admin Mode.

Usage Guide: Display the BSR information maintained by the PIM.

Example: show ip pim bsr-router

PIMv2 Bootstrap information

This system is the Bootstrap Router (BSR)

BSR address: 10.1.4.3 (?)

Uptime: 00:06:07, BSR Priority: 0, Hash mask length: 10

Next bootstrap message in 00:00:00

Role: Candidate BSR

State: Elected BSR

Next Cand_RP_advertisement in 00:00:58

RP: 10.1.4.3(Vlan1)

Displayed Information	Explanations
BSR address	Bsr-router Address
Priority	Bsr-router Priority
Hash mask length	Bsr-router hash mask length
State	The current state of this candidate BSR, Elected BSR is selected BSR

6.3.34 show ip pim interface

Command: show ip pim interface

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display PIM interface information

Example: testS2(config)#show ip pim interface

Address	Interface	VIFindex	Ver/ Mode	Nbr Count	DR Prior	DR
10.1.4.3	Vlan1	0	v2/S	1	1	10.1.4.3
10.1.7.1	Vlan2	2	v2/S	0	1	10.1.7.1

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority

DR	The interface's DR address

6.3.35 show ip pim mroute sparse-mode

Command: show ip pim mroute sparse-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]

Function: Display the multicast route table of PIM-SM.

Parameter: group <A.B.C.D>: Display redistributed items that related to this multicast address
source <A.B.C.D>: Display redistributed items that related to this source

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the BSP routers in the network maintained by PIM-SM.

Example: Switch #show ip pim mroute sparse-mode

IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0

(*, 239.192.1.10)
RP: 10.1.6.1
RPF nbr: 10.1.4.10
RPF idx: Vlan1
Upstream State: JOINED
Local ..l.....
Joined .....
Asserted .....
Outgoing ..o.....

Displayed Information	Explanations
Entries	The counts of each item
RP	Share tree's RP address
RPF nbr	RP direction or upneighbor of source direction.
RPF idx	RPF nbr interface
Upstream State	Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for（S,G,rpt.）
Local	Local join interface, this interface receive IGMPJoin
Joined	PIM join interface, this interface receive J/P

	messages
Asserted	Asserted state
Outgoing	Final outgoing of multicast data, in this example, the index of the outgoing interface is 2. Command “show ip pim interface” can query interface information.

6.3.36 show ip pim neighbor

Command: show ip pim neighbor

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example: Switch (config)#show ip pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.1.6.1	Vlan1	00:00:10/00:01:35	v2	1 /
10.1.6.2	Vlan1	00:00:13/00:01:32	v2	1 /
10.1.4.2	Vlan3	00:00:18/00:01:30	v2	1 /
10.1.4.3	Vlan3	00:00:17/00:01:29	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface’s DP.

6.3.37 show ip pim nexthop

Command: show ip pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

Switch(config)#show ip pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable

Destination	Type	Nexthop Num	Nexthop Addr	Nexthop Ifindex	Nexthop Name	Metric	Pref	Refcnt
192.168.1.1	N...	1	0.0.0.0	2006		0	0	1
192.168.1.9	..S.	1	0.0.0.0	2006		0	0	1

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop, RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

6.3.38 show ip pim rp-hash

Command: show ip pim rp-hash <*A.B.C.D*>

Function: Display the RP address of A.B.C.D's merge point

Parameter: Group address

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the RP address corresponding to the specified group address

Example: Switch (Config-if-Vlan1)#show ip pim rp-hash 239.192.1.10

RP: 10.1.6.1

Info source: 10.1.6.1, via bootstrap

Displayed Information	Explanations
RP	Queried group'sRP
Info source	The source of Bootstrap information

6.3.39 show ip pim rp mapping

Command: show ip pim rp mapping

Function: Display Group-to-RP Mapping and RP.

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the current RP and mapping relationship.

Example: Switch (Config-if-Vlan1)#show ip pim rp mapping

PIM Group-to-RP Mappings

Group(s): 224.0.0.0/4

RP: 10.1.6.1

Info source: 10.1.6.1, via bootstrap, priority 6

Uptime: 00:11:04

Displayed Information	Explanations
Group(s)	Group address range of RP
Info source	Source of Bootstrap messages
Priority	Priority of Bootstrap messages

6.4 MSDP

6.4.1 cache-sa-holdtime

Command: cache-sa-holdtime <*150-3600*>

no cache-sa-holdtime

Function: To configure the longest holdtime of SA table within MSDP Cache.

Parameter: *seconds*: the units are seconds, range between 150 to 3600.

Command Mode: MSDP Configuration Mode.

Default: 150 seconds by default.

Usage Guide: To configure the aging time of (S, G) table for MSDP cache as requirement.

Example:

Switch(config)#router msdp

Switch(router-msdp)#cache-sa-holdtime 350

6.4.2 cache-sa-maximum

Command: cache-sa-maximum <*sa-limit*>

no cache-sa-maximum

Function: To configure the maximum sa-limit of MSDP Peer cache specified.

Parameter: <*sa-limit*>: The maximum cache SA number， range between 1 to 75000.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: The maximum of cache SA number is 20000 by default.

Usage Guide: This command can be used to configure the maximum number of cached SA messages on the router in order to prevent the DoS – Deny of Service attack. The maximum number of cached SA messages can be configured in global configuration mode or in the MSDP Peer configuration mode. If the configured value is less than the current number of cached SA messages, or the number configured in global mode is less than that configured in peer mode, the configuration will not function.

Example:
Switch(config)#router msdp
Switch(router-msdp)#cache-sa-maximum50000
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# cache-sa-maximum 22000

6.4.3 cache-sa-state

Command: cache-sa-state
no cache-sa-state
Function: To configure the SA cache state of route.
Parameter: None.
Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.
Default: Enabled.
Usage Guide: To configure the SA cache state. If configured, the new groups will be able to get information about all the active sources from the SA cache and join the related source tree without having to wait for new SA messages. SA-cache should be enabled on all the MSDP speakers. The no form of this command will remove the configuration of SA cache. To be mentioned, this command should be issued exclusively with the sa-request command.
Example:
Switch(config)#router msdp
Switch(router-msdp)#no cache-sa-state

6.4.4 clear msdp peer

Command: clear msdp peer {*peer-address| **}
Function: Disconnected between specified MSDP Peer and TCP, to clear the statistics of the Peer.
Parameter: *peer-address*: The IP address of the Peer;
***:** Disconnected with all the Peers.
Command Mode: Admin Mode.
Default: None.
Usage Guide: If this command is issued with peer-address, the TCP connection to the specified MSDP Peer will be removed. And all the statistics about the peer will be cleared. If no peer-address is appended, all the MSDP connections as long as relative statistics about peers will be removed.
Example:
Switch#clear msdp peer *

6.4.5 clear msdp sa-cache

Command: clear msdp sa-cache {group A.B.C.D|* }
Function: To clear the Source Active information in MSDP cache: the correspond data with all the sources from specified group, or the correspond data with one specified (S, G) item.

Parameter: ***group-address :***The IP address of multicast group, to clear group (S, G) in the Cache.

***:** To clear all the items in the cache.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If group is specified, the non-local SA entries of the MSDP cache of the specified group. If no parameters are appended, all the non-local SA entries in the MSDP cache will be removed.

Example:

Switch#clear msdp sa-cache group 224.1.1.1

6.4.6 clear msdp statistics

Command: clear msdp statistics {*peer-address| **}

Function: To clear MSDP statistic information, and not reset the session of MSDP Peer.

Parameter: ***peer-address*:** The IP address of Peer.

***** Disconnection with all the Peers.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch#clear msdp statistics *

6.4.7 connect-source

Command: connect-source <*interface-type <interface-number>*

no connect-source <*interface-type> <interface-number>*

Function: To configure the interface address, which used for all the MSDP Peers to set up correspond connection between MSDP Peer and MSDP.

Parameter: <*interface-type> <interface-number>*: Interface type and interface number.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: There is no specified interface by default.

Usage Guide: The router use the IP address of this port to set up MSDP Peer connection with MSDP Peer. Pay attention: specified connect-source address must consitant with the configuration of Peer address, otherwise can not set up TCP connection. The configuration under MSDP Peer mode will cover with MSDP Mode. No command will cancel the configuration and set again all the MSDP connection of this port.

Example:

Switch(config)#router msdp

Switch(router-msdp)#connect-source vlan 2

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#connect-source loopback 10

6.4.8 debug msdp all

Command: debug msdp all

no debug msdp all

Function: To enable all the debugging information about MSDP; the no command disable all the debugging information.

Command Mode: Admin Configuration Mode.

Default: Disabled.

Usage Guide: Enable the debugging switch of MSDP, display the protocol packet send/receive information of MSDP Peer---packet, keepalive packet send/receive information---keepalive, event information---event, NSM mutual information---nsm, timer information---timer, protocol state information---fsm, filter policy information---filter.

Exampe:

Switch#debug msdp all

6.4.9 debug msdp events

Command: debug msdp events

no debug msdp events

Function: Enable /disable the switch of **msdp events debug**.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The event of running MSDP protocol can be monitored after enable this switch.

Example:

Switch#debug msdp events

6.4.10 debug msdp filter

Command: debug msdp filter

no debug msdp filter

Function: Enable/disable debug switch of MSDP filter policy information.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The filter information of MSDP receiving/sending message can be monitored after enable this switch.

Example:

Switch#debug msdp filter

6.4.11 debug msdp fsm

Command: debug msdp fsm

no debug msdp fsm

Function: Enable/disable debug switch of MSDP fsm.

Parameter: None.
Default: Close the switch.
Command Mode: Admin Mode.
Usage Guide: Enable this switch, the fsm information of MSDP Peer will be displayed.
Example:
Switch#debug msdp fsm

6.4.12 debug msdp keepalive

Command: debug msdp keepalive
no debug msdp keepalive
Function: Enable/disable the debug switch of keepalive message information for MSDP protocol.
Parameter: None.
Default: close the switch.
Command Mode: Admin Mode.
Usage Guide: The information of receiving/sending keepalive message for MSDP protocol can be monitored after enables this switch.
Example:
Switch#debug msdp keepalive

6.4.13 debug msdp nsm

Command: debug msdp nsm
no debug msdp nsm
Function: Enable/disable the switch of **msdp nsm debug**.
Parameter: None.
Default: Close the switch.
Command Mode: Admin Mode.
Usage Guide: The alternation information between running MSDP protocol and NSM module can be monitored after enable this switch.
Example:
Switch#debug msdp nsm

6.4.14 debug msdp packet

Command: debug msdp packet {send | receive}
no debug msdp packet {send | receive}
Function: Enable/disable the debug switch of sending/receiving message for the MSDP protocol.
Parameter: None.
Default: Close the switch.
Command Mode: Admin Mode.
Usage Guide: The receiving/sending messages of MSDP protocol can be monitored after enable this switch.

Example:
Switch#debug msdp packet send

6.4.15 debug msdp peer

Command: debug msdp peer A.B.C.D
no debug msdp peer
Function: Enable/disable all the debug information switch of specified MSDP Peer.
Parameter: None.
Default: Close the switch.
Command Mode: Admin Mode.
Usage Guide: Enable all the debug information of specified MSDP Peer as requirement, the debug information of other MSDP Peers will not be displayed. This command is take effect only for the specified last one MSDP peer.
Example:
Switch#debug msdp peer 10.1.1.1

6.4.16 debug msdp timer

Command: debug msdp timer
no debug msdp timer
Function: Enable/disable the debug switch of MSDP timer.
Parameter: None.
Default: Close the switch.
Command Mode: Admin Mode.
Usage guide: Enable dubug information for the specified timer as requirement.
Example:
Switch#debug msdp timer

6.4.17 default-rpf-peer

Command: default-rpf-peer <peer-address> [rp-policy <acl-list-number>|<word>]
no default-rpf-peer
Function: To configure static RPF peer.
Parameter: <peer-address>: the IP address of the MSDP peer.
<acl-list-number>: the ACL number, only support standard ACL from 1 to 99.
<word>: the standard ACL name.
Command Mode: MSDP Configuration Mode.
Default: There is no static RPF peer by default. If the peer command only configures one MSDP peer, this peer will be treated as the default peer.
Usage Guide: To configure more than one static RPF peers, make sure to use the following two configuration methods:

Both use the rp-policy parameter: multiple RPFs take effect at the same time, and filter RP in SA messages according to the configured prefix list, and only accept SA messages allowed to pass.
Neither uses the rp-policy parameter: according to the sequence of configuration, only the first static RPF peer in the state of UP is active. All SA messages from this peer can be received while those from other peers will be dropped. If the active peer loses effect (such as the configuration is canceled or the connection is disconnected), still choose the first static RPF peer in the state of UP in the configuration sequence to be the active static RPF peer.

Example:

Switch(config)#router msdp
Switch(router-msdp)#default-rpf-peer 10.0.0.1 rp-policy 10

6.4.18 description

Command: description <*text*>
no description

Function: Add description information of specified MSDP Peer.

Parameter: *text*: Description text, range between 1 to 80 bytes.

Command Mode: MSDP Peer Configuration Mode.

Default: There is no specified by default.

Usage Guide: To add description for the specified MSDP Peer in order to identify the different MSDP configuration. The no form of this command will remove the description.

Example:

Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# description test-20

6.4.19 exit-peer-mode

Command: exit-peer-mode

Function: Quit MSDP Peer configuration mode, and enter MSDP configuration mode.

Command Mode: MSDP Peer Configuration Mode.

Default: None.

Usage Guide: MSDP configuration mode can be returned to with the exit-peer-mode command, when configuration to an MSDP Peer is done.

Example: Back to MSDP configuration mode from MSDP Peer configuration mode.

Switch(config-msdp-peer)# exit-peer-mode

6.4.20 mesh-group

Command: mesh-group <*name*>
no mesh-group <*name*>

Function: To configure MSDP Peer as specified mesh group number, if set the same MSDP Peer to many mesh groups, then the last mesh group is available.
Parameter: name: Mesh-group name.
Command Mode: MSDP Peer Configuration Mode.
Default: MSDP Peer doesn't belong to any mesh group by default.
Usage Guide: Mesh group can reduce SA message flooding and predigest Peer-RPF checking.
Example:
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# mesh-group test-1

6.4.21 originating-rp

Command: originating-rp <*interface-type*> <*interface-number*>
no originating-rp
Function: Configure Originating RP address that to configure the IP address of the specified interface as the IP address of the RP in the SA messages.
Parameter: <*interface-type*> < *interface-number*>: type and number of the port.
Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.
Default: The default RP address of SA message is the RP address of PIM configured.
Usage Guide: To configure the IP address of the specified interface as the IP address of the RP in the SA messages. If no IP address is configured for the specified interface, or the interface is down, no SA messages will be advertised. In this occasion, if multiple RP is configured for the device, other SA messages for other RP will not be advertised either. Hence, it is required that the interface should be working when being configured.
Example:
Switch(config)#router msdp
Switch(router-msdp)#originating-rp vlan 20

6.4.22 peer

Command: peer <*A.B.C.D*>
no peer <*A.B.C.D*>
Function: To configure MSDP Peer, enter MSDP Peer mode; the no form command delete the configured MSDP Peer.
Command Mode: MSDP Configuration Mode.
Default: There is no MSDP Peer configured by default.
Usage Guide: To configure the IP address of the MSDP Peer, and enter the peer configuration mode. When the command is issued, the router will setup the TCP session to the specified peer. The no form of this command will remove the configured MSDP Peer, and destroy all the sessions and related statistics with the specified peer. Pay attention: specified Peer address must be corresponded with the interface address. If configure the Connect-source, the Peer address must be Connect-source interface address; if not specified Connect-source, the Peer address is the

egress address, otherwise cannot set up TCP connection.

Example: To configure MSDP Peer in MSDP congfiguration mode.

Switch(config-msdp)#peer 10.1.1.1

Switch(config-msdp-peer)#

6.4.23 redistribute

Command: redistribute [list <*acl-list-number | acl-name*>]

no redistribute

Function: To configure the redistribute of SA messages.

Parameter: *acl-number*: specified advanced ACL number (100-199).

acl-name: specified ACL name.

Command Mode: MSDP Configuration Mode.

Default: When set up SA message, announce all the source within fired, but not confine the (S, G) item.

Usage Guide: If ACL list number is specified, only the (S, G) entries which have passed the ACL check will be advertised in the SA messages. If no ACL is specified, no (S, G) entry will be advertised in the SA messages.

Example:

Switch(config)#router msdp

Switch(router-msdp)#redistribute list 130

6.4.24 remote-as

Command: remote-as <*as-num*>

no remote-as <*as-num*>

Function: To configure AS number of specified MSDP Peer.

Parameter: *as –num*: AS number, range from 1 to 65535.

Command Mode: MSDP Peer Configuration Mode.

Default: The AS number isn't initialized to 0 by default.

Usage Guide: This command set the AS number for specified Peer. The no command restores the AS number of specified MSDP Peer.

Example:

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)# remote-as 20

6.4.25 router msdp

Command: router msdp

no router msdp

Function: Enable the MSDP protocol of the switch, enter MSDP mode; the no form command disable MSDP protocol.

Command Mode: Global Mode.
Default: Disabled.
Usage Guide: Enable MSDP on global mode, but even configured PIM SM at the same time, then the MSDP can be work.
Example: Enable MSDP on global mode.
Switch(config)#router msdp

6.4.26 sa-filter

Command: sa-filter {in | out} [list <*acl-number* / *acl-name*> / rp-list <*rp-acl-number* / *rp-acl-name*>]

no sa-filter {in | out} [list <*acl-number*/ *acl-name*> / rp-list <*rp-acl-number* / *rp-acl-name*>]

Function: To configure the filter policy of receiving or transmitting messages, which can be used to controls the receiving and transmitting source message.
Parameter: in: To filter the SA messages from specified MSDP Peer.

out: To filter the SA messages transmitted from specified MSDP Peer.

***acl-number*:** Specified advanced ACL number (100-199).

***acl-name*:** Specified advanced ACL name.

***rp-acl-number*:** Specified standard ACL number (1-99).

rp-*acl-name*: Specified standard ACL name.

If the parameter isn't specified, the entire SA messages which include (S, G) item will be filtered.
Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.
Default: All the SA messages receiving or transmitting will not be filtered.
Usage Guide: Configuration in the peer mode will override that in the MSDP configuration mode. The distribution of SA messages can be controlled through this command or the redistribute command.
Example:
Switch(config)#router msdp
Switch(router-msdp)#sa-filter in
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# sa-filter in list 120

6.4.27 sa-request

Command: sa-request

no sa-request

Function: To configure the route sending SA request message to specified MSDP Peer when received the joined message from a new group.
Parameter: None.
Command Mode: MSDP Peer Configuration Mode.

Default: Not sending SA Request message by default.

Usage Guide: This command makes the switch (RP) send SA request messages to the specified MSDP. When there is a new group or member, the switch (RP) will send SA request messages to the specified MSDP and wait for the latter's response of its cached local SA messages. After sending a SA message to the specified MSDP, RP will receive a SA_response message from the peer, and know all active sources of the peer (not including the source information learnt via MSDP SA). If RP is configured with SA cache state, this configuration won't take effect. This command is mutually exclusive to sa-cache-sate. If the MSDP is configured with SA cache state, it won't be able to configure sa-request. The switch will show a prompt to notice the users. Please notice this command only applies to RP.

Example:

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)# sa-request

6.4.28 sa-request-filter

Command: sa-request-filter [list <*access-list-number* | *access-list-name*>]

no sa-request-filter [list <*access-list-number* | *access-list-name*>]

Function: All the SA request messages from MSDP Peer will be filtered.

Parameter: *access-list-number*: The ACL number, it only supported standard ACL from 1 to 99.

***access-list-name*:** ACL name.

Command Mode: MSDP Configuration Mode.

Default: The route receives all the SA request messages from MSDP Peer.

Usage Guide: If no list parameter is specified, all the SA request messages from MSDP Peers will be filtered. If specified, SA request messages will be filtered with the specified ACL list.

Example:

Switch(config)#router msdp

Switch(router-msdp)# sa-request-filter list 1

6.4.29 show msdp global

Command: show msdp global

Function: Show the configuration information in MSDP Mode.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the configuration information in MSDP mode; include the state of MSDP protocol, Cache and so on.

Example:

Switch#show msdp global

Multicast Source Discovery Protocol (MSDP):

SA-Cached, Originator: Vlan2, Connect-Source: Vlan2

MAX External SA Entry: 200000

MAX Peer External SA Entry: 20000
TTL Threshold: 0
SA Entry Hold Time: 350
Filters:
Redistribute_filter: Not set
SA-filter:
[IN]: RP-list: None, SG-list: None
[OUT]: Not Configured
SA-Request-Filter: Not Configured
Default Peer:
Not Configured
Mesh Group:
test-1
The introduction of showed items:

Field	Explaination
SA-Cached	MSDP SA-Cached state.
Originator	The RP interface of MSDP originated.
MAX External SA Entry	The max entries configured in MSDP configuration mode.
MAX Peer External SA Entry	The max entries of each Peer.
TTL Threshold	TTL Threshold.
SA Entry Hold Time	The multicast source hold time of MSDP cache.
Redistribute_filter	To establish the filter policy of SA message.
SA-filter [IN | OUT]	The filter policy of receiving or sending SA message.
Default Peer	Static RPF Peer.
Mesh Group	The name and members of mesh group.

6.4.30 show msdp local-sa-cache

Command: show msdp local-sa-cache
Function: Display the information for local-sa-cache.
Parameter: None.
Command Mode: Admin Mode and Configuration Mode.
Usage Guide: Display the information for local-sa-cache.
Example:
Switch#show msdp local-sa-cache
MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.

Cache SA Entry:

Source Address	Group Address	RP Address	TTL
5.5.5.9	225.0.0.1	11.1.1.1	64
5.5.5.9	225.0.0.2	11.1.1.1	64
5.5.5.9	225.0.0.3	11.1.1.1	64
5.5.5.9	225.0.0.4	11.1.1.1	64

6.4.31 show msdp peer

Command: show msdp peer {A.B.C.D}

Function: Show the configuration information in MSDP Mode.

Parameter: A.B.C.D: MSDP Peer Address.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the configuration information in MSDP configuration mode.

Example:

Switch#show msdp peer 31.1.1.3

MSDP Peer 31.1.1.3, AS 0, Description:

Connection status:

State: Established, Resets: 0,

Connection Source: Not set, Connect address: 31.1.1.1

Uptime (Downtime): 00h:07m:53s, SA messages received: 16

TLV messages sent/received: 8/24

SA messages incoming Rrjected: 0

SA messages outgoing Rrjected: 0

SA Filtering:

Input filter Not Configured

Output filter Not Configured

SA-Requests:

Input filter Not Configured

Sending SA-Requests to peer: Disabled

Peer ttl threshold: 0

The introduction of showed items:

Field	Explaination
MSDP Peer	IP address of MSDP Peer.
AS	Autonomous system number belonged toMSDP Peer.
State	MSDP Peer state.
Connection source	The interface used in local TCP connection.
Uptime(Downtime)	The uptime or downtime of MSDP peer.
Messages sent/received	The statistics of messages sent and received from the Peer.
SA Filtering	The filtering policy configured with Peers.
SA-Requests	The configured filtering policy of SA requests.
SAs learned from this peer	The SA numbers learned from MSDP Peers in

	the cache.
SAs limit	The configured SA limit numbers with this MSDP Peer.

6.4.32 show msdp sa-cache

Command: show msdp sa-cache {<*source-address*> [<*group-address*>] | as-num <*sas-number*> | peer <*peer-address*>| rpaddr <*rp-address*>}

Function: Display the configuration information for cache-exterior source under MSDP.

Parameter: ***source-address:*** Source address;

group-address: Group address;

as-number: autonomous-system-number autonomous system number;

peer-address: Peer address;

rp-address: RP address.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the configuration information for cache-exterior source under MSDP.

Example:

Switch#show msdp sa-cache 30.30.30.1

MSDP Flags:

E - set MRIB E flag, L - domain local source is active,

EA - externally active source, PI - PIM is interested in the group,

DE - SAs have been denied.

Cache SA Entry:

(S:30.30.30.1, G: 224.1.1.1, RP: 10.1.1.2), AS: 0, 00h:00m:11s/00h:02m:19s

Learn From Peer:20.1.1.1, RPF Peer: 10.1.1.10

SA Received: 10 Encapsulated data received: 0

grp flags: None source flags: EA, DE

The explanation of showed items:

field	Explaination
(S, G, RP)	running source message information(S, G, RP).
AS Num	Autonomous system number.
update time	SA message cache time.
expire time	SA message expire time.
Learn From Peer	The table is learned from the Peer.
RPF Peer	RPF Peer of the entry.
SA Received	SA message which include the entry.
Encapsulated data received	The multicast message encapsulated in SA message.
grp flags	The multicast group flag in the entry.
source flags	The multicast source flag in the entry.

6.4.33 show msdp sa-cache summary

Command: show msdp sa-cache summary
Function: Show the summary of MSDP Cache.
Command Mode: Admin and Configuration Mode.
Usage Guide: Show the summary of MSDP Cache.
Example:
Switch#show msdp sa-cache summary

MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.

Cache SA Entry:
Total number of SA Entries = 1
Total number of Sources = 1
Total number of Groups = 1
Total number of RPs = 1

Originator-RP SA total RPF peer
10.1.1.2 1 10.1.1.10

AS-num SA total
0 1
The introduction of showed items:

Field	Explaination
Total number of SA Entries	Total number of SA entries in the cache.
Total number of Sources	Total number of different multicast sources in the cache.
Total number of Groups	Total number of different multicast groups in the cache.
Total number of RPs	Total number of different RP in the cache.
Originator-RP	Originated RP address.
SA total	Total number of received SA message from RP.
RPF peer	The RPF Peer address of corresponding RP.
AS-num	Autonomous system number.

6.4.34 show msdp statistics

Command: show msdp statistics peer [*Peer-address*]
Function: Show all the statistics of specified Peer or receiving/sending messages from all the Peers.

Parameter: Peer-address: Show the statistics of messages from specified Peer.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show all the statistics of specified Peer or receiving/sending messages from all the Peers.

Example:

Switch#show msdp sta peer 2.2.2.4

MSDP Peer Statistics :

Peer 2.2.2.4 , AS is 0 , State is Inactive

TLV Rcvd : 76 total

39 keepalives, 37 SAs

0 SA Requests, 0 SA responses

TLV Send : 80 total

41 keepalives, 39 SAs

0 SA Requests, 0 SA responses

SA msgs : 37 received, 39 sent

The introduction of showed items:

Field	Explaination
Peer	MSDP Peer address.
AS	Autonomous system number.
State	MSDP Peer state.
TLV Rcvd	The TLV type and statistics of Peer received.
TLV Send	The TLV type and statistics of Peer sent
SA msgs	The SA message statistics of Peer received and send.

6.4.35 show msdp summary

Command: show msdp summary

Function: Show the summary of MSDP.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the summary of MSDP.

Example:

Switch#show msdp summary

Maximum External SA's Global : 20000

MSDP Peer Status Summary

Peer Address AS State Uptime/ Reset Peer Active Cfg.Max TLV

Downtime Count Name SA Cnt Ext.SAs recv/sent

2.2.2.4 0 Established THU JAN 01 00:00:00 10 0 121/100

The introduction of showed items:

Field	Explaination
Peer Address	IP address of MSDP Peer.
AS	Autonomous system number belonged toMSDP Peer.
State	MSDP Peer state.
Uptime/Downtime	The uptime or downtime of MSDP peer.
Reset Count	The reset count of MSDP Peer.
Peer Name	The description of MSDP Peer.
Active SA	The numbers of active SA.
TLV sent/received	The statistics of TLV messages sent and received from the Peer.

6.4.36 shutdown

Command: shutdown

no shutdown

Function: Disable specified MSDP Peer.

Parameter: None.

Command Mode: MSDP Peer Configuration Mode.

Default: Enabled.

Usage Guide: When configuring a MSDP Peer with multiple commands, sometimes it is required that these commands should be effect together but not one by one. The shutdown command can be used to disable the peer before configuration and the no shutdown used after configuration in order to make the peer configuration effect together. The shutdown command will remove all the TCP sessions with the specified MSDP Peer as well as the statistics.

Example:

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)# shutdown

6.4.37 ttl-threshold

Command: ttl-threshold <*ttl*>

no ttl-threshold

Function: To configure the minimum TTL value of multicast source encapsulated in SA message.

Parameter: *ttl*: minimum TTL value, range from 1 to 255.

Command Mode: MSDP Configuration Mode.

Default: TTL value will not be filtered when TTL value is 0.

Usage Guide: The redistribution of multicast datagrams can be controlled through the TTL value. SA messages will be advertised only if the TTL value in the packet is less than the TTL threshold.

Example:

Switch(config)#router msdp

Switch(router-msdp)#ttl-threshold 10

6.5 ANYCAST RP

6.5.1 debug pim anycast-rp

Command: debug pim anycast-rp

no debug pim anycast-rp

Function: Enable the debug switch of ANYCAST RP function; the no operation of this command will disable this debug switch.

Command Mode: Admin Mode.

Default: The debug switch of ANYCAST RP is disabled by default.

Usage Guide: This command is used to enable the debug switch of ANYCAST RP of the router, it can display the information of handling PIM register packet of the switch——packet, and the information of events——event.

Example:

Switch#debug pim anycast-rp

6.5.2 ip pim anycast-rp

Command: ip pim anycast-rp

no ip pim anycast-rp

Function: Enable the ANYCAST RP of the switch; the no operation of this command is to disable the ANYCAST RP function.

Command Mode: Global Configuration Mode.

Default: The switch will not enable the ANYCAST RP by default.

Usage Guide: This command will globally enable ANYCAST RP protocol, but in order to make ANYCAST RP work, it is necessary to configure self-rp-address and other-rp-address set.

Example: Enable ANYCAST RP in global configuration mode.

Switch(config)#ip pim anycast-rp

6.5.3 ip pim anycast-rp

Command: ip pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>

no ip pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>

Function: Configure ANYCAST RP address (ARA) and the unicast addresses of other RP communicating with this router (as a RP). The no operation of this command will cancel the unicast address of another RP in accordance with the configured RP address.

Parameters: *anycast-rp-addr*: RP address, the absence of the candidate interface in accordance with the address is allowed.

***other-rp-addr*:** The unicast address of other RP communicating with this router (as a RP).

Command Mode: Global Configuration Mode.

Default: There is no configuration by default.

Usage Guide:

1. The anycast-rp-addr configured on this router (as a RP) is actually the RP address configured on multiple RP in the network, in accordance with the address of RP candidate interface (or Loopback interface). The current absence of the candidate interface in accordance with the address is allowed when configuring.
2. Configure the other-rp-address of other RP communicating with this router (as a RP). The unicast address identifies other RP, and is used to communicate with the local router.
3. Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RP in the network to notify all the RP in the network of the source (S.G) state. While forwarding, the router will change the destination address of the register message into other-rp-address.
4. Multiple other-rp-addresses can be configured in accordance with one anycast-rp-addr, once the register message from a DR is received; it should be forwarded to all of these other RP one by one.

Example: Configure other-rp-address in global configuration mode.

Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.3.2

6.5.4 ip pim anycast-rp self-rp-address

Command: ip pim anycast-rp self-rp-address <*self-rp-addr*>

no ip pim anycast-rp self-rp-address

Function: Configure the self-rp-address of this router (as a RP). This address will be used to exclusively identify this router from other RP, and to communicate with other RP. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RP.

Parameters: *self-rp-addr*: The unicast address used by this router (as a RP) to communicate with other RP.

Command Mode: Global Configuration Mode.

Default: No self-rp-address is configured by default.

Usage Guide:

1. Once this router (as a RP) receives the register message from DR unicast, it needs to forward the register message to all the other RP in the network, notifying them of the state of source (S.G). While forwarding the register message, this router will change the source address of it into self-rp-address.
2. Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a register-stop message, whose destination address is the source address of the register message.

3. self-rp-address has to be the address of a three-layer interface on this router, but the configuration is allowed to be done with the absence of the interface.

Example: Configure the self-rp-address of this router in global configuration mode.

Switch(config)#ip pim anycast-rp self-rp-address 1.1.1.1

6.5.5 ip pim rp-candidate

Command: ip pim rp-candidate {vlan<*vlan-id*> |loopback<*index*> |<*ifname*>} [<*A.B.C.D*>] [<*priority*>]

no ip pim rp-candidate

Function: Add a Loopback interface as a RP candidate interface based on the original PIM-SM command; the no operation of this command is to cancel the Loopback interface as a RP candidate interface.

Parameters: *index*: Loopback interface index, whose range is <1-1024>.

***vlan-id*:** the VLAN ID.

***ifname*:** the specified name of the interface.

A.B.C.D/M: the ip prefix and mask.

***<priority>*:** the priority of RP election, ranging from 0 to 255, the default value is 192, the smaller the value is the higher the priority is.

Command Mode: Global Configuration Mode.

Default Setting: No RP interface is configured by default.

Usage Guide: In order to support ANYCAST RP function, new rule allows configuring a Loopback interface to be the RP candidate interface, the RP candidate interface should be currently unique, and the address of which should be added into the router to make sure that PIM router can find the nearest RP. The “no ip pim rp-candidate” command can be used to cancel the RP candidate.

Example: Configure Loopback1 interface as the RP candidate interface in global configuration mode.

Switch(config)#ip pim rp-candidate loopback1

6.5.6 show debugging pim

Command: show debugging pim

Command Mode: Admin Mode.

Usage Guide: The current state of ANYCAST RP debug switch.

Example:

Switch(config)#show debugging pim

Debugging status:

PIM anycast-rp debugging is on

6.5.7 show ip pim anycast-rp first-hop

Command: show ip pim anycast-rp first-hop

Command Mode: Admin and Configuration Mode.
Usage Guide: Display the state information of ANYCAST RP, and display the mrt node information generated in the first hop RP which is currently maintained by the protocol.
Example:
Switch(config)#show ip pim anycast-rp first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0

INCLUDE (192.168.1.136, 224.1.1.1)
Local .l.....

Display	Explanation
Entries	The number of all kinds of entries.
INCLUDE	The information of mrt generated in the first hop RP.

6.5.8 show ip pim anycast-rp non-first-hop

Command: show ip pim anycast-rp non-first-hop
Command Mode: Admin and Configuration Mode.
Usage Guide: Display the state information of ANYCAST RP, and display the mrt node information generated in the non first hop RP which is currently maintained by the protocol, that is the mrt node information which is created after the first hop RP transfers the register message it received to this RP.
Example:
Switch(config)#show ip pim anycast-rp non-first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0

INCLUDE (192.168.10.120, 225.1.1.1)
Local .l.....

Display	Explanation
Entries	The number of all kinds of entries.
INCLUDE	The mrt information created in the first hop RP.

6.5.9 show ip pim anycast-rp status

Command: show ip pim anycast-rp status
Command Mode: Admin and Configuration Mode.
Usage Guide: Display the configuration information of ANYCAST RP, whether ANYCAST RP globally enables, whether the self-rp-address is configured and the list of currently configured ANYCAST RP set.
Example:
Switch(config)#show ip pim anycast-rp status

Anycast RP status:
anycast-rp:Enabled!

self-rp-address:192.168.3.2

anycast-rp address: 1.1.1.1
other rp unicast rp address: 192.168.2.1
other rp unicast rp address: 192.168.5.1

anycast-rp address: 192.168.1.4
other rp unicast rp address: 192.168.2.1

Display	Explanation
anycast-rp:	Whether the ANYCAST RP switch is globally enabled.
self-rp-address:	The configured self-rp-address.
anycast-rp address:	The configured anycast-rp-address.
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address.
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address.
anycast-rp address:	The configured anycast-rp-address*.
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address.

6.6 PIM-SSM

6.6.1 ip multicast ssm

Command: ip multicast ssm {default|range <*access-list-number* >}

no ip multicast ssm

Function: Configure the range of pim ssm multicast address. The "**no ip multicast ssm**" command deletes configured pim ssm multicast group.

Parameter: default: indicates the default range of pim ssm multicast group is 232/8.

<*access-list-number* > is the applying access-list number; it ranges from 1 to 99.

Default: Do not configure the range of pim ssm group address.

Command Mode: Global Mode.

Usage Guide:

1. Only this command is configured, pim ssm can be available.

2. Before configuring this command, make sure ip pim multicasting succeed. This command can't work with DVMRP.

3. Access-list can't used the lists created by ip access-list, but the lists created by access-list.

4. Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ip pim ssm can release the bondage.

5 .If ssm is needed, this command should be configured at the related edge route. For example, the local switch with IGMP (must) and multicast source DR or RP (at least one of the two) configure this command, the middle switch need only enable PIM-SM.

Example: Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23.

Switch (config)#ip multicast ssm range 23

6.7 DVMRP

6.7.1 debug dvmrp

Command: debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm|mfc|mib|timer [probe[probe-timer|neighbor-expiry-timer]| prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|route[report-timer| flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]]|packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]

no debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]|nsm|mfc|mib|timer[probe[probe-timer|neighbor-expiry-timer]|prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|route[report-timer|flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]]|packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]

Function: Display DVMRP protocol debugging message; the "**no debug dvmrp**

[events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm|
mfc|mib|timer [probe[probe-timer|neighbor-expiry-timer]|
prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|
route[report-timer|flash-upd-timer|route-expiry-timer|
route-holdown-timer|route-burst-timer]]
|packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]" command disenables this debugging switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable this switch, and display DVMRP protocol executed relevant messages.

6.7.2 ip dvmrp enable

Command: ip dvmrp enable

no ip dvmrp

Function: Configure to enable DVMRP protocol on interface; the "**no ip dvmrp**" command disenables DVMRP protocol.

Parameter: None

Default: Disable DVMRP Protocol

Command Mode: Interface Configuration Mode

Usage Guide: The interface processes DVMRP protocol messages, only executing DVMRP protocol on interface.

Example: Enable DVMRP Protocol on interface vlan1.

Switch (config)#interface vlan 1

Switch(Config-If-vlan1)#ip dvmrp enable

6.7.3 ip dvmrp metric

Command: ip dvmrp metric <*metric_val*>

no ip dvmrp metric

Function: Configure interface DVMRP report message metric value; the "**no ip dvmrp metric**" command restores default value.

Parameter: ***<metric_val>*** is metric value, value range from 1 to 31

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: The routing information in DVMRP report messages includes a groupsource network and metric list. After configuring interface DVMRP report message metric value, it makes all received routing entriy from the interface adding configured interface metric value as new metric value of the routing. The metric value applies to calculate posion reverse, namely ensuring up-downstream relations. If the metric value of some route on the switch is not less than 32, it explains the route can be reach. If it is downstream of some route after calculation and judgment, it will transmit report message included the route to upstream. The route metric increases 32

based on original value in order to indicate downstream itself.

Example: Configure interface DVMRP report message metric value: 2

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip dvmrp metric 2

6.7.4 ip dvmrp multicast-routing

Command: ip dvmrp multicast-routing

no ip dvmrp multicast-routing

Function: Globally enable DVMRP protocol; the "no ip dvmrp multicast-routing" command globally disenables DVMRP protocol

Parameter: None

Default: Default

Command Mode: Global Mode

Usage Guide: Dvmrp multicast-protocol can enable after globally execute the command

Example: Switch (config)#ip dvmrp multicast-routing

6.7.5 ip dvmrp output-report-delay

Command: ip dvmrp output-report-delay <*delay_val*> [<*burst_size*>]

no ip dvmrp output-report-delay

Function: Configure the delay of DVMRP report message transmitted on interface and transmitted message quantity every time, the "**no ip dvmrp output-report-delay**" command restores default value.

Parameter: <*delay_val*> is the delay of periodically transmitted DVMRP report message, value range from 1s to 5s.

<*burst_size*> is a quantity of transmitted message every time, value range from 1 to 65535

Default: Default the delay of transmitted DVMRP report message as 1s, default: transmitting two messages every time.

Command Mode: Interface Configuration Mode

Usage Guide: Avoid message burst if setting an appropriate delay.

Example:

Switch (Config-If-vlan1)#ip dvmrp output-report-delay 1 1024

6.7.6 ip dvmrp reject-non-pruners

Command: ip dvmrp reject-non-pruners

no ip dvmrp reject-non-pruners

Function: Configure to reject neighbor ship with DVMRP router of non pruning/grafting on the interface, the "**no ip dvmrp reject-non-pruners**" command restores neighbor ship can be established.

Parameter: None

Default: Default
Command Mode: Interface Configuration Mode
Usage Guide: The command determines if it will establish neighboringship with DVMRP router of non pruning/grafting or not.
Example:
Switch (Config-If-vlan1)#ip dvmrp reject-non-pruners

6.7.7 ip dvmrp tunnel

Command: ip dvmrp tunnel <*index*> <*src-ip*> <*dst-ip*>
no ip dvmrp tunnel {<*index*> |<*src-ip*> <*dst-ip*>}
Function: Configure a DVMRP tunnel; the "**no ip dvmrp tunnel** {**<*index*> |<*src-ip*> <*dst-ip*>}**" command deletes a DVMRP tunnel.
Parameter: ***<src-ip>*** is source IP address,
<dst-ip> is remote neighbor IP address,
<index> is tunnel index number, value range from 1 to 65535.
Default: Do not Configure DVMRP tunnel.
Command Mode: Global Mode
Usage Guide: Because not all of switches support multicast, DVMRP supports tunnel multicast communication. The tunnel is a way of transmitted multicast data packet among DVMRP switches partitioned off switches without supporting multicast routing. It acts as a virtual network between two DVMRP switches. Multicast data packets packed in unicast data packets, directly are transmitted to next supporting multicast switch. DVMRP protocol equally deal with tunnel interface and general physical interface. After configuring no ip dv multicast-routing, all of the tunnel configurations are deleted.
Example:
Switch(config)#ip dvmrp tunnel 1 12.1.1.1 24.1.1.1

6.7.8 show ip dvmrp

Command: show ip dvmrp
Function: Display DVMRP protocol information.
Parameter: None
Default: Do not display (Off)
Command Mode: Any Configuration Mode
Usage Guide: The command applies to display some total statistic information of DVMRP protocol
Example: Switch#show ip dvmrp
DVMRP Daemon Start Time: MON JAN 01 00:00:09 2001
DVMRP Daemon Uptime: 17:37:03
DVMRP Number of Route Entries: 2
DVMRP Number of Reachable Route Entries: 2
DVMRP Number of Prune Entries: 1

DVMRP Route Report Timer: Running
DVMRP Route Report Timer Last Update: 00:00:56
DVMRP Route Report Timer Next Update: 00:00:04
DVMRP Flash Route Update Timer: Not Running

6.7.9 show ip dvmrp interface

Command: show ip dvmrp interface [<*ifname*>]
Function: Display DVMRP interface
Parameter: ***<ifname>*** is interface name, namely displaying configured interface information of specified interface.
Default: Do not display (Off)
Command Mode: Any Configuration Mode
Example: Switch #show ip dvmrp neighbor vlan 4

Address	Interface	Vif Index	Ver.	Nbr Cnt	Type	Remote Address
13.1.1.3	Vlan1	1	v3.ff	0	BCAST	N/A
10.1.35.3	Vlan2	0	v3.ff	0	BCAST	N/ASwitch #

Displayed Information	Explanations
Address	Address
Interface	Interface corresponding physical interface name
Vif Index	Virtual interface index
Ver	Interface supporting version
Nbr Cnt	Neighbor count
Type	Interface type
Remote Address	Remote address

6.7.10 show ip dvmrp neighbor

Command: show ip dvmrp neighbor [{<*ifname*> <*A.B.C.D*> [detail]}|{ <*ifname*>[detail]}|detail]
Function: Display DVMRP neighbor.
Parameter: ***<ifname>*** is interface name, namely displaying neighbor information of specified interface.
Default: Do not display (Off).
Command Mode: Any Configuration Mode
Example: Display interface vlan1 neighbor on Ethernet.
Switch #show ip dvmrp neighbor

Neighbor Address	Interface	Uptime/Expires	Maj Ver	Min Ver	Cap Flg
10.1.35.5	Vlan2	00:00:16/00:00:29	3	255	2e

Displayed Information	Explanations

Neighbor Address	Neighbor address
Interface	Detect the neighbor's interface
Uptime/Expires	The neighbor uptime/expire time
Maj Ver	Major version
Min Ver	Mini version
Cap Flg	Capacity flag

6.7.11 show ip dvmrp prune

Command: show ip dvmrp prune [{group <A.B.C.D> [detail]}|{source <A.B.C.D/M> group <A.B.C.D> [detail]}|{source <A.B.C.D/M> [detail] }|detail]

Function: Display DVMRP message forwarding item.

Parameter: None

Default: Do not display

Command Mode: Any Configuration Mode

Usage Guide: This command applies to display DVMRP multicast forwarding item, namely multicast forwarding table calculated by dvmrp protocol.

Example:

Switch#show ip dvmrp prune

Flags: P=Pruned,H=Host,D=Holddown,N=NegMFC,I=Init

Source Address	Mask Len	Group Address	State	FCR Exptime Cnt	Prune/Graft ReXmit-Time
13.1.1.0	24	239.0.0.1	 1	01:59:56	Off

Displayed Information	Explanations
Source Address	Source address
Mask Len	Mask length
Group Address	Group address
State	Table item state
FCR Exptime	FCR expire time
Prune/Graft ReXmit-Time	Prune expire time/ Graft retransmit time

6.7.12 show ip dvmrp route

Command: show ip dvmrp route [{<A.B.C.D/M>[detail]}|{nexthop <A.B.C.D>[detail]}|{best-match <A.B.C.D> [detail]}|detail]

Function: Prune expire time/ Graft retransmit time

Parameter: None

Default: Do not display

Command Mode: Any Configuration Mode

Usage Guide: The command applies to display DVMRP routing table item; DVMRP maintains individual unicast routing table to check RPF.

Example: Display DVMRP routiing.

Switch #show ip dvmrp route

Flags: N = New, D = DirectlyConnected, H = Holddown

Network	Flags	Nexthop Xface	Nexthop Neighbor	Metric	Uptime	Exptime
10.1.35.0/24	.D.	Vlan2	Directly Connected	1	00:11:16	00:00:00
13.1.1.0/24	.D.	Vlan1	Directly Connected	1	00:10:22	00:00:00

Displayed Information	Explanations
Network	Target net segment or address and mask
Flags	Routing state flag
Nexthop Xface	Next hop interface address
Nexthop Neighbor	Next hop neighbor
Metric	Routing metric value
Uptime	Routing uptime
Exptime	Routing expire time

6.8 DCSCM

6.8.1 access-list (Multicast Destination Control)

Command: **access-list <6000-7999> {{{add | delete} profile-id WORD} | {{deny|permit} (ip) {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}}**

no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip> {range <2-65535>|}}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip> {range <2-255>|}}|any-destination}

Function: Configure destination control multicast access-list, the "**no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**" command deletes the access-list.

Parameter: <6000-7999>: destination control access-list number.

{add | delete}: add or delete the profile.

{deny|permit}: deny or permit.

<source/M>: multicast source address and mask length.

<source-host-ip>: multicast source host address.

<2-65535>: the range of multicast source host.

<destination/M>: multicast destination address and mask length.

<destination-host-ip>: multicast destination host address.

<2-255>: the range of multicast destination host.

Default: None

Command Mode: Global Mode

Usage Guide: ACL of Multicast destination control list item is controlled by specifical ACL number from 6000 to 7999, the command applies to configure this ACL. ACL of ip Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use mask length to configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list. And adding or deleting the profile-id can be used to change the multicast destination control ACL.

Example:

Switch(config)#access-list 6000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

Switch(config)#access-list 6000 add profile-id 1

Switch(config)#

6.8.2 access-list (Multicast Source Control)

Command: **access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**

no access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

Function: Configure source control multicast access-list; the "**no access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**" command deletes the access-list.

Parameter: <5000-5099>: source control access-list number.

{deny|permit}: deny or permit.

<source>: multicast source address..

<source-wildcard>: multicast source address wildcard character.

<source-host-ip>: multicast source host address.

<destination>: multicast destination address.

<destination-wildcard>: multicast destination address wildcard character.

<destination-host-ip>: multicast destination host address.

Default: None

Command Mode: Global Mode

Usage Guide: ACL of Multicast source control list item is controlled by specifical ACL number from 5000 to 5099, the command applies to configure this ACL. ACL of Multicast source control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard character to configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.

Example: Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

6.8.3 ip multicast destination-control

Command: ip multicast destination-control
no ip multicast destination-control
Function: Enable multicast purpose control access list, whose NO form is disable
Parameter: None
Default: Off
Command Mode: Global Mode
Usage Guide: This command is used in conjunction with 5.8.5 and 5.8.6 to control access lists for multicast purposes
Example:
Switch (config)#ip multicast destination-control
Switch (config)#

6.8.4 ip multicast destination-control access-group (sip)

Command: ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>
no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>
Function: Configure multicast destination-control access-list used on specified net segment, the "**no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>**" command deletes this configuration.
Parameter: <IPADDRESS/M>: IP address and mask length;
<6000-7999>: Destination control access-list number.
Default: None
Command Mode: Global Mode
Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING or IGMP is enabled, for adding the members to multicast group. If configuring multicast destination-control on specified net segment of transmitted igmp-report, and match configured access-list, such as matching permit, the interface can be added, otherwise do not be added. If relevant group or source in show ip igmp groups detail has been established before executing the command, it needs to execute clear ip igmp groups command to clear relevant groups in Admin mode.
Example:
Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000

6.8.5 ip multicast destination-control access-group (vmac)

Command: ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>
no ip multicast destination-control <1-4094> <macaddr >access-group

<6000-7999>

Function: Configure multicast destination-control access-list used on specified vlan-mac, the "**no ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>**" command deletes this configuration.

Parameter: <1-4094>: VLAN-ID;

<macaddr>: Transmitting source MAC address of IGMP-REPORT, the format is "xx-xx-xx-xx-xx-xx";

<6000-7999>: Destination-control access-list number.

Default: None

Command Mode: Global Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the members to multicast group. If configuring multicast destination-control to source MAC address of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.

Example:

Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000

6.8.6 ip multicast policy

Command: ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>

no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos

Function: Configure multicast policy, the "**no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos**" command deletes it.

Parameter:

<IPADDRESS/M>: are multicast source address, mask length, destination address, and mask length separately.

<priority>: specified priority, range from 0 to 7

Default: None

Command Mode: Global Mode

Usage Guide: The command configuration modifies to a specified value through the switch matching priority of specified range multicast data packet, and the TOS is specified to the same value simultaneously.Carefully, the packet transmitted in UNTAG mode does not modify its priority.

Example: Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7

6.8.7 ip multicast source-control

Command: ip multicast source-control

no ip multicast source-control

Function: Configure to globally enable multicast source control, the "**no ip multicast source-control**" command restores global multicast source control disabled.

Parameter: None

Default: Disabled

Command Mode: Global Mode

Usage Guide: The source control access-list applies to interface with only enabling global multicast source control, and configure to disabled global multicast source control without configuring source control access-list on every interface. After configuring the command, multicast data received from every interface does not have matching multicast source control list item, and then they will be thrown away by switches, namely only multicast data matching to PERMIT can be received and forwarded.

Example: Switch(config)#ip multicast source-control

6.8.8 ip multicast source-control access-group

Command: ip multicast source-control access-group <5000-5099>

no ip multicast source-control access-group <5000-5099>

Function: Configure multicast source control access-list used on interface, the "no ip multicast source-control access-group <5000-5099>" command deletes the configuration.

Parameter: <5000-5099>: Source control access-list number**.**

Default: None

Command Mode: Interface Configuration Mode

Usage Guide: The command configures with only enabling global multicast source control. After that, it will match multicast data message imported from the interface according to configured access-list, such as matching: permit, the message will be received and forwarded; otherwise the message will be thrown away.

Example:

Switch (config)#interface ethernet1/0/4

Switch (Config-If-Ethernet1/0/4)#ip multicast source-control access-group 5000

Switch (Config-If-Ethernet1/0/4)#

Switch(router-msdp)#default-rpf-peer 10.0.0.1 rp-policy 10

6.8.9 multicast destination-control

Command: multicast destination-control

no multicast destination-control

Function: Configure to globally enable IPv4 and IPv6 multicast destination control, after configuring this command, IPv4 and IPv6 multicast destination control will take effect at the same time. The no operation of this command is to recover and disable the IPv4 and IPv6 multicast destination control globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Configuration Mode.

Usage Guide: Only after globally enabling the multicast destination control, the other destination control configuration can take effect; the destination access list can be applied to ports, VLAN-MAC and SIP. After configuring this command, IGMP-SNOOPING and IGMP will match

according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT.

Example:

switch(config)# multicast destination-control

6.8.10 profile-id (Multicast Destination Control Rule List)

Command: profile-id <1-50> {deny|permit} {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}

no profile-id <1-50>

Function: Configure the destination control profile rule. The no command deletes the profile rule.

Parameters: <1-50>: profile-id.

{deny|permit}: deny or permit.

<source/M>: multicast source address and mask length.

<source-host-ip>: multicast source host address.

<2-65535>: range of multicast source host.

<destination/M>: multicast destination address and mask length.

<destination-host-ip>: multicast destination host address.

<2-255>: range of multicast destination host.

Default: None.

Command Mode: Global Mode.

Usage Guide: Profile-list of Multicast destination control list item is controlled by specifical profile-id number from 1 to 50, the command applies to configure this profile to add it into the ACL for using. Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to ACLs, and use mask length to configure address range, and also specify a host address or all address. Remarkable, “all address” is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.

Example:

Switch (config)# profile-id 1 deny ip any-source host-destination 224.1.1.2

6.8.11 show ip multicast destination-control

Command: show ip multicast destination-control [detail]

show ip multicast destination-control interface <Interfacename> [detail]

show ip multicast destination-control host-address <ipaddress> [detail]

show ip multicast destination-control <vlan-id> <mac-address> [detail]

Function: Display multicast destination control

Parameter: detail: expresses if it display information in detail or not..

<Interfacename>: interface name or interface aggregation name, such as Ethernet1/0/1, port-channel 1 or ethernet1/0/1.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast destination control rules of configuration, including detail option, and access-list information applied in detail.

Example:

Switch (config)#show ip multicast destination-control
ip multicast destination-control is enabled
ip multicast destination-control 11.0.0.0/8 access-group 6003
ip multicast destination-control 1 00-03-05-07-09-11 access-group 6001
multicast destination-control access-group 6000 used on interface Ethernet1/0/13
switch(config)#

6.8.12 show ip multicast destination-control access-list

Command: show ip multicast destination-control access-list
show ip multicast destination-control access-list <6000-7999>

Function: Display destination control multicast access-list of configuration.

Parameter: <6000-7999>: access-list number.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays destination control multicast access-list of configuration.

Example:

Switch# sh ip multicast destination-control acc
access-list 6000 deny ip any any-destination
access-list 6000 deny ip any host-destination 224.1.1.1
access-list 6000 deny ip host 2.1.1.1 any-destination
access-list 6001 deny ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6002 permit ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6003 permit ip 2.1.1.0 0.0.0.255 225.0.0.0 0.255.255.255

6.8.13 show ip multicast destination-control filter-profile-list

Command: show ip multicast destination-control filter-profile-list
show ip multicast destination-control filter-profile-list <1-50>

Function: Show the configured destination control profile rule list.

Parameters: <1-50>: profile-id.

Default: None.

Command Mode: Admin and configuration mode.

Usage Guide: This command can show the configured destination control profile rule list.

Example:
Switch#show ip multicast destination-control filter-profile-list
profile-id 1 deny ip any-source any-destination
profile-id 2 deny ip any-source host-destination 224.1.1.1
profile-id 3 deny ip host-source 2.1.1.1 any-destination

6.8.14 show ip multicast policy

Command: show ip multicast policy
Function: Display multicast policy of configuration
Parameter: None
Default: None
Command Mode: Admin Mode and Global Mode
Usage Guide: The command displays multicast policy of configuration
Example:
Switch#show ip multicast policy
ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5

6.8.15 show ip multicast source-control

Command: show ip multicast source-control [detail]
show ip multicast source-control interface <Interfacename> [detail]
Function: Display multicast source control configuration
Parameter: detail: expresses if it displays information in detail.
<Interfacename>: interface name, such as Ethernet 1/0/1 or ethernet1/0/1.
Default: None
Command Mode: Admin Mode and Global Mode
Usage Guide: The command displays multicast source control rules of configuration, including detail option, and access-list information applied in detail.
Example:
Switch#show ip multicast source-control detail
ip multicast source-control is enabled
Interface Ethernet1/0/13 use multicast source control access-list 5000
access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255

6.8.16 show ip multicast source-control access-list

Command: show ip multicast source-control access-list
show ip multicast source-control access-list <5000-5099>
Function: Display source control multicast access-list of configuration
Parameter: <5000-5099>: access-list number
Default: None

Command Mode: Admin Mode and Global Mode
Usage Guide: The command displays source control multicast access-list of configuration
Example:
Switch#sh ip multicast source-control access-list
access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255

6.9 IGMP

6.9.1 clear ip igmp group

Command: clear ip igmp group [A.B.C.D | IFNAME]
Function: Delete the group record of the specific group or interface.
Parameters: A.B.C.D the specific group address; IFNAME the specific interface.
Command Mode: Admin Configuration Mode
Usage Guide: Use show command to check the deleted group record.
Example: Delete all groups.
Switch#clear ip igmp group
Relative Command: show ip igmp group

6.9.2 debug igmp event

Command: debug igmp event
no debug igmp event
Function: Enable debugging switch of IGMP event; the "**no debug igmp event**" command disenables the debugging switch
Parameter: None
Default: Disabled
Command Mode: Admin Mode
Usage Guide: Enable debugging switch if querying IGMP event information
Example:
Switch# debug igmp event
igmp event debug is on
Switch# 01:04:30:56: IGMP: Group 224.1.1.1 on interface vlan1 timed out

6.9.3 debug igmp snooping all/packet/event/timer/mfc/authentication/ha

Command: debug igmp snooping all/packet/event/timer/mfc/authentication/ha

no debug igmp snooping all/packet/event/timer/mfc/authentication/ha

Function: Enable the IGMP Snooping switch of the switch; the "**no debug igmp snooping all/packet/event/timer/mfc**" disables the debugging switch.

Command Mode: Admin Mode

Default: IGMP Snooping debugging switch is disabled on the switch by default.

Usage Guide: The command is used for enable the IGMP Snooping debugging switch of the switch, switch IGMP data packet message can be shown with "packet" parameter, event message with "event", timer message with "time", downsending hardware entries message with "mfc", authention message with "authentication", Highly Available message with "ha" and all debugging messages with "all".

6.9.4 ip igmp access-group

Command: ip igmp access-group {<*acl_num* | *acl_name*>}

no ip igmp access-group

Function: Configure interface to filter IGMP group; the "**no ip igmp access-group**" command cancels the filter condition

Parameter: {<acl_num | acl_name>} is SN or name of access-list, value range of **acl_num** is from 1 to 99.

Default: Default no filter condition

Command Mode: Interface Configuration Mode

Usage Guide: Configure interface to filter groups, permit or deny some group joining.

Example: Configure interface vlan1 to permit group 224.1.1.1, deny group 224.1.1.2.

Switch (config)#access-list 1 permit 224.1.1.1 0.0.0.0

Switch (config)#access-list 1 deny 224.1.1.2 0.0.0.0

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp access-group 1

6.9.5 ip igmp immediate-leave

Command: ip igmp immediate-leave group-list {<number>|<name>}

no ip igmp immediate-leave

Function: Configure IGMP working in immediate-leave mode, that is, when the host transmits member identity report of equivalent to leave a group, router does not transmit query, it directly confirms there is no member of this group in subnet; the "**no ip igmp immediate-leave**" command cancels immediate-leave mode.

Parameter: ***<number>*** is access-list SN, value is from 1 to 99.

<name> is access-list name.

Default: Interface default and no immediate-leave group of configuration after finished product

Command Mode: Interface Configuration Mode

Usage Guide: The command only can apply in only one host condition in subnet.

Example: Configure immediate-leave mode on access-group list 1

Switch (Config-if-Vlan1)#ip igmp immediate-leave group-list 1
Switch (Config-if-Vlan1)#

6.9.6 ip igmp join-group

Command: ip igmp join-group <*A.B.C.D* >
no ip igmp join-group <*A.B.C.D* >
Function: Configure interface to join some IGMP group; the "no ip igmp join-group" command cancels this join
Parameter: ***<A.B.C.D>:*** is group address
Default: Do not join
Command Mode: Interface Configuration Mode
Usage Guide: When the switch is the HOST, the command configures HOST to join some group; that is, if configuring the interface join-group 224.1.1.1, it will transmit IGMP member report including group 224.1.1.1 when the switch receives IGMP group query transmitted by other switches. Carefully, it is the diffence between the command and **ip igmp static-group** command.
Example: Configure join-group 224.1.1.1 on interface vlan1.
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp join-group 224.1.1.1

6.9.7 ip igmp last-member-query-interval

Command: ip igmp last-member-query-interval <interval>
no ip igmp last-member-query-interval
Function: Configure interval of specified group query transmitting on interface; the "**no ip igmp last-member-query-interval**" command cancels the value of user manual configuration, and restores default value.
Parameter: ***<interval>*** is interval of specified group query, range from 1000ms to 25500ms; the value is integer times of 1000ms, namely if input value is not integer times of 1000ms, the system automatically changes to integer times of 1000ms.
Default: 1000ms
Command Mode: Interface Configuration Mode
Example: Configure interface vlan1 IGMP last-member-query-interval to 2000.
Switch (config)#int vlan 1
Switch (Config-if-vlan1)#ip igmp last-member-query-interval 2000

6.9.8 ip igmp limit

Command: ip igmp limit <state-count>
no ip igmp limit
Function: Configure limit IGMP state-count on interface; the "**no ip igmp limit**" command cancels the value of user manual configuration, and restores default value.
Parameter: ***<state-count>*** is maximum IGMP state reserved by interface, range from 1 to 65000

Default: 0, no limit.

Command Mode: Interface Configuration Mode

Usage Guide: After configuring maximum state state-count, interface only saves states which are not more than state-count groups and sources. If it reaches upper limit of state-count, it does not deal with when receiving related new group member identity report. If it has saved some IGMP group states before configuring the command, it deletes all of the states, and then immediately transmits IGMP general query to collect the member identity report which is not more than state-count group. Static state and static source are not in the limit

Example: Configure interface vlan1 IGMP limit to 4000.

Switch (config)#int vlan 1

Switch (Config-if-vlan1)#ip igmp limit 4000

6.9.9 ip igmp query-interval

Command: ip igmp query-interval <*time_val*>

no ip igmp query-interval

Function: Configure interval of periodically transmitted IGMP query information; the "**no ip igmp query-interval**" command restores default value.

Parameter: **<*time_val*>** is interval of periodically transmitted IGMP query information, value range from 1s to 65535s.

Default: Default interval of periodically transmitted IGMP query information to 125s.

Command Mode: Interface Configuration Mode

Usage Guide: Periodically transmitting IGMP query information on interface when some interface enables some group multicast protocol. The command applies to configure this query period time.

Example: Configure interval of periodically transmitted IGMP query message to 10s

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp query-interval 10

6.9.10 ip igmp query-max-response-time

Command: ip igmp query-max-response-time <*time_val*>

no ip igmp query- max-response-time

Function: Configure IGMP query-max-response-time of interface; the "**no ip igmp query-max-response-time**" command restores default value.

Parameter: <***time_val***> is IGMP query-max-response-time of interface, value range from 1s to 25s

Default: 10s.

Command Mode: Interface Configuration Mode

Usage Guide: After the switch receives a query message, the host will configure a timer for its affiliated every multicast group, the value of timer is selected random from 0 to maximum response time, the host will transmit member report message of the multicast group. Reasonable configuring maximum response time, it can make host quickly response query message. The

router can also quickly grasp the status of multicast group member.

Example: configure the maximum period responding to the IGMP query messages to 20s

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp query- max-response-time 20

6.9.11 ip igmp query-timeout

Command: ip igmp query-timeout <*time_val*>

no ip igmp query-timeout

Function: Configure IGMP query timeout of interface; the "**no ip igmp query-timeout**" command restores default value.

Parameter: <***time_val***> is IGMP query-timeout, value range from 60s to 300s.

Default: 255s.

Command Mode: Interface Configuration Mode

Usage Guide: When multi-running IGMP switches are exist on sharing network, a switch will be voted as query processor on the sharing network, and other switches will be a timer monitoring the state of query processor; It still does not receive query message transmitting by query processor over query time-out, thus it re-votes another switch as new query processor.

Example: Configure timeout of IGMP query message on interface to 100s.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp query-timeout 100

6.9.12 ip igmp robust-variable

Command: ip igmp robust-variable <value>

no ip igmp robust-variable

Function: Configure the robust variable value， the "**no ip igmp robust-variable**" command restores default value.

Parameter: value: range from 2 to 7.

Command Mode: Interface Configuration Mode

Default: 2.

Usage Guide: It is recommended using the default value.

Example:

Switch (config-if-vlan1)#ip igmp robust-variable 3

6.9.13 ip igmp static-group

Command: ip igmp static-group <*A.B.C.D* > [source <*A.B.C.D* >]

no ip igmp static -group <*A.B.C.D* > [source <*A.B.C.D* >]

Function: Configure interface to join some IGMP static group; the "no ip igmp static-group" command cancels this join.

Parameter: ***<A.B.C.D>*** is group address;

Source *<A.B.C.D>* expresses SSM source address of configuration.

Default: Do not join static group

Command Mode: Interface Configuration Mode

Usage Guide: When configuring some interface to join some static group, it will receives about the multicast packet of the static group whether the interface has a real receiver or not; that is, if configuring the interface to join static group 224.1.1.1, the interface always receives about multicast packet about group 224.1.1.1 whether the interface has a receiver or not. Carefully, it is the difference between the command and ip igmp join-group command.

Example: Configure static-group 224.1.1.1 on interface vlan1.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp static-group 224.1.1.1

6.9.14 ip igmp version

Command: ip igmp version <*version*>

no ip igmp version

Function: Configure IGMP version on interface; the "**no ip igmp version**" command restores default value.

Parameter: <***version***> is IGMP version of configuration, currently supporting version 1, 2 and 3.

Default: version 2.

Command Mode: Interface Configuration Mode

Usage Guide: The command mainly applies to supply upward compatibility of the different version; it is not communicated between version 1 and version 2, therefore it must configure to the same version IGMP in the same network. When other routers which are not upgraded to IGMPv3 on interface-connected subnet need to join member identity collection of subnet IGMP together, the interface is configured to corresponding version.

Example: Configure IGMP on interface to version 3.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp version 3

6.9.15 show ip igmp groups

Command: show ip igmp groups [<*A.B.C.D*>] [*detail*]

Function: Display IGMP group information

Parameter: ***<group_addr>*** is group address, namely querying specified group information; Detail expresses group information in detail

Default: Do not display

Command Mode: Admin Mode

Example:

Switch (config)#show ip igmp groups

IGMP Connected Group Membership (2 group(s) joined)

Group Address	Interface	Uptime	Expires	Last Reporter
226.0.0.1	Vlan1	00:00:01	00:04:19	1.1.1.1
239.255.255.250	Vlan1	00:00:10	00:04:10	10.1.1.1

Switch#

Displayed Information	Explanations
Group Address	Multicast group IP address
Interface	Interface affiliated with multicast group
Uptime	Multicast group uptime
Expires	Multicast group expire time
Last Reporter	Last reporter to the host of the multicast group

Switch (config)#show ip igmp groups 234.1.1.1 detail
IGMP Connect Group Membership (2 group(s) joined)
Flags: SG - Static Group, SS - Static Source, SSM - SSM Group, V1 - V1 Host Pres
ent, V2 - V2 Host Present
Interface: Vlan1
Group: 234.1.1.1
Flags:
Uptime: 00:00:19
Group Mode: INCLUDE
Last Reporter: 10.1.1.1
Exptime: stopped
Source list: (2 members S - Static)

Source Address	Uptime	v3 Exp	Fwd	Flags
1.1.1.1	00:00:19	00:04:01	Yes	
2.2.2.2	00:00:19	00:04:01	Yes	

Displayed Information	Explanations
Group	Mutlicast group IP address
Interface	Interface affiliated with Mutlicast group
Flags	Group property flag
Uptime	Mutlicast group uptime
Group Mode	Group mode, including INCLUDE and EXCLUDE. Group V3 will be available, group V1 and group V2 are regards as EXCLUDE mode.
Exptime	Mutlicast group expire time
Last Reporter	Last reporter to the host of the Mutlicast group
Source Address	Source address of this group
V3 Exp	Source expire time
Fwd	If the data of the source is forwarded or not.
Flags	Source property flag

6.9.16 show ip igmp interface

Command: show ip igmp interface {vlan *<vlan_id>*|*<ifname>*}

Function: Display related IGMP information on interface.

Parameter: ***<ifname>*** is interface name, namely displaying IGMP information of specified interface.

Default: Do not display

Command Mode: Admin Mode

Example: Display interface vlan1 IGMP message on Ethernet.

```
Switch (config)#show ip igmp interface Vlan1
Interface Vlan1(2005)
  Index 2005
  Internet address is 10.1.1.2
  IGMP querier
  IGMP current version is V3, 2 group(s) joined
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 ms
  Group Membership interval is 260 seconds
  IGMP is enabled on interface
```

6.10 IGMP Snooping

6.10.1 clear ip igmp snooping vlan

Command: clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]

Function: Delete the group record of the specific VLAN.

Parameters: <1-4094> the specific VLAN ID; A.B.C.D the specific group address.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

```
Switch#clear ip igmp snooping vlan 1 groups
```

Relative Command: show ip igmp snooping vlan <1-4094>

6.10.2 clear ip igmp snooping vlan <1-4094> mrouter-port

Command: clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet IFNAME | IFNAME]

Function: Delete the mrouter port of the specific VLAN.

Parameters: <1-4094> the specific VLAN ID; ethernet the Ethernet port name; IFNAME the port name.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted mrouter port of the specific VLAN.

Example: Delete mrouter port in vlan 1.

Switch# clear ip igmp snooping vlan 1 mrouter-port

Relative Command: show ip igmp snooping mrouter-port

6.10.3 debug igmp snooping all/packet/event/timer/mfc

Command: debug igmp snooping all/packet/event/timer/mfc

no debug igmp snooping all/packet/event/timer/mfc

Function: Enable the IGMP Snooping switch of the switch; the "**no debug igmp snooping all/packet/event/timer/mfc**" disables the debugging switch.

Command Mode: Admin Mode

Default: IGMP Snooping debugging switch is disabled on the switch by default.

Usage Guide: The command is used for enable the IGMP Snooping debugging switch of the switch, switch IGMP data packet message can be shown with "packet" parameter, event message with "event", timer message with "time", downsending hardware entries message with "mfc", and all debugging messages with "all".

6.10.4 ip igmp snooping

Command: ip igmp snooping

no ip igmp snooping

Function: Enable the IGMP Snooping function; the "**no ip igmp snooping**" command disables this function.

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: Use this command to enable IGMP Snooping, that is permission every VLAN config the function of IGMP snooping. The "**no ip igmp snooping**" command disables this function.

Example: Enable IGMP Snooping.

Switch(config)#ip igmp snooping

6.10.5 ip igmp snooping proxy

Command: ip igmp snooping proxy

no ip igmp snooping proxy

Function: Enable IGMP Snooping proxy function, the no command disables the function.

Parameter: None.

Command Mode: Global Mode
Default: Enable.
Example:
Switch(config)#no ip igmp snooping proxy

6.10.6 ip igmp snooping vlan

Command: ip igmp snooping vlan *<vlan-id>*
no ip igmp snooping vlan *<vlan-id>*
Function: Enable the IGMP Snooping function for the specified VLAN; the "**no ip igmp snooping vlan <vlan-id>**" command disables the IGMP Snooping function for the specified VLAN.
Parameter: ***<vlan-id>*** is the VLAN number.
Command mode: Global Mode
Default: IGMP Snooping is disabled by default.
Usage Guide: To configure IGMP Snooping on specified VLAN, the global IGMP Snooping should be first enabled. Disable IGMP Snooping on specified VLAN with the "**no ip igmp snooping vlan <vlan-id>**" command.
Example: Enable IGMP Snooping for VLAN 100 in Global Mode.
Switch(config)#ip igmp snooping vlan 100

6.10.7 ip igmp snooping vlan immediate-leave

Command: ip igmp snooping vlan *<vlan-id>* immediate-leave
no ip igmp snooping vlan *<vlan-id>* immediate-leave
Function: Enable the IGMP Snooping fast leave function for the specified VLAN; the "**no ip igmp snooping vlan *<vlan-id>* immediate-leave**" command disables the IGMP Snooping fast leave function.
Parameter: *<vlan-id>* is the VLAN number specified.
Command mode: Global Mode
Default: This function is disabled by default.
Usage Guide: Enable immediate-leave function of the IGMP Snooping in specified VLAN; the"no" form of this command disables the immediate-leave function of the IGMP Snooping.
Example: Enable the IGMP Snooping fast leave function for VLAN 100.
Switch(config)#ip igmp snooping vlan 100 immediate-leave

6.10.8 ip igmp snooping vlan <id> immediately-leave mac-based

Command: ip igmp snooping vlan <id> immediately-leave **mac-based**
no ip igmp snooping vlan <id> immediately-leave mac-based

Function: Configure this command to delete the existed igmp snooping table entries according to the source mac in leave packet when the switch which is enabled the igmp snooping function receives the leave packet. Only when the received the port, source mac and multicast group of the leave packet are the same as the port, host mac and multicast group of the existed igmp snooping table entry, the snooping table entry can be deleted. If this command is not configured, delete the existed igmp snooping table entry according to the port and multicast group of the leave packet.

Command mode: Global Mode

Default: This function is disabled by default.

Usage Guide: Configure the immediately-leave under the same vlan at the same time to make this command effective. In this time, deal with it according to the host mac of the port.

Example: Use the following configuration when delete the table entry according to the host mac of the port.

switch(config)#ip igmp snooping vlan 12 immediately-leave

switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based

6.10.9 ip igmp snooping vlan l2-general-querier

Command: ip igmp snooping vlan < *vlan-id* > l2-general-querier

no ip igmp snooping vlan < *vlan-id* > l2-general-querier

Function: Set this VLAN to layer 2 general querier.

Parameter: ***vlan-id***: is ID number of the VLAN, ranging is <1-4094>.

Command Mode: Global mode

Default: VLAN is not as the IGMP Snooping layer 2 general querier.

Usage Guide: It is recommended to configure a layer 2 general querier on a segment. IGMP Snooping function will be enabled by this command if not enabled on this VLAN before configuring this command, IGMP Snooping function will not be disabled when disabling the layer 2 general querier function. This command is mainly for sending general queries regularly to help switches within this segment learn mrouter ports.

Comment: There are three paths IGMP snooping learn mrouter

1 Port receives the IGMP query messages

2 Port receives multicast protocol packets, and supports DVMRP, PIM

3 Static configured port

6.10.10 ip igmp snooping vlan l2-general-querier-source

Command: ip igmp snooping vlan <vlanid> L2-general-query-source <A.B.C.D>

no ip igmp snooping vlan <vlanid> L2-general-query-source

Function: Configure source address of query of igmp snooping

Parameters: <vlanid>: the id of the VLAN, with limitation to <1-4094>. **<A.B.C.D>** is the source address of the query operation.

Command Mode: Global mode.

Default: 0.0.0.0

Usage Guide: It is not supported on Windows 2000/XP to query with the source address as 0.0.0.0. So the layer 2 query source address configuration does not function. The client will stop sending requesting datagrams after one is sent. And after a while, it can not receive multicast datagrams.

Example:

Switch(config)#iip igmp snooping vlan 2 L2-general-querier-source 192.168.1.2

6.10.11 ip igmp snooping vlan l2-general-querier-version

Command: ip igmp snooping vlan <vlanid> L2-general-query-version <version>

Function: Configure igmp snooping.

Parameters: vlan-id is the id of the VLAN, limited to <1-4094>. **version** is the version number, limited to <1-3>.

Command Mode: Global mode.

Default: version 3.

Usage Guide: When the switch is connected to V1 and V2 capable environment, and for VLAN which has source of layer 2 query configuration, the VLAN can be queried only if the version number has been specified. This command is used to query the layer 2 version number.

Example:

Switch(config)#ip igmp snooping vlan 2 l2-general-querier-version 2

6.10.12 ip igmp snooping vlan limit

Command: ip igmp snooping vlan *<vlan-id>* limit {group *<g_limit>* | source *<s_limit>*}
no ip igmp snooping vlan *<vlan-id>* limit

Function: Configure the max group count of VLAN and the max source count of every group. The "**no ip igmp snooping vlan *<vlan-id>* limit**" command cancels this configuration.

Parameter: *<vlan-id>* is the VLAN number.

g_limit：<1-65535>, max number of groups joined.

s_limit：<1-65535>, max number of source entries in each group, consisting of include source and exclude source.

Command mode: Global Mode.

Default: Maximum 50 groups by default, with each group capable with 40 source entries.

Usage Guide: When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, IGMP snooping must be enabled on VLAN. The "no" form of this command restores the default other than set to "no limit". For the safety considerations, this command will not be configured to "no limit". It is

recommended to use default value and if layer 3 IGMP is in operation, please make this configuration in accordance with the IGMP configuration as possible.

Example: Switch(config)#ip igmp snooping vlan 2 limit group 300

6.10.13 ip igmp snooping vlan interface (ethernet | port-channel|) IFNAME limit

Command：ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit {group <1-65535>| source <1-65535>} strategy (replace | drop)

no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit group source strategy

Function： Configure the number of groups which are allowed joining and the maximum of the source in each group under the IGMP Snooping port. Configure the strategy when it is up to the upper limit, including “replace” and “drop”.

Parameters：*vlan-id*: VLAN ID range is <1-4094>

***ehternet*：** Ethernet port name

***ifname*：** Interface name

port-channel: ports aggregation

***<1-65535>*：** The maximum number of groups allowed joining

***<1-65535>*：** The maximum number of source table entries in each group, including include source and exclude source.

***replace*：** Replace the group and source information

***drop*：** Drop the new group and source information

Command mode: Global Mode.

Default: There is no limitation as default.

Usage Guide: When the number of the groups joined under the port or the number of sources in this group exceeds the limit, it will be dealt according to the configured strategy. If it is drop, drop the new group and source information; if it is replace, find a dynamic group and source from the port to conduct deleting and replacing, and then add the new group and source information. The premise of using this command is that this VLAN is enabled IGMP Snooping function. No command configures as “no limitation”.

Example：

Switch(config)#ip igmp snooping vlan 2 interface ethernet 1/0/11 limit group 300 source 200 strategy replace

Switch(config)#

6.10.14 ip igmp snooping vlan mrouter-port interface

Command: ip igmp snooping vlan <*vlan-id*> mrouter-port interface[<ehternet> | <port-channel>] <ifname>

no ip igmp snooping vlan <*vlan-id*> mrouter-port interface[<ehternet> | <port-channel>] <ifname>

Function: Configure static mrouter port of VLAN. The no form of the command cancels this configuration.

Parameter: ***vlan-id***: ranging between <1-4094>

ehternet: Name of Ethernet port

ifname: Name of interface

***port-channel*:** Port aggregation

Command Mode: Global mode

Default: No static mrouter port on VLAN by default.

Usage Guide: When a port is a static mrouter port while also a dynamic mrouter port, it should be taken as a static mrouter port. Deleting static mrouter port can only be realized by the no command.

Example: Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/0/13

6.10.15 ip igmp snooping vlan mrouter-port learnpim

Command: ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim

no ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim

Function: Enable the function that the specified VLAN learns mrouter-port (according to pim packets), the no command will disable the function.

Parameter: <*vlan-id*>: The specified VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode

Default: Enable

Usage Guide: Enable the function that the specified VLAN learns mrouter-port (according to pim packets). After a port received pim packets, it will be set to mrouter port for implementing the automatic learning.

Example: Disable the function that vlan 100 learns mrouter-port (according to pim packets).

Switch(config)#no ip igmp snooping vlan 100 mrouter-port learnpim

6.10.16 ip igmp snooping vlan mrpt

Command: ip igmp snooping vlan <*vlan-id*> mrpt <*value*>

no ip igmp snooping vlan <*vlan-id*> mrpt

Function: Configure this survive time of mrouter port.

Parameter: ***vlan-id*:** VLAN ID, ranging between <1-4094>

***value*:** mrouter port survive period, ranging between <1-65535>seconds

Command Mode: Global mode

Default: 255s

Usage Guide: This command validates on dynamic mrouter ports but not on mrouter port. To use this command, IGMP Snooping of this VLAN should be enabled previously.

Example: Switch(config)#ip igmp snooping vlan 2 mrpt 100

6.10.17 ip igmp snooping vlan query-interval

Command: ip igmp snooping vlan <*vlan-id*> query-interval <*value*>

no ip igmp snooping vlan <*vlan-id*> query-interval

Function: Configure this query interval.

Parameter: ***vlan-id***: VLAN ID, ranging between <1-4094>

value: query interval, ranging between <1-65535>seconds

Command Mode: Global mode

Default: 125s

Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example: Switch(config)#ip igmp snooping vlan 2 query-interval 130

6.10.18 ip igmp snooping vlan query-mrsp

Command: ip igmp snooping vlan <*vlan-id*> query-mrsp <*value*>

no ip igmp snooping vlan <*vlan-id*> query-mrsp

Function: Configure the maximum query response period. The "**no ip igmp snooping vlan <*vlan-id*> query-mrsp**" command restores to the default value.

Parameter: ***vlan-id***: VLAN ID, ranging between <1-4094>

value: ranging between <1-25> seconds

Command Mode: Global mode

Default: 10s

Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example:

Switch(config)#ip igmp snooping vlan 2 query-mrsp 18

6.10.19 ip igmp snooping vlan query-robustness

Command: ip igmp snooping vlan <vlan-id> query-robustness <*value*>

no ip igmp snooping vlan <vlan-id> query-robustness

Function: Configure the query robustness. The "**no ip igmp snooping vlan <vlan-id> query-robustness**" command restores to the default value.

Parameter: ***vlan-id***: VLAN ID, ranging between <1-4094>

value: ranging between <2-10>

Command Mode: Global mode

Default: 2

Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example:

Switch(config)#ip igmp snooping vlan 2 query- robustness 3

6.10.20 ip igmp snooping vlan report source-address

Command: ip igmp snooping vlan *<vlan-id>* report source-address *<A.B.C.D>*

no ip igmp snooping vlan *<vlan-id>* report source-address

Function: Configure forward report source-address for IGMP, the "**no ip igmp snooping vlan *<vlan-id>* report source-address**" command restores the default setting.

Parameter: *vlan-id*: VLAN ID range<1-4094>;

***A.B.C.D*:** IP address, can be 0.0.0.0.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: Default configuration is recommended here. If IGMP snooping needs to be configured, the source address for forwarded IGMP messages can be 0.0.0.0. If it is required by the upstream that IGMP messages should use the same network address, the source address of IGMP messages should be configured to be the same with upstream.

Example:

Switch (config)#ip igmp snooping vlan 2 report source-address 10.1.1.1

6.10.21 ip igmp snooping vlan specific-query-mrsp

Command: ip igmp snooping vlan <vlan-id> specific-query-mrsp <value>

no ip igmp snooping vlan <vlan-id> specific-query-mrspt

Function: Configure the maximum query response time of the specific group or source, the no command restores the default value.

Parameters: <vlan-id>: the specific VLAN ID, the range from 1 to 4094.

<value>: the maximum query response time, unit is second, the range from 1 to 25, default value is 1.

Command Mode: Global mode

Default: Enable the function.

Usage Guide: After enable vlan snooping in global mode, input this command to configure the maximum query response time of the specific group.

Example: Configure/cancel the specific-query-mrsp of vlan3 as 2s.

Swith(config)#ip igmp snooping vlan 3 specific-query-mrsp 2

Swith(config)#no ip igmp snooping vlan 3 specific-query-mrspt

6.10.22 ip igmp snooping vlan static-group

Command: ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>

no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>]interface [ethernet | port-channel] <IFNAME>

Function: Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.

Parameter: ***vlan-id***: ranging between <1-4094>

A.B.C.D: the address of group or source

ethernet: Name of Ethernet port

port-channel: Port aggregation

ifname: Name of interface

Command Mode: Global mode

Default: No configuration by default.

Usage Guide: When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.

Example:

Switch(config)#ip igmp snooping vlan 1 static-group 224.1.1.1 source 192.168.1.1 interface ethernet 1/0/1

6.10.23 ip igmp snooping vlan passthrough-group

Command：ip igmp snooping vlan <*vlan-id*> passthrough-group <A.B.C.D>

no ip igmp snooping vlan <*vlan-id*> passthrough-group <A.B.C.D>

Function： Configure transparent transmission group, no operation restores default value

Command ： *vlan-id*: VLAN ID Value range<1-4094>

A.B.C.D： IP address。

Command mode： Global Mode。

Default： Do not configure transparent transmission group

Usage Guide： The group configured for transparent transmission will forward the corresponding multicast traffic to all ports within the VLAN

Examples：

Switch(config)#ip igmp snooping vlan 1 passthrough-group 224.1.1.1

6.10.24 ip igmp snooping vlan not-forward

Command: ip igmp snooping vlan <*vlan-id*> not-forward

no ip igmp snooping vlan <*vlan-id*> not-forward

Function: Configure multicast traffic not to be forwarded to the mroute port, The no form of the command cancels this configuration.

Parameter: ***vlan-id*:** VLAN ID, ranging between <1-4094>.

Command Mode: Global mode

Default: No configuration by default.

Usage Guide: After enabling the not forward feature, all multicast traffic will no longer be forwarded to the mroute port.

Example:

Switch(config)#ip igmp snooping vlan 1 not-forward

6.10.25 ip igmp snooping vlan suppression-query-time

Command: ip igmp snooping vlan <*vlan-id*> suppression-query-time <*value*>

no ip igmp snooping vlan <*vlan-id*> suppression-query-time

Function: Configure the suppression query time. The "**no ip igmp snooping vlan <*vlan-id*> suppression-query-time**" command restores to the default value.

Parameter: ***vlan-id***: VLAN ID, ranging between <1-4094>

value: ranging between<1-65535> seconds

Command Mode: Global mode

Default: 255s

Usage Guide: This command can only be configured on L2 general querier. The Suppression-query-time refers to the period of suppression state in which the querier enters when receives query from the layer 3 IGMP in the segments.

Example: Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270

6.10.26 show ip igmp snooping

Command: show ip igmp snooping [vlan <*vlan-id*>]

Parameter: <*vlan-id*> is the VLAN number specified for displaying IGMP Snooping messages.

Command Mode: Admin Mode

Usage Guide: If no VLAN number is specified, it will show whether global IGMP Snooping switch is on, which VLAN is configured with l2-general-querier function, and if a VLAN number is specified, detailed IGMP messages for this VLAN will be shown.

Example:

1. Show IGMP Snooping summary messages of the switch

```
 Switch(config)#show ip igmp snooping
Global igmp snooping status:    Enabled
L3 multicasting:                running
Igmp snooping is turned on for vlan 1(querier)
Igmp snooping is turned on for vlan 2
---------------------------------
```

Displayed Information	Explanation
Global igmp snooping status	Whether the global igmp snooping switch on the switch is on
L3 multicasting	whether the layer 3 multicast protocol of the switch is running
Igmp snooping is turned on for vlan 1(querier)	which VLANs on the switch is enabled with igmp snooping function, whether they are l2-general-querier

2. Display the IGMP Snooping summary messages of vlan1.

```
Switch#show ip igmp snooping vlan 1
Igmp snooping information for vlan 1

Igmp snooping L2 general querier                    :Yes(COULD_QUERY)
Igmp snooping query-interval                        :125(s)
Igmp snooping max reponse time                      :10(s)
Igmp snooping robustness                            :2
Igmp snooping mrouter port keep-alive time          :255(s)
Igmp snooping query-suppression time                :255(s)

IGMP Snooping Connect Group Membership
Note:*-All Source, (S)- Include Source, [S]-Exclude Source
Groups          Sources          Ports              Exptime    System Level
238.1.1.1       (192.168.0.1)    Ethernet1/1/8      00:04:14   V2
                (192.168.0.2)    Ethernet1/1/8      00:04:14   V2

Igmp snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/1/2
```

Displayed Information	Explanation
Igmp snooping L2 general querier	Whether the VLAN enables l2-general-querier function and show whether the querier state is could-query or suppressed
Igmp snooping query-interval	Query interval of the VLAN
Igmp snooping max reponse time	Max response time of the VLAN
Igmp snooping robustness	IGMP Snooping robustness configured on the VLAN
Igmp snooping mrouter port keep-alive time	keep-alive time of dynamic mrouter of the VLAN
Igmp snooping query-suppression time	Suppression timeout of VLAN when as l2-general-querier
IGMP Snooping Connect Group Membership	Group membership of this VLAN, namely the correspondence between ports and (S,G)
Igmp snooping vlan 1 mrouter port	mrouter port of the VLAN, including both static and dynamic

6.11 IGMP Proxy

6.11.1 clear ip igmp proxy agggroup

Command: clear ip igmp proxy agggroup

Function: Delete all group records.

Parameters: None.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

Switch#clear ip igmp proxy agggroup

Relative Command: show ip igmp proxy upstream group

6.11.2 debug igmp proxy all

Command: debug igmp proxy all

no debug igmp proxy all

Function: Enable all the debugging switches of IGMP Proxy; the "**no debug igmp proxy all**" command disenables all the debugging switches.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use to enable debugging switches of IGMP Proxy, it can display IGMP packet, event, timer, mfc, which disposed in the switch.

Example:

Switch# debug igmp proxy all

6.11.3 debug igmp proxy event

Command: debug igmp proxy event

no debug igmp proxy event

Function: Enable/Disable debug switch of IGMP Proxy event.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: Enable debugging switch if querying event information of IGMP Proxy.

Example:

Switch# debug igmp proxy event

6.11.4 debug igmp proxy mfc

Command: debug igmp proxy mfc

no debug igmp proxy mfc

Function: Enable/Disable debug switch of IGMP Proxy multicast forwarding cache.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: Enable IGMP Proxy mfc debug switch and display multicast information created and distributed.

Example:

Switch# debug igmp proxy mfc

6.11.5 debug igmp proxy packet

Command: debug igmp proxy packet

no debug igmp proxy packet

Function: Enable/Disable debug switch of IGMP Proxy.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: Enable the debugging switch, you can monitor the packets receiving/sending of IGMP Proxy.

Example:

Switch# debug igmp proxy packet

6.11.6 debug igmp proxy timer

Command: debug igmp proxy timer

no debug igmp proxy timer

Function: Enable/Disable each timer of IGMP Proxy.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: The command is used for enable the IGMP Proxy timer debugging switch which appointed.

Example:

Switch# debug ip igmp proxy timer

6.11.7 ip igmp proxy

Command: ip igmp proxy

no ip igmp proxy

Function: Enable the IGMP Proxy function; the "**no ip igmp proxy**" command disables this function.

Command Mode: Global Mode.

Default: The switch disables IGMP Proxy by default.

Usage Guide: Use this command to enable IGMP Proxy, and configure one upstream port and at least one downstream port under interface configuration mode if make the IGMP Proxy operate.

Example: Enable IGMP Proxy under Global Mode.

Switch (config)#ip igmp proxy

6.11.8 ip igmp proxy aggregate

Command: ip igmp proxy aggregate

no ip igmp proxy aggregate

Function: To configure non-query downstream ports to be able to aggregate the IGMP operations.

Command Mode: Global Mode.

Default: The non-query downstream ports are not to be able to aggregate the IGMP operations in default.

Usage Guide: By default non-query downstream ports cannot aggregate and redistribute the multicast messages. This command is used to enable all the downstream ports to be able to aggregate and redistribute the multicast dataflow.

Example:

Switch(config)#ip igmp proxy aggregate

6.11.9 ip igmp proxy downstream

Command: ip igmp proxy downstream

no ip igmp proxy downstream

Function: Enable the appointed IGMP Proxy downstream port function; the "**no ip igmp proxy upstream**" disables this function.

Command Mode: Interface Configuration Mode.

Default: Disabled.

Usage Guide: To configure the interface to function as the downstream port of IGMP Proxy. In order to make IGMP Proxy work, at least one upstream interface should be configured. The "**no ip igmp proxy downstream**" command will disable the configuration.

Example: Enable IGMP Proxy downstream port function in interface VLAN2 under interface configuration mode.

Switch (config)#interface vlan 2

Switch(Config-if-Vlan2)#ip igmp proxy downstream

6.11.10 ip igmp proxy limit

Command: ip igmp proxy limit {group <*g_limit*> | source <*s_limit*>}

no ip igmp proxy limit

Function: To configure the maximum number of groups that upstream ports can join, and the maximum number of sources in a single group.

Parameter: *g_limit*: <1-500>, the group number limitation.

***s_limit*:** <1-500>, the source number limitation.

Command Mode: Global Mode.

Default: Most 50 groups in default, and most 40 sources in one group.
Usage Guide: If the group number limitation is exceeded, new group membership request will be rejected. This command is used to prevent malicious group membership requests.
Example:
Switch(config)#ip igmp proxy limit group 30 source 20

6.11.11 ip igmp proxy multicast-source

Command: ip igmp proxy multicast-source
no ip igmp proxy multicast-source
Function: To configure the port as downstream port for the source of multicast datagram; the no from of this command disables the configuration.
Command Mode: Interface Configuration Mode.
Default: The downstream port is not for the source of multicast datagram.
Usage Guide: When a downstream port is configured as the multicast source port, the switch will be able to receive multicast data flow from that port, and forward it to the upstream port. To make this command function, the multicast router which is connected to the upstream port of the switch, should be configured to view the multicast source from the upstream port is directly connected to the router.
Example: Enable **igmp proxy multicast-source** in downstream port VLAN1.
Switch (config)#interface vlan 1
Switch (Config-if-Vlan1)#ip igmp proxy multicast-source

6.11.12 ip igmp proxy unsolicited-report interval

Command: ip igmp proxy unsolicited-report interval <*value*>
no ip igmp proxy unsolicited-report interval
Function: To configure how often the upstream ports send out unsolicited report.
Parameter: The interval is between 1 to 5 seconds for the upstream ports send out unsolicited report.
Command Mode: Global Mode.
Default: The interval is 1 second for the upstream ports send out unsolicited report in default.
Usage Guide: The upstream ports re-transmit the unsolicited reports in order that the router will not miss the report packet due to link down or packet loss. This command configures the interval for re-transmission.
Example:
Switch(config)#ip igmp proxy unsolicited-report interval 3

6.11.13 ip igmp proxy unsolicited-report robustness

Command: ip igmp proxy unsolicited-report robustness <*value*>
no ip igmp proxy unsolicited-report robustness
Function: To configure the retry times of upstream ports' sending unsolicited reports. **Parameter:**

***value*:** <2~10>. The retry time for upstream ports' sending unsolicited report is limited between 2 and 10.

Command Mode: Global Mode.

Default: Retry time is 2 by default.

Usage Guide: The upstream ports re-transmit the unsolicited reports in order that the router will not miss the report packet due to link down or packet loss.

Example:

Switch(config)#ip igmp proxy unsolicited-report robustness 3

6.11.14 ip igmp proxy upstream

Command: ip igmp proxy upstream

no ip igmp proxy upstream

Function: Enable the appointed IGMP Proxy upstream port function. The "**no ip igmp proxy upstream**" disables this function.

Command Mode: Interface Configuration Mode.

Default: Disabled.

Usage Guide: To configure the interface to function as the upstream port of IGMP Proxy. In order to make IGMP Proxy work, at least one downstream interface should be configured. The "**no ip igmp proxy upstream**" command will disable the configuration.

Example: Enable IGMP Proxy upstream port function in interface VLAN1 under interface configuration mode.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp proxy upstream

6.11.15 ip multicast ssm

Command: ip multicast ssm {range *<access-list-number>* | default}

no ip multicast ssm

Function: To configure the address range for IGMP Proxy ssm multicast groups; the no form of this command will delete the ssm multicast groups.

Parameter: default: show the address range 232/8 for ssm multicast groups.

<access-list-number> is the applied access list number, range is 1-99.

Command Mode: Global Mode.

Default: The default address range is 232/8 for ssm multicast groups.

Usage Guide: The command configures the address filter for multicast group membership request. The request for the specified address ranges will be dropped. This command is also available for both the IGMP PROXY and PIM configuration. To be mentioned, this command cannot be applied with DVMRP configuration.

Example: To enable SSM configuration on the switch, and specify the address in access-list 23 as the filter address for SSM.

Switch(config)# access-list 23 permit host-source 224.1.1.1

Switch(config)#ip multicast ssm range 23

6.11.16 ip pim bsr-border

Command: ip pim bsr-border

no ip pim bsr-border

Function: To configure the PIM enabled port to consider all multicast source is directly connected; the no form of this command will remove the configuration.

Command Mode: Interface Configuration Mode.

Default: Disabled.

Usage Guide: Configuring the multicast source to be considered as directly connected for the PIM enabled port is used to determine the identity of DR and ORIGINATOR.

Example: To configure PIM enabled VLAN 2 as the port for BSR BORDER. For all the multicast flow from external network through VLAN 2, the switch will consider the multicast source is directly connected to the switch.

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ip pim bsr-border

6.11.17 show debugging igmp proxy

Command: show debugging igmp proxy

Function: Display the status of debug switch of IGMP Proxy.

Command Mode: Admin Mode.

Usage Guide: The debuging switch status of IGMP Proxy.

Example:

Switch(config)#show debugging igmp proxy

IGMP PROXY debugging status:

IGMP PROXY event debugging is on

IGMP PROXY packet debugging is on

IGMP PROXY timer debugging is on

IGMP PROXY mfc debugging is on

6.11.18 show ip igmp proxy

Command: show ip igmp Proxy

Function: Display the IGMP Proxy configuration information.

Command Mode: Admin Mode.

Usage Guide: To show configuration for **igmp proxy** about whether the **igmp proxy** is enabled globally, and whether upstream ports and downstream ports has been configured.

Example:

Switch(config)#show ip igmp Proxy

```
IGMP PROXY MRT running: Enabled
  Total active interface number: 2

Global igmp proxy configured: YES
Total configured interface number: 2
Upstream Interface configured: YES
    Upstream Interface Vlan1(2005)
Upstream Interface configured: YES
    Downstream Interface Vlan2(2006)
  --------------------------------
```

Show Information	Explanation
IGMP PROXY MRT running	Whether the protocol is running
Total active interface number	Number of active upstream and downstream ports
Global igmp proxy configured	Whether global igmp proxy is enabled
Upstream Interface configured	Whether upstream port is configured
Upstream Interface Vlan	The VLAN which the upstream port belongs to
Upstream Interface configured	Whether downstream port is configured
Downstream Interface Vlan	The VLAN which the downstream port belongs to

6.11.19 show ip igmp proxy mroute

Command: show ip igmp Proxy mroute

Function: Display the status information of **igmp proxy mroute**.

Command Mode: Admin Mode.

Usage Guide: Display the status information of **igmp proxy mroute**, and information about the mrt node.

Example:

```
Switch(config)#show ip igmp proxy mroute

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 2

(1.1.1.2, 225.0.0.1)
  Local_include_olist       ..l.....................
  Local_exclude_olist       .....................
  Outgoing                   ..o.....................

(1.1.1.3, 225.0.0.1)
  Local_include_olist       ..l.....................
  Local_exclude_olist       .....................
```

Outgoing ..o.....

Show Information	Explanation
Entries	The counts of each item
Local_include_olist	index for local include olist
Local_exclude_olist	index for local exclude olist
Outgoing	Final outgoing index of multicast data(S, G)

6.11.20 show ip igmp proxy upstream groups

Command: show ip igmp proxy upstream groups {A.B.C.D}

Command Mode: Admin Mode.

Usage Guide: To show the group membership information of the upstream port. If the group is not specified, information of all groups will be displayed, otherwise, only the specified will be displayed.

Example:

Switch(config)#show ip igmp proxy upstream groups

IGMP PROXY Connect Group Membership

Groups	Filter-mode	source
224.1.1.1	INCLUDE	192.168.1.136
226.1.1.1	*	

Show Information	Explanation
Groups	IP addresses of multicast groups
Filter-mode	Filter-mode of the multicast group
source	Source hold by the multicast group

6.12 Multicast VLAN

6.12.1 multicast-vlan

Command: multicast-vlan

no multicast-vlan

Function: Enable multicast VLAN function on a VLAN; the “no” form of this command disables the multicast VLAN function.

Parameter: None.

Command Mode: VLAN Configuration Mode.

Default: Multicast VLAN function not enabled by default.

Usage Guide: The multicast VLAN function can not be enabled on Private VLAN. To disabling the multicast VLAN function of the VLAN, configuration of VLANs associated with the multicast VLAN should be deleted. Note that the default VLAN can not be configured with this command and only one multicast VLAN is allowed on a switch.

Examples:

Switch(config)#vlan 2

Switch(Config-Vlan2)# multicast-vlan

6.12.2 multicast-vlan association

Command: multicast-vlan association *<vlan-list>*

no multicast-vlan association *<vlan-list>*

Function: Associate several VLANs with a multicast VLAN; the "no" form of this command cancels the association relations.

Parameter: *<vlan-list>* the VLAN ID list associated with multicast VLAN. Each VLAN can only be associated with one multicast VLAN and the association will only succeed when every VLAN listed in the VLAN ID table exists.

Command Mode: VLAN Mode.

Default: The multicast VLAN is not associated with any VLAN by default.

Usage Guide: After a VLAN is associated with the multicast VLAN, when there comes the multicast order in the port of this VLAN, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. The VLAN associated with the multicast VLAN should not be a Private VLAN. A VLAN can only be associated with another VLAN after the multicast VLAN is enabled. Only one multicast VLAN can be enabled on a switch.

Examples:

Switch(config)#vlan 2

Switch(Config-Vlan2)# multicast-vlan association 3, 4

6.12.3 multicast-vlan association interface

Command: multicast-vlan association interface (ethernet | port-channel|) IFNAME

no *multicast-vlan* association interface (ethernet | port-channel|) IFNAME

Function: Associate the specified port with the multicast VLAN, so the associated ports are able to receive the multicast flow. The no command cancels the association between the ports and the multicast VLAN.

Parameter: IFNAME: The name of the ethernet port or port-channel port

Command Mode: VLAN configuration mode

Default: None.

Usage Guide:

1. 'associated VLAN' and 'associated port' of the multicast VLAN are absolute, they do not affect each other when happening the cross.

2. The port of the aggregation member cannot be associated, but the associated

port is able to be added to port-group and cancelling the association.

3. The configured port type includes port-channel port or ethernet port and the port is only configured as ACCESS mode.

4. The port (it will be associated) cannot belong to the multicast VLAN, in the same way, the associated port cannot be divided in multicast VLAN.

5. When the associated port mode is set as non ACCESS mode, the mode cannot be changed.

Example: Suppose vlan2 is multicast VLAN.

Switch(config-vlan2)#multicast-vlan association interface ethernet 1/0/2

Switch(config-vlan2)#multicast-vlan association interface port-channel 2

Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/0/2

Switch(config-vlan2)#no multicast-vlan association interface port-channel 2

6.12.4 multicast-vlan mode

Command: multicast-vlan mode {dynamic| compatible}

no multicast-vlan mode {dynamic| compatible}

Function: This command is used to configure the two modes of the multicast vlan; the no command cancels this configuration.

Parameters: dynamic: dynamic mode;

compatible: compatible mode.

Command mode: VLAN configuration mode.

Default: Neither of the two modes.

Usage Guide: When configured as dynamic mode, the mrouter port will not be added automatically any mort when issuing the multicast entries; when configured as compatible mode, the report packet will be not transmitted to the mrouter port any more. When it is not configured as default, the mrouter port will be added when issuing the multicast entries and the report packet will be transmitted to the mrouter port when it is received.

Example:

Switch(Config-Vlan2)#multicast vlan mode dynamic

Switch(Config-Vlan2)#

6.12.5 switchport association multicast-vlan

Command: switchport association multicast-vlan <vlan-id> out-tag <tag-id>

no switchport association multicast-vlan <vlan-id>

Function: Associate a port with a specified multicast VLAN; The 'no' operation of this command cancels the association relationship.

Parameters: <vlan-id>is a multicast VLAN associated with a port, and each port can only be associated with one multicast VLAN. The association will only be successful if the multicast VLAN does exist.

<tag id>, with a value range of<1-4094>, specifies the VLAN tag carried by multicast data forwarded from this associated port. This tag id will only take effect if the associated port tag

allows the multicast VLAN.

Command mode: Interface Configuration Mode.

Default: this port is not associated with any multicast VLAN.

Usage Guide: If a port is associated with a multicast VLAN, it is added to the multicast VLAN. If this port requests traffic from the multicast source of the multicast VLAN, multicast data will be sent from the multicast VLAN to this port without configuring the incoming port of the traffic as a trunk port, thereby reducing multicast replication. If the associated port is a trunk port and the multicast VLAN is allowed, the multicast traffic will be forwarded with the VLAN tag specified in this command. The function of associating multicast VLANs with trunk ports can support the downstream port's need to connect to the downstream on-demand end through a layer 2 network, without being limited to the downstream port's requirement to directly connect to the on-demand end. Only after configuring the multicast VLAN function can the associated ports be configured.

Example:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)#multicast-vlan
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport mode trunk
Switch(config-if-ethernet1/0/1)#switchport association multicast-vlan 2 out-tag 5
```

Chapter 7 Commands for Security Function

7.1 ACL

7.1.1 absolute-periodic/periodic

Command: [no] absolute-periodic {Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<start_time>to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday} <end_time>

[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily| weekdays | weekend} <start_time> to <end_time>

Functions: Define the time-range of different commands within one week, and every week to circulate subject to this time.

Parameters:

Friday （Friday)

Monday （Monday)

Saturday （Saturday)

Sunday （Sunday)

Thursday （Thursday）

Tuesday （Tuesday)

Wednesday （Wednesday)

daily （Every day of the week）

weekdays （Monday thru Friday）

weekend （Saturday thru Sunday）

start_time start time ,HH:MM:SS (hour: minute: second)

end_time end time,HH:MM:SS (hour: minute: second)

Remark: time-range polling is one minute per time, so the time error shall be <= one minute.

Command Mode: time-range mode

Default: No time-range configuration.

Usage Guide: Periodic time and date. The definition of period is specific time period of Monday to Saturday and Sunday every week.

day1 hh:mm:ss To day2 hh:mm:ss or {[day1+day2+day3+day4+day5+day6+day7]|weekend|weekdays|daily} hh:mm:ss To hh:mm:ss

Examples: Make configurations effective within the period from9:15:30 to 12:30:00 during Tuesday to Saturday.

Switch(config)#time-range dc_timer

Switch(Config-Time-Range-dc_timer)#absolute-periodic Tuesday 9:15:30 to Saturday 12:30:00

Make configurations effective within the period from 14:30:00 to 16:45:00 on Monday, Wednesday, Friday and Sunday.

Switch(Config-Time-Range-dc_timer)#periodic Monday Wednesday Friday Sunday 14:30:00 to 16:45:00

7.1.2 absolute start

Command: [no] absolute start *<start_time> <start_data>* [end *<end_time> <end_data>*]

Functions: Define an absolute time-range, this time-range operates subject to the clock of this equipment.

Parameters: *start_time* : start time, HH:MM:SS (hour: minute: second)

***end_time* :** end time, HH:MM:SS (hour: minute: second)

***start_data* :** start data, the format is, YYYY.MM.DD （ year.month.day ）

***end_data* :** end data, the format is, YYYY.MM.DD（year.month.day）

Remark: time-range is one minute per time, so the time error shall be <= one minute.

Command Mode: Time-range mode

Default: No time-range configuration.

Usage Guide: Absolute time and date, assign specific year, month, day, hour, minute of the start, shall not configure multiple absolute time and date, when in repeated configuration, the latter configuration covers the absolute time and date of the former configuration.

Examples: Make configurations effective from 6:00:00 to 13:30:00 from Oct. 1, 2004 to Jan. 26, 2005.

Switch(config)#Time-range dcn_timer

Switch(Config-Time-Range-dcn_timer)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26

7.1.3 access-list deny-preemption

Command: [no] access-list deny-preemption

Function: Enable deny-preemption function, the no command disables deny-preemption function.

Parameters: None.

Command Mode: Global Mode.

Default: Enable deny-preemption.

Usage Guide: Enable deny-preemption function to ensure the preemptive rule of deny action between ACL module and other modules, but it limits the number of ACL rules. firewall must be enabled before using this command. if ACL has been sent to hardware, this command takes effect after resetting firewall.

Attention: No access-list deny-preemption command not support by the switch.

7.1.4 access-list (ip extended)

Command: access-list *<num>* {deny | permit} icmp {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<icmp-type>* [*<icmp-code>*]] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]

access-list *<num>* {deny | permit} igmp {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<igmp-type>*] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]

access-list *<num>* {deny | permit} tcp {{ *<sIpAddr>* *<sMask>* } | any-source | {host-source *<sIpAddr>* }} [s-port { *<sPort>* | range *<sPortMin>* *<sPortMax>* }] {{ *<dIpAddr>* *<dMask>* } | any-destination | {host-destination *<dIpAddr>* }} [d-port { *<dPort>* | range *<dPortMin>* *<dPortMax>* }] [ack+ fin+ psh+ rst+ urg+ syn] [precedence *<prec>*] [tos *<tos>*][time-range *<time-range-name>*]

access-list <num> {*deny* / permit} udp *{{* <sIpAddr> *<sMask> }* | any-source | {host-source *<sIpAddr>* }} [s-port *{ <sPort>* | range *<sPortMin>* *<sPortMax>*] {{ <dIpAddr> *<dMask> }* | any-destination | *{host-destination* <dIpAddr> *}} [d-port* { <dPort> / range <dPortMin> *<dPortMax>* }] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]

access-list *<num>* {deny / permit} {eigrp | *gre* / *igrp* / ipinip | ip | ospf | *<protocol-num>* } {{ *<sIpAddr>* <sMask> } / any-source / *{*host-source <sIpAddr> *}} {{ <dIpAddr>* <dMask> } | *any-destination* / {host-destination <dIpAddr> }} *[precedence <prec>*] *[tos* <tos>][time-range *<time-range-name>]*

no access-list *<num>*

Functions: Create a numeric extended IP access rule to match specific IP protocol or all IP protocol; if access-list of this coded numeric extended does not exist, thus to create such a access-list.

Parameters: ***<num>*** is the No. of access-list, 100-299; ***<protocol>*** is the No. of upper-layer protocol of ip, 0-255; ***<sIpAddr>*** is the source IP address, the format is dotted decimal notation; ***<sMask >*** is the reverse mask of source IP, the format is dotted decimal notation; ***<dIpAddr>*** is the destination IP address, the format is dotted decimal notation; ***<dMask>*** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position1;***<igmp-type>***,the type of igmp, 0-255; ***<icmp-type>***, the type of icmp, 0-255;**<icmp-code>,** protocol No. of icmp, 0-255;**<prec>**, IP priority, 0-7; ***<tos>***, to value, 0-15; ***<sPort>***, source port No., 0-65535; ***<sPortMin>***, the down boundary of source port; ***<sPortMax>***, the up boundary of source port; ***<dPortMin>***, the down boundary of destination port; ***<dPortMax>***, the up boundary of destination port; ***<dPort>***, destination port No., 0-65535; ***<time-range-name>***, the name of time-range.

Command Mode: Global mode

Default: No access-lists configured.

Usage Guide: When the user assign specific ***<num>*** for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 200-299 can configure not continual reverse mask of IP address.

<igmp-type> represent the type of IGMP packet, and usual values please refer to the following description:

17(0x11): IGMP QUERY packet

18(0x12): IGMP V1 REPORT packet
22(0x16): IGMP V2 REPORT packet
23(0x17): IGMP V2 LEAVE packet
34(0x22): IGMP V3 REPORT packet
19(0x13): DVMR packet
20(0x14): PIM V1 packet

Particular notice: The packet types included here are not the types excluding IP OPTION. Normally, IGMP packet contains OPTION fields, and such configuration is of no use for this type of packet. If you want to configure the packets containing OPTION, please directly use the manner where OFFSET is configured.

Examples: Create the numeric extended access-list whose serial No. is 110. deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

Switch(config)#access-list 110 deny icmp any any-destination
Switch(config)#access-list 110 permit udp any host-destination 192.168.0.1 d-port 32

7.1.5 access-list (ip standard)

Command: access-list *<num>* {deny | permit} {{*<sIpAddr>* *<sMask* >} | any-source| {host-source *<sIpAddr>*}}

no access-list *<num>*

Functions: Create a numeric standard IP access-list. If this access-list exists, then add a rule list; the "**no access-list *<num>***" operation of this command is to delete a numeric standard IP access-list.

Parameters: *<num>* is the No. of access-list, 100-199; ***<sIpAddr>*** is the source IP address, the format is dotted decimal notation; ***<sMask >*** is the reverse mask of source IP, the format is dotted decimal notation.

Command Mode: Global mode

Default: No access-lists configured.

Usage Guide: When the user assign specific ***<num>*** for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Create a numeric standard IP access-list whose serial No. is 20, and permit date packets with source address of 10.1.1.0/24 to pass, and deny other packets with source address of 10.1.1.0/16.

Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255
Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255

7.1.6 access-list(mac extended)

Command: access-list *<num>* {deny | permit} {any-source-mac | {host-source-mac *<host_smac>*} | *{<smac>* *<smac-mask>*}} {any-destination-mac | {host-destination-mac *<host_dmac>*} | *{<dmac>* *<dmac-mask>*}} {untagged-eth2 | tagged-eth2 | untagged-802-3 | tagged-802-3} [*<offset1>* *<length1>* <value1> [*<offset2>* *<length2>* <value2> [<offset3>

<length3> <value3> [*<offset4> <length4> <value4>*]]]]]

no *access-list* <num>

Functions*: Define an extended *numeric* MAC *ACL* rule, 'no access-list <num>' command deletes an extended numeric *MAC access-list rule.

Parameters:* <num> is the** access-list No. which is a decimal's No. from 1100-1199; **deny** if rules are matching, deny access; **permit** if rules are matching, permit access; ***<any-source-mac> any source address; ***<any-destination-mac>*** any destination address; ***<host_smac>, <smac>*** source MAC address; ***<smac-mask>*** mask (reverse mask) of source MAC address; ***<host_dmac> , <dmac>*** destination MAC address; ***<dmac-mask>*** mask (reverse mask) of destination MAC address; **untagged-eth2** format of untagged ethernet II packet; **tagged-eth2** format of tagged ethernet II packet; **untagged-802-3** format of untagged ethernet 802.3 packet; **tagged-802-3** format of tagged ethernet 802.3 packet. Offset**(x)** the offset from the packet head, the range is (12-79), the windows must start from the back of source MAC, and the windows cannot superpose each other, and that is to say: Offset(x＋1) must be longer than Offset(x)＋len（x）; **Length(x)** length is 1-4, and **Offset(x)＋Length(x)** should not be longer than 80（currently should not be longer than 64）; ***Value(x)*** hex expression, **Value range**: when **Length(x)** =1, it is 0-ff, when **Length(x)** =2, it is 0-ffff , when **Length(x)** =3, it is0-ffffff, when **Length(x)** =4, it is 0-ffffffff ;

For Offset(*x),* different types of data frames are with different value ranges:

for untagged-eth2 type frame: <12～75>

for untagged-802.2 type frame**: *<20～75>***

for untagged-eth2 type frame: <12～79>

for untagged-eth2 type frame: <12～15> <24～79>

Command Mode: Global mode

Default Configuration: No access-list configured

Usage Guide*: When* the user assign specific <num> for the first time, ACL of **the** serial number is created, then the lists are added into this ACL.

Examples: Permit tagged-eth2 with any **source** MAC addresses and any destination MAC addresses and the packets whose 17th and 18th byte is 0x08, 0x0 to pass.

Switch(config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 16 2 0800

7.1.7 access-list(mac-ip extended)

Command:

access-list<*num*>{deny|permit}{any-source-mac|
{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}
{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp
{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}
{{<*destination*><*destination-wildcard*>}|any-destination|
{host-destination<*destination-host-ip*>}}[<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]
access-list<*num*>{deny|permit}{any-source-mac|
{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}

{any-destination-mac|{host-destination-mac *<host_dmac>*}|{*<dmac><dmac-mask>*}}igmp {{*<source><source-wildcard>*}|any-source|{host-source*<source-host-ip>*}} {{*<destination><destination-wildcard>*}|any-destination| {host-destination*<destination-host-ip>*}} [*<igmp-type>*] [precedence *<precedence>*] [tos *<tos>*][time-range*<time-range-name>*]

access-list *<num>* {deny|permit}{any-source-mac| {host-source-mac *<host_smac>* }|{ *<smac> <smac-mask>* }}{any-destination-mac| {host-destination-mac *<host_dmac>* }|{ *<dmac> <dmac-mask>* }}tcp {{ *<source> <source-wildcard>* }|any-source| {host-source *<source-host-ip>* }}[s-port{ *<port1>* | range *<sPortMin> <sPortMax>* }] {{ *<destination>* <destination-wildcard> } | any-destination | {host-destination <destination-host-ip> }} [d-port { *<port3>* | range *<dPortMin> <dPortMax>* }] [ack+fin+psh+rst+urg+syn] [precedence *<precedence>*] [tos *<tos>*] [time-range *<time-range-name>*]

access-list <num> *{deny*|permit}{any-source-mac| *{host-source-mac* <host_smac> *}|{* <*smac> <smac-mask>* }}{any-destination-mac| {host-destination-mac *<host_dmac>* }|{ *<dmac> <dmac-mask>* }}udp {{ *<source> <source-wildcard>* }|any-source| {host-source *<source-host-ip>* }}[s-port{ *<port1>* | range *<sPortMin> <sPortMax>* }] {{ <destination> *<destination-wildcard>* }|any-destination*/ {host-destination* <destination-host-ip> *}}[d-port{* <port3> *| range* <dPortMin> *<dPortMax>* }] [precedence *<precedence>*] [tos *<tos>*][time-range *<time-range-name>*]

access-list *<num>* {deny|permit}{any-source-mac| {host-source-mac *<host_smac>* }|{ *<smac> <smac-mask>* }} {any-destination-mac|{host-destination-mac *<host_dmac>* }|{ *<dmac> <dmac-mask>* }} {eigrp|gre*/igrp|ip|ipinip|ospf*|{ <protocol-num> *}} {{* <source> *<source-wildcard>* }|any-source|{*host-source <source-host-ip> }}* {{ <destination> *<destination-wildcard>* }|any-destination| *{host-destination* <destination-host-ip> }} [precedence <precedence>] [tos <tos*>][time-range* <time-range-name>]

Functions: Define an extended numeric MAC-IP ACL rule, no command deletes a extended numeric MAC-IP ACL access-list rule.

Parameters: num access-list serial No. this is a decimal's No. from 3100-3299; **deny** if rules are matching, deny to access; **permit** if rules are matching, permit to access; **any-source-mac**: any source MAC address; **any-destination-mac**: any destination MAC address; **host_smac , smac**: source MAC address; **smac-mask: mask** (reverse mask) of source MAC address ; **host_dmac , dmas** destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **protocol** No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list; **source-host-ip, source** No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression; host: means the address is the IP address of source host, otherwise the IP address of network; **source-wildcard**: reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **destination-host-ip**, destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression; **host:** means the address is the that the destination host address, otherwise the network IP address; **destination-wildcard**: mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point

separated, reverse mask; **s-port(optional):** means the need to match TCP/UDP source port; **port1(optional):** value of TCP/UDP source interface No., Interface No. is an integer from 0-65535; **d-port(optional)**: means need to match TCP/UDP destination interface; ***<sPortMin>,*** the down boundary of source port; ***<sPortMax>***, the up boundary of source port; **port3(optional)**: value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535; ***<dPortMin>***, the down boundary of destination port;***<dPortMax>***, the up boundary of destination port; **[ack] [fin] [psh] [rst] [urg] [syn]**,(optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection; **precedence** (optional) packets can be filtered by priority which is a number from 0-7; **tos** (optional) packets can be filtered by service type which ia number from 0-15; **icmp-type** (optional) ICMP packets can be filtered by packet type which is a number from 0-255; **icmp-code** (optional) ICMP packets can be filtered by packet code which is a number from 0-255; **igmp-type** (optional) ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255; **<time-range-name>**, name of time range

Command Mode: Global mode

Default Configuration: No access-list configured.

Usage Guide: When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 3200-3299 can configure not continual reverse mask of IP address.

Examples: Permit the passage of TCP packet with source MAC 00-12-34-45-XX-XX, any destination MAC address, source IP address 100.1.1.0 0.255.255.255, and source port 100 and destination interface 40000.

Switch(config)#access-list **3199** permit 00-12-34-45-67-00 00-00-00-00-FF-FF any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination d-port 40000

7.1.8 access-list(mac standard)

Command: access-list *<num>* {deny|permit} {any-source-mac | {host-source-mac *<host_smac>* } | {*<smac>* *<smac-mask>*} }

no access-list <num>

Functions: Define a standard numeric MAC ACL rule, no command deletes a standard numeric MAC ACL access-list rule.

Parameters: *<num>* is the access-list No. which is a decimal's No. from 700-799; **deny** if rules are matching, deny access; **permit** if rules are matching, permit access; ***<host_smac>***, ***<sumac>*** source MAC address; ***<sumac-mask>*** mask (reverse mask) of source MAC address.

Command Mode: Global mode

Default Configuration: No access-list configured.

Usage Guide: When the user assign specific *<num>* for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Permit the passage of packets with source MAC address 00-00-XX-XX-00-01, and deny passage of packets with source MAC address 00-00-00-XX-00-ab.

Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00

Switch(config)# access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-00

7.1.9 clear access-group

Command: clear access-group (in **| out) statistic interface { <interface-name> | ethernet<interface-name> }**

Functions: Empty packet statistics information of the specified interface.

Parameters: <interface-name>: Interface name.

Command Mode: Admin mode

Default: None

Examples: Empty packet statistics information of interface1/0/1.

Switch#clear access-group out statistic interface ethernet 1/0/1

7.1.10 firewall

Command: firewall {enable | disable}

Functions: Enable or disable firewall.

Parameters: enable means to enable of firewall; **disable** means to disable firewall.

Default: It is no use if default is firewall.

Command Mode: Global mode

Usage Guide: Whether enabling or disabling firewall, access rules can be configured. But only when the firewall is enabled, the rules can be used in specific orientations of specific ports. When disabling the firewall, all ACL tied to ports will be deleted.

Examples: Enable firewall.

Switch(config)#firewall enable

7.1.11 ip access extended

Command: ip access extended <*name*>

no ip access extended <*name*>

Function: Create a named extended IP access list. The no prefix will remove the named extended IP access list including all the rules.

Parameters: <name> is the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 64.

Command Mode: Global Mode.

Default: No access list is configured by default.

Usage Guide: When this command is issued for the first time, an empty access list will be created.

Example: To create a extended IP access list name tcpFlow.

Switch(config)#ip access-list extended tcpFlow

7.1.12 ip access standard

Command: ip access standard <*name*>

no ip access standard <*name*>

Function: Create a named standard access list. The no prefix will remove the named standard access list including all the rules in the list.

Parameters: <*name*> is the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 64.

Command Mode: Global Mode.

Default: No access list is configured by default.

Usage Guide: When this command is issued for the first time, an empty access list will be created.

Example: To create a standard IP access list name ipFlow.

Switch(config)#ip access-list standard ipFlow

7.1.13 ipv6 access-list

Command: ipv6 access-list *<num-std>* {deny | permit} {*<sIPv6Prefix/sPrefixlen>* | any-source | {host-source *<sIPv6Addr>*}}

ipv6 access-list <*num-ext*> {deny | permit} icmp {{ *<sIPv6Prefix/sPrefixlen>* } | any-source | {host-source *<sIPv6Addr>* }} { *<dIPv6Prefix/dPrefixlen>* | any-destination | {host-destination *<dIPv6Addr>* }} [*<icmp-type>* [*<icmp-code>*]] [dscp *<dscp>*] [flow-label *<fl>*][time-range *<time-range-name>*]

ipv6 access-list <num-ext> {deny / permit*} tcp* {{ <sIPv6Prefix/<sPrefixlen> *} /* any-source | {*host-source <sIPv6Addr>* }} [s-port { *<sPort>* / range <sPortMin> <sPortMax> *}]* {{ <dIPv6Prefix/*<dPrefixlen>* } | any-destination / {host-destination *<dIPv6Addr>* }} [dPort { <dPort> | range <*dPortMin> <dPortMax*> }] [syn | ack / urg | rst / fin | psh] [dscp *<dscp>*] [flow-label *<flowlabel>*][time-range *<time-range-name>*]

ipv6 access-list* <num-ext> {*deny /* permit} udp *{{* <sIPv6Prefix**/**<sPrefixlen*> } | any-source | {host-source <sIPv6Addr> }} [s-port *{* <sPort> | range <sPortMin> <sPortMax> }] {{ <dIPv6Prefix/<dPrefixlen> } */ any-destination* | {host-destination <dIPv6Addr> }} *[*dPort { *<dPort> /* range *<dPortMin>* <dPortMax> }] [dscp *<dscp>*] [flow-label *<flowlabel>*][time-range *<time-range-name>*]**

ipv6 access-list *<num-ext>* {deny | permit} <next-header> { *<sIPv6Prefix/sPrefixlen>* | any-source | {host-source <sIPv6Addr> *}}* { <dIPv6Prefix/dPrefixlen> / any-destination | *{host-destination <dIPv6Addr>* }} [dscp <dscp>] *[flow-label* <fl>][*time-range* <time-range-name> *]*

no ipv6 access-list { <num-std> / <num-ext> }

Functions*: Creates a numbered* standard IP access-list, if the *access-list already* exists, then a *rule* will add to *the current* access-list; the 'no **access-list {*<num-std>|<num-ext>*}**' command deletes a numbered standard IP access-list.

Parameters:* <num-std> is the list *number, list* range is between *500～599*; *<num-ext>* is the list number, list range is between 600～699*; <sIPv6Prefix>* is the prefix of the *ipv6* source address; <*sPrefixlen>* is the length of prefix *of the ipv6 source address, range is between 1～128; ***<sIPv6Addr>*** is the ipv6 source address; ***<dIPv6Prefix>*** is the prefix of the ipv6 destination

address; ***<dPrefixlen>*** is the length of prefix of the ipv6 destination address, range is between 1～128; ***<dIPv6Addr>*** is the ipv6 destination address; ***<icmp-type>***, the type of icmp; ***<icmp-code>***，the protocol code of icmp; ***<dscp>***，IPv6 priority, range from 0 to 63; ***<flowlabel>***，value of flow tag, range from 0 to 1048575; **syn，ack，urg，rst，fin，psh，tcp** label position; ***<sPort>***, source port No., 0-65535; ***<sPortMin>***, the down boundary of source port; ***<sPortMax>***, the up boundary of source port; <dPort>， destination port No., range from 0 to 65535; ***<dPortMin>***, the down boundary of destination port; ***<dPortMax>***, the up boundary of destination port; ***<next-header>***， the next header of IPv6, range from 0 to 255; ***<time-range-name>***, the name of time-range.

***Command Mode*: Global Mode.**

Default:* No access-list *configured.

Usage Guide: Creates a numbered 520 standard IP access-list first time, the following configuration will add to the current access-list.

Examples: Creates a *numbered 520* standard IP access-list*, allow* the source *packet* from 2003:1:2:3::1/64 pass through the net, and deny all the other packet from the source address 2003:1:2::1/48 pass through.

Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64

Switch (config)#ipv6 access-list 520 deny 2003:1:2:::1/48

7.1.14 ipv6 access standard

Command: ipv6 access-list standard *<name>*

no ipv6 access-list standard *<name>*

Function: Create a name-based standard IPv6 access list; the "**no ipv6 access-list standard*<name>***" command deletes the name-based standard IPv6 access list (including all entries).

Parameter: *<name>* is the name for access list, the character string length is from 1 to 64.

Command Mode: Global Mode.

Default: No access list is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Create a standard IPv6 access list named ip6Flow.

Switch(config)#ipv6 access-list standard ip6Flow

7.1.15 ipv6 access extended

Command: ipv6 access-list extended *<name>*

no ipv6 access-list extended *<name>*

Function: Create a name-based extended IPv6 access list; the no command delete the name-based extended IPv6 access list.

Parameter: *<name>* is the name for access list, the character string length is from 1 to 64.

Command Mode: Global Mode.

Default: No IP address is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Create an extensive IPv6 access list named tcpFlow.

Switch (config)#ipv6 access-list extended tcpFlow

7.1.16 {ip|ipv6|mac|mac-ip} access-group

Command: {ip|ipv6|mac|mac-ip} access-group *<name>* {in | out} [traffic-statistic]

no {ip|ipv6|mac|mac-ip} access-group *<name>* {in | out}

Function: Apply an access-list on some **direction *of* port, and determine if** ACL rule is added statistic counter or not by options; the no command deletes access-list binding on the port.

Parameter: <name> is the name for access list, the character string length is from 1 to 32.

Command Mode: Port Mode

Default: The entry of port is not bound ACL.

Usage *Guide: One* port can bind ingress and egress rules.Egress ACL can implement the filtering of the packets on egress and ingress direction, the packets match the specific rules can be allowed or denied. ACL can support IP ACL, MAC ACL, MAC-IP ACL, IPv6 ACL. Ingress direction of the port can bind four kinds of ACL at the same time, there are four resources on egress direction of the port, IP ACL and MAC ACL engage one resource severally, MAC-IP ACL and IPv6 ACL engage two resources severally, so egress direction of the port can not bind four kinds of ACL at the same time. When binding three kinds of ACL at the same time, it should be the types of IP, MAC, MAC-IP or IP, MAC, IPv6. When binding two kinds of ACL at the same time, any combination of ACL type is valid. Each type can only apply one on the port.

At present, notice the following contents when binding Egress ACL to port.

1. IP ACL that match tcp/udp range can not be bound

2. MAC-IP ACL that match tcp/udp range can not be bound

3. IP ACL that match flowlabel can not be bound

There are four kinds of packet head field based on concerned: MAC ACL, IP ACL, MAC-IP ACL and IPv6 ACL; to some extent, ACL filter behavior (permit, deny) has a conflict when a data packet matches multi types of four ACLs. The strict priorities are specified for each ACL based on outcome veracity. It can determine final behavior of packet filter through priority when the filter behavior has a conflict.

When binding ACL to port, there are some limits as below:

1. Each port can bind a MAC-IP ACL, a IP ACL, a MAC ACL and a IPv6 ACL;

2. When binding four ACLs and data packet matching the multi ACLs simultaneity, the priority from high to low are shown as below,

Ingress IPv6 ACL

Ingress MAC-IP ACL

Ingress MAC ACL

Ingress IP ACL

Example: Binding AAA access-list to entry direction of port.

Switch(Config-If-Ethernet1/0/5)#ip access-group aaa in

7.1.17 {ip|ipv6|mac|mac-ip} access-group (Interface Mode)

This command is not supported by switch.

7.1.18 mac access extended

Command: mac-access-list extended *<name>*

no mac-access-list extended <*name*>

Functions: Define a name-manner MAC ACL or enter access-list configuration mode, "**no mac-access-list extended *<name>***" command deletes this ACL.

Parameters: *<name>* name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 64. (remark: sensitivity on capital or small letter.)

Command Mode: Global mode

Default Configuration: No access-lists configured.

Usage Guide: After assigning this command for the first time, only an empty name access-list is created and no list item included.

Examples: Create an MAC ACL named mac_acl.

Switch(config)# mac-access-list extended mac_acl

Switch(Config-Mac-Ext-Nacl-mac_acl)#

7.1.19 mac-ip access extended

Command: mac-ip-access-list extended <*name*>

no mac-ip-access-list extended *<name>*

Functions: Define a name-manner MAC-IP ACL or enter access-list configuration mode, "**no mac-ip-access-list extended *<name>***" command deletes this ACL.

Parameters: *<name>*: name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 64 (remark: sensitivity on capital or small letter).

Command Mode: Global Mode.

Default: No named MAC-IP access-list.

Usage Guide: After assigning this command for the first time, only an empty name access-list is created and no list item included.

Examples: Create an MAC-IP ACL named macip_acl.

Switch(config)# mac-ip-access-list extended macip_acl

Switch(Config-MacIp-Ext-Nacl-macip_acl)#

7.1.20 permit | deny (ip extended)

Command: [no] {deny | permit} icmp {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}}

[*<icmp-type>* [*<icmp-code>*]] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]

[no] {deny | permit} igmp {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<igmp-type>*] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]

[no] {deny | permit} tcp {{ *<sIpAddr> <sMask>* } | any-source | {host-source *<sIpAddr>* }} [s-port { *<sPort>* | range *<sPortMin> <sPortMax>* }] {{ *<dIpAddr> <dMask>* } | any-destination | {host-destination *<dIpAddr>* }} [d-port { *<dPort>* | range *<dPortMin> <dPortMax>* }] [ack+fin+psh+rst+urg+syn] [precedence *<prec>*] [tos *<tos>*][time-range *<time-range-name>*]

[no] {deny */ permit}* udp {{ *<sIpAddr>* <sMask> *} / any-source **| {host-source *<sIpAddr>* }} [s-port *{ <sPort>* | range *<sPortMin> <sPortMax>* }] {{ <dIpAddr> *<dMask>* } | any-destination */ {host-destination* <dIpAddr> *}} [*d-port { *<dPort> /* range *<dPortMin> <dPortMax>* }] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]**

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <*protocol-num*>} {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]

Functions: Create a name extended IP access rule to match specific IP protocol or all IP protocol.

Parameters: *<sIpAddr>* is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation; ***<dIpAddr>*** is the destination IP address, the format is dotted decimal notation; **<*dMask*>** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position 1; **<*igmp-type*>**, the type of igmp, 0-255; ***<icmp-type>***, the type of icmp, 0-255 ; **<icmp-code>,** protocol No. of icmp, 0-255; **<prec>**, IP priority, 0-7; ***<tos>***, to value, 0-15; ***<sPort>***, source port No., 0-65535; ***<sPortMin>***, the down boundary of source port; ***<sPortMax>***, the up boundary of source port; ***<dPort>***, destination port No. 0-65535; ***<dPortMin>***, the down boundary of destination port; ***<dPortMax>***, the up boundary of destination port; ***<time-range-name>***, time range name.

Command Mode: Name extended IP access-list configuration mode

Default: No access-list configured.

Examples: Create the extended access-list, deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

Switch(config)# access-list ip extended udpFlow

Switch(Config-IP-Ext-Nacl-udpFlow)#deny igmp any any-destination

Switch(Config-IP-Ext-Nacl-udpFlow)#permit udp any host-destination 192.168.0.1 d-port 32

7.1.21 permit | deny(ip standard)

Command: {deny | permit} {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}}

no {deny | permit} {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}}

Functions: Create a name standard IP access rule, and "**no {deny | permit} {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}}**" action of this command deletes this name standard IP access rule.

Parameters: *<sIpAddr>* is the source IP address, the format is dotted decimal notation; **<*sMask* >**

is the reverse mask of source IP, the format is dotted decimal notation.

Command Mode: Name standard IP access-list configuration mode

Default: No access-list configured.

Example: Permit packets with source address 10.1.1.0/24 to pass, and deny other packets with source address 10.1.1.0/16.

Switch(config)# access-list ip standard ipFlow

Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255

Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255

7.1.22 permit | deny(ipv6 extended)

Command: [no] {deny | permit} icmp {{<*sIPv6Prefix/sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [<*icmp-type*> [<*icmp-code*>]] [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny | permit} tcp { <*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*> }} [s-port { <*sPort*> | range <*sPortMin*> <sPortMax> }] { <*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <*dPort*> | range <*dPortMin*> <*dPortMax*> }] [syn | ack | urg | rst | fin | psh] [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny / *permit}* udp { <*sIPv6Prefix/sPrefixlen*> | *any-source* / {host-source <*sIPv6Addr*> }} [s-port *{* <*sPort*> | *range* <*sPortMin*> <sPortMax> }] { <*dIPv6Prefix/dPrefixlen*> | any-destination / *{host-destination* <dIPv6Addr> *}}* [d-port { <*dPort*> | range <*dPortMin*> <dPortMax> }] [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny / permit} <next-header> *{<sIPv6Prefix/*sPrefixlen> | *any-source* / {host-source <*sIPv6Addr*>}} {<dIPv6Prefix/*dPrefixlen*> | any-destination | *{host-destination* <*dIPv6Addr*>}} [dscp <*dscp>]* [flow-label <fl>*][*time-range <*time-range-name>]*

[no*]* {deny | *permit}* {<sIPv6Prefix/*sPrefixlen*> / *any-source* / {host-source <sIPv6Addr>*}}* {<dIPv6Prefix/dPrefixlen> / any-destination | *{host-destination* <dIPv6Addr>}} [dscp <*dscp*>] [flow-label <*fl*>] [time-range<*time-range-name*>]

Function: Create an *extended* nomenclature IPv6 access control *rule for* specific IPv6 protocol.

Parameter: <*sIPv6Addr*> is the source IPv6 address; **<sPrefixlen>** is the length of the IPv6 address prefix, the range is 1～128; **<dIPv6Addr>** is the destination IPv6 address; **<*dPrefixlen*>** is the length of the IPv6 address prefix, the range is 1～128; ***<igmp-type>***, type of the IGMP; ***<icmp-type>***, icmp type; ***<icmp-code>***, icmp protocol number; ***<dscp>***, IPv6 priority ,the range is 0～63; ***<flowlabel>***, value of the flow label, the range is 0～1048575; **syn**,**ack**,**urg**,**rst**,**fin**,**psh**,**tcp** label position; ***<sPort>***, source port number, the range is 0～65535; ***<sPortMin>***, the down boundary of source port; <sPortMax>***, the** *up* boundary of source ***port;*** <dPort>, destination port number, the range is 0～65535; ***<dPortMin>***, the down boundary of destination port; ***<dPortMax>***, the up boundary of destination port. ***<next-header>,*** the IPv6 next-header. ***<time-range-name>***, time range name.

Command Mode: IPv6 nomenclature extended access control list mode

Default: No access control list configured.

Example: Create an extended access control list named udpFlow, denying the igmp packets while

allowing udp packets with destination address 2001:1:2:3::1 and destination port 32.
Switch(config)#ipv6 access-list extended udpFlow
Switch(Config-IPv6-Ext-Nacl-udpFlow)#deny igmp any any-destination
Switch(Config-IPv6-Ext-Nacl-udpFlow)#permit udp any-source host-destination 2001:1:2:3::1 dPort 32

7.1.23 permit | deny(ipv6 standard)

Command: [no] {deny | permit} {{*<sIPv6Prefix/sPrefixlen>*} | any-source | {host-source *<sIPv6Addr>*}}
Function: Create a standard nomenclature IPv6 access control rule; the no form of this command deletes the nomenclature standard IPv6 access control rule.
Parameter: ***<sIPv6Prefix>*** is the prefix of the source IPv6 address, ***<sPrefixlen>*** is the length of the IPv6 address prefix, the valid range is 1~128. ***<sIPv6Addr>*** is the source IPv6 address.
Command Mode: Standard IPv6 nomenclature access list mode
Default: No access list configured by default.
Usage Guide:
Example: Permit packets with source address of 2001:1:2:3::1/64 while denying those with source address of 2001:1:2:3::1/48.
Switch(config)#ipv6 access-list standard ipv6Flow
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# permit 2001:1:2:3::1/64
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# deny 2001:1:2:3::1/48

7.1.24 permit | deny(mac extended)

Command:

[no]{deny|permit} {any-source-mac|{host-source-mac *<host_smac>* }|{ *<smac>* *<smac-mask>* }} {any-destination-mac|{host-destination-mac *<host_dmac>* }|{ *<dmac>* *<dmac-mask>* }} [cos *<cos-val>* [*<cos-bitmask>*][vlanid <vid-value> *[* <vid-mask> *]*[ethertype <protocol> *[* <protocol-mask> *]]]*]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [ethertype <protocol> [<protocol-mask>]]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [vlanid <vid-value> [<vid-mask>][ethertype <protocol> [<protocol-mask>]]]

[no]{deny|permit} {any-source-mac|{host-source-mac *<host_smac>* }|{ *<smac>* *<smac-mask>* }} {any-destination-mac|{host-destination-mac *<host_dmac>* }|{ *<dmac>* *<dmac-mask>* }} [untagged-eth2 [ethertype <protocol> [protocol-mask]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [untagged-802-3]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <*smac*> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [tagged-eth2 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype <protocol> [<protocol-mask>]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} [tagged-802-3 [cos <cos-val> [<cos-bitmask>]] [vlanId <*vid-value*> [<*vid-mask*>]]]

Functions: Define an extended name MAC ACL rule, and no command deletes this extended name IP access rule.

Parameters: any-source-mac: any source of MAC address; **any-destination-mac**: any destination of MAC address; **host_smac**, **smac**: source MAC address; **smac-mask**: mask (reverse mask) of source MAC address; **host_dmac**, **dmas** destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **untagged-eth2** format of untagged ethernet II packet; **tagged-eth2** format of tagged ethernet II packet; **untagged-802-3** format of untagged ethernet 802.3 packet; **tagged-802-3** format of tagged ethernet 802.3 packet; **cos-val:** cos value, 0-7; **cos-bitmask:** cos mask, 0-7reverse mask and mask bit is consecutive; **vid-value:** VLAN No, 1-4094; **vid-bitmask:** VLAN mask, 0-4095, reverse mask and mask bit is consecutive; **protocol:** specific Ethernet protocol No., 1536-65535; **protocol-bitmask:** protocol mask, 0-65535, reverse mask and mask bit is consecutive.

Notice: mask bit is consecutive means the effective bit must be consecutively effective from the first bit on the left, no ineffective bit can be added through. For example: the reverse mask format of one byte is: 00001111b; mask format is 11110000; and this is not permitted: 00010011.

Command Mode: Name extended MAC access-list configuration mode

Default configuration: No access-list configured.

Example: The forward source MAC address is not permitted as 00-12-11-23-XX-XX of 802.3 data packet.

Switch(config)# mac-access-list extended macExt

Switch(Config-Mac-Ext-Nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac untagged-802-3

Switch(Config-Mac-Ext-Nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff any tagged-802

7.1.25 permit | deny(mac-ip extended)

Command:

[no] {deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}

{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}
icmp{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}
{{<*destination*><*destination-wildcard*>}|any-destination|{host-destination
<*destination-host-ip*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit}
{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}
{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}
igmp{{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}}
{{<*destination*><*destination-wildcard*>}|any-destination|{host-destination
<*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*> }| { <*smac*> <*smac-mask*> }}{any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }}tcp{{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port { <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <*destination*> <*destination-wildcard*> } | any-destination| {host-destination <*destination-host-ip*> }} [d-port { <*port3*> | range <*dPortMin*> <*dPortMax*> }] [ack＋fin＋psh＋rst＋urg＋syn] [precedence <*precedence*>] [tos <*tos*>][time-range <*time-range-name*>]

[no]{deny|*permit}{any-source-mac*|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }}{any-destination-mac|{host-destination-mac <*host_dmac*> }| { <*dmac*> <*dmac-mask*> }}udp{{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port{ <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <destination> <*destination-wildcard*> }|any-destination| *{host-destination* <destination-host-ip> *}} [d-port* { <port3> / range <dPortMin> <*dPortMax*> }] [precedence <*precedence*>] [tos <*tos*>][time-range <*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*>
<*smac-mask*>*}*}{any-destination-mac|{host-destination-mac<*host_dmac*>}|
{<*dmac*><*dmac-mask*>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}}
{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}
{{<*destination*><*destination-wildcard*>}|any-destination|{host-destination
<*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

Functions: Define an extended name MAC-IP ACL rule, no form deletes one extended numeric MAC-IP ACL access-list rule.

Parameters: num access-list serial No. this is a decimal's No. from 3100-3199; **deny** if rules are matching, deny to access; **permit** if rules are matching, permit to access; **any-source-mac**: any source MAC address; **any-destination-mac**: any destination MAC address; **host_smac**, smac: source MAC address; smac-mask: mask (reverse mask) of source MAC address ; **host_dmac** , dmas destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address;

protocol No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list; **source-host-ip**, source No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression; **host**: means the address is the IP address of source host, otherwise the IP address of network; **source-wildcard**: reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **destination-host-ip**, destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression; **host**: means the address is that the destination host address, otherwise the network IP address; **destination-wildcard**: mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **s-port(optional)**: means the need to match TCP/UDP source port; **port1(optional):** value of TCP/UDP source interface No., Interface No. is an integer from 0-65535; ***<sPortMin>***, the down boundary of source port; ***<sPortMax>***, the up boundary of source port; **d-port(optional):** means need to match TCP/UDP destination interface; **port3(optional)**: value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535; ***<dPortMin>***, the down boundary of destination port; ***<dPortMax>***, the up boundary of destination port; **[ack] [fin] [psh] [rst] [urg] [syn]**, (optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection; **precedence (optional)** packets can be filtered by priority which is a number from 0-7; **tos (optional)** packets can be filtered by service type which ia number from 0-15; **icmp-type (optional)** ICMP packets can be filtered by packet type which is a number from 0-255; **icmp-code (optional)** ICMP packets can be filtered by packet code which is a number from 0-255; **igmp-type (optional)** ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255; ***<time-range-name>***, name of time range.

Command Mode: Name extended MAC-IP access-list configuration mode

Default: No access-list configured.

Examples: Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100 and destination port 40000.

Switch(config)# mac-ip-access-list extended macIpExt

Switch(Config-MacIp-Ext-Nacl-macIpExt)# deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000

7.1.26 show access-lists

Command: show access-lists [*<num>*|*<acl-name>*]

Functions: Reveal ACL of configuration.

Parameters: *<acl-name>*, specific ACL name character string; ***<num>,*** specific ACL No.

Default: None.

Command Mode: Admin and Configuration Mode

Usage Guide: When not assigning names of ACL, all ACL will be revealed, used x time（s）indicates

the times of ACL to be used.

Examples:

Switch#show access-lists

access-list 10(used 0 time(s))

access-list 10 deny any-source

access-list 100(used 1 time(s))

access-list 100 deny ip any any-destination

access-list 100 deny tcp any any-destination

access-list 1100(used 0 time(s))

access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800

access-list 3100(used 0 time(s))

access-list 3100 deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000

Displayed information	Explanation
access-list 10(used 1 time(s))	Number ACL10, 0 time to be used
access-list 10 deny any-source	Deny any IP packets to pass
access-list 100(used 1 time(s))	Nnumber ACL10, 1 time to be used
access-list 100 deny ip any-source any-destination	Deny IP packet of any source IP address and destination address to pass
access-list 100 deny tcp any-source any-destination	Deny TCP packet of any source IP address and destination address to pass
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800	Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets whose 15th and 16th byte is respectively 0x08 , 0x0 to pass
access-list 3100 permit any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000	Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100 and destination interface 40000

7.1.27 show access-group

Command: show access-group in (interface {Ethernet | Ethernet IFNAME | port-channel IFNAME})

Functions: Display the ACL binding status on the port.

Parameters: IFNAME*,* Port name.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: When not assigning interface names, all ACL tied to port will be revealed.

Examples:

Switch#show access-group

interface name: Ethernet 1/0/1

IP Ingress access-list used is 100, traffic-statistics Disable.

interface name: Ethernet1/0/2

IP Ingress access-list used is 1, packet(s) number is 11110.

Displayed information	Explanation
interface name: Ethernet 1/0/1	Tying situation on port Ethernet1/0/1
IP Ingress access-list used is 100	No. 100 numeric expansion ACL tied to entrance of port Ethernet1/0/1
packet(s) number is 11110	Number of packets matching this ACL rule

7.1.28 show firewall

Command: show firewall

Functions: Reveal configuration information of packet filtering functions.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Examples:

Switch#show firewall

Firewall status: Enable.

Displayed information	Explanation
fire wall is enable	Packet filtering function enabled

7.1.29 show ipv6 access-lists

Command: show ipv6 access-lists [*<num>*|*<acl-name>*]

Function: Show the configured IPv6 access control list.

Parameter:<num> is the number of specific access control list, the valid range is 500～699, amongst 500～599 is digit standard IPv6 ACL number, 600～699 is the digit extended IPv6 ACL number; <acl-name> is the nomenclature character string of a specific access control list, lengthening within 1～16.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: When no access control list is specified, all the access control lists will be displayed; in used x time（s） is shown the times the ACL had been quoted.

Example:

Switch #show ipv6 access-lists
ipv6 access-list 500(used 1 time(s))
    ipv6 access-list 500 deny any-source

ipv6 access-list 510(used 1 time(s))
    ipv6 access-list 510 deny ip any-source any-destination
    ipv6 access-list 510 deny tcp any-source any-destination

ipv6 access-list 520(used 1 time(s))
    ipv6 access-list 520 permit ip any-source any-destination

7.1.30 show time-range

Command: show time-range *<word>*
Functions: Reveal configuration information of time range functions.
Parameters: *word* assign name of time-range needed to be revealed.
Default: None.
Command Mode: Admin and Configuration Mode
Usage Guide: When not assigning time-range names, all time-range will be revealed.
Examples:
Switch#show time-range
time-range timer1 (inactive, used 0 times)
        absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
time-range timer2 (inactive, used 0 times)
        absolute-periodic Monday 0:0:0 to Friday 23:59:59

7.1.31 time-range

Command: [no] time-range *<time_range_name>*
Functions: Create the name of time-range as time range name, enter the time-range mode at the same time.
Parameters: *time_range_name*, time range name must start with letter, and the length cannot exceed 16 characters long.
Command Mode: Global mode
Default: No time-range configuration.
Usage Guide: None
Examples: Create a time-range named dc_timer.
Switch(config)#Time-range dc_timer

7.2 Self-defined ACL

7.2.1 permit | deny

This command is not supported by switch.

7.2.2 udf-access-list standard

This command is not supported by switch.

7.2.3 userdefined-access-list standard offset

Command: userdefined-access-list standard offset [window1 <*offset*>] [window2 <*offset*>] [window3 <*offset*>] [window4 <*offset*>][window5 <*offset*>][l2start <*offset*> | l3start <*offset*>| l4start <*offset*>]

no userdefined-access-list standard offset [window1] [window2] [window3] [window4][window5]

Function: Create a standard self-defined ACL template. If the template exists, the corresponding window of the template can be modified; the no command deletes the window of the standard self-defined ACL template. If the window is not specified, the standard self-defined ACL template will be deleted.

Parameter:

window1-window5 self-defined window 1 to 5

offset The configured offset is from 0 to 31 (*unit* is 2Bytes)

Command Mode: Global Mode

Default: No Configuration Template

Usage Guide: <offset>is used to configure the offset of a window, with a value range of<0-31>and a unit of 2Bytes. That is, 0 represents the offset of 0Bytes, and 1 represents the offset of 2Bytes. It can be configured with up to 4 window offset starting positions and offsets. A basic custom ACL template is shared globally. When configuring a custom ACL rule that uses a certain window, the corresponding window in the template cannot be modified. When there are no rules referencing a certain window, this command can be used to modify the configuration of that window.

The delete template command can delete the offset configuration of one or some windows in the template or delete the configuration of the entire template (without specifying any specific window). The deletion can only be successful when the window corresponding to the template is not used by custom ACL rules.

Example: Create a global template, use window3, and configure the offset starting position and offset separately

***Switch*(config)#**userdefined-access-list standard offset window3 l2 0 window4

7.2.4 userdefined-access-list extended offset

This command is not supported by switch.

7.2.5 userdefined-access-list standard

Command:userdefined-access-list standard <num> {deny | permit} [any-source-mac | host-source-mac ***<mac-address>|<mac-address> <mac-address>*** (any-source-mac | host-source-mac ***<mac-address>|<mac-address> <mac-address>***) }] [window1 <word> <word>] [window2 <word> <word>] [window3 <word> <word>] [window4 <word> <word>] [window5 <word> <word>]

no userdefined-access-list <num>

***Function: Create* a numbered standard *self-defined ACL. If* the standard *self-defined ACL exists,* then a rule** will be added to the ACL. The no command deletes a numbered standard self-defined ACL.

Parameter: <num>Access table number, which is a decimal number from 1200-1299; Deny denies access if the rules match; If the rules match, access is allowed< Word>is a 2-byte length hexadecimal number< Mac address>is the MAC address.

Command Mode: *Global Mode*

Default:* No any access-list *configured

***Usage Guide:* When users *specify the specified* <num> for *the first time,* create the ACL *with this serial* number, then *add the entry into* this ACL.**

***Example: Allow* the** packet whose first and second byte is 0x4501 passing.

Switch(config)#userdefined-access-list standard 1200 permit any-source-mac any-destination-mac window1 45 01

Switch(config)#

7.2.6 userdefined-access-list extended

This command is not supported by switch.

7.2.7 userdefined access-group

This command is not supported by switch.

7.2.8 vacl userdefined access-group

Command: vacl userdefined access-group <*name*> *{*in} vlan <*vlanId*> [traffic-statistic]

no vacl userdefined access-group <*name*> {in} vlan <*vlanId*>

Function: Apply userdefined-access-list to *one direction* of the specified *VLAN,*

decide whether the statistical counter should be added to the ACL according to the options or. Theno command deletes the configuration bound to the specified VLAN.
Parameter: <name> is the access-list name from 1200 to 1399 in decimal notation;

<vlanId> the bound VLAN，the range is 1-4095.

Command Mode: Global Mode
Default: userdefined-access-list is not bound to any VLAN
Usage Guide**:** A self-defined access-list can be bound to the ingress of a VLAN and can be configured at the ingress of the same VLAN with other access-lists at the same time. The deny rule is precedent when different access-lists are matching, that means if there is a access-lists match the deny rule, the deny rule must be executed, the permit rule will be executed oppositely.
Example: *The configured* self-defined access-list is shown in the following:
Switch(config)#userdefined-access-list standard *offset window1* l3 0 window2 l4 1 **window3** l3 1
Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF
Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000
Bind the self-defined access-list to VLAN1:
Switch(config)#vacl userdefined access-group 1300 in vlan 1.

7.3 802.1x

7.3.1 authentication dot1x radius none

This command is not supported by the switch.

7.3.2 debug dot1x detail

Command: debug dot1x detail {pkt-send | pkt-receive | internal | all | userbased | webbased} interface *[*ethernet] <*interface-name*>

no debug *dot1x* detail { pkt-send | pkt-receive | internal | all | userbased | webbased} interface [ethernet] <*interface-name*> | **port-channel <*interface-name*>**

Function: Enable the debug information of dot1x details; the no operation of this command will disable that debug information.
Parameters: pkt-send: Enable the debug information of dot1x about sending packets;
pkt-receive: Enable the debug information of dot1x about receiving packets;
internal: Enable the debug information of dot1x about internal details;
all: Enable the debug information of dot1x about all details mentioned above;
userbased: user-based authentication;

webbased: Web-based authentication;

<*interface-name*>: the name of the interface.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of dot1x details, users can check the detailed processes of the Radius protocol operation, which might help diagnose the cause of faults if there is any.

Example: Enable all debug information of dot1x details on interface1/0/1.

Switch#debug dot1x detail all interface ethernet1/0/1

7.3.3 debug dot1x error

Command: debug dot1x error

no debug dot1x error

Function: Enable the debug information of dot1x about errors; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of dot1x about errors, users can check the information of errors that occur in the processes of the Radius protocol operation, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x about errors.

Switch#debug dot1x error

7.3.4 debug dot1x fsm

Command: debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>| port-channel <*interface-name*>

no debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name> | port-channel <*interface-name*>

Function: Enable the debug information of dot1x state machine; the no operation of this command will disable that debug information.

Command Mode: Admin Mode.

Parameters: all: Enable the debug information of dot1x state machine;

aksm: Enable the debug information of Authenticator Key Transmit state machine;

asm: Enable the debug information of Authenticator state machine;

basm: Enable the debug information of Backend Authentication state machine;

ratsm: Enable the debug information of Re-Authentication Timer state machine;

<interface-name>: the name of the interface.

Usage Guide: By enabling the debug information of dot1x, users can check the negotiation process of dot1x protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x state machine.

Switch#debug dot1x fsm asm interface ethernet1/0/1

7.3.5 debug dot1x packet

Command: debug dot1x packet {all | receive | send} interface <*interface-name*>| port-channel <*interface-name*> | port-channel <*interface-name*>

no debug dot1x packet {all | receive | send} interface <*interface-name*>| port-channel <*interface-name*> | port-channel <*interface-name*>

Function: Enable the debug information of dot1x about messages; the no operation of this command will disable that debug information.

Command Mode: Admin Mode.

Parameters: send: Enable the debug information of dot1x about sending packets;

receive: Enable the debug information of dot1x about receiving packets;

all: Enable the debug information of dot1x about both sending and receiving packets;

<*interface-name*>: The name of the interface.

Usage Guide: By enabling the debug information of dot1x about messages, users can check the negotiation process of dot1x protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x about messages.

Switch#debug dot1x packet all interface ethernet1/0/1

7.3.6 dot1x accept-mac

Command: dot1x accept-mac <mac-address> [interface <interface-name>]

no dot1x accept-mac <mac-address> [interface <interface-name>]

Function: Add a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports. The 'no dot1x accept-mac <mac-address> [interface <interface-name>]' command deletes the entry from dot1x address filter table.

Parameters: <mac-address> stands for MAC address;

<interface-name> for interface name and port number.

Command mode: Global Mode.

Default: N/A.

Usage Guide: The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user. When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted, the rest will be rejected.

Example: Adding MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/0/5.

Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/0/5

7.3.7 dot1x eapor enable

Command: dot1x eapor enable
no dot1x eapor enable
Function: Enables the EAP relay authentication function in the switch; the “no dot1x eapor enable” command sets EAP local end authentication.
Command mode: Global Mode.
Default: EAP relay authentication is used by default.
Usage Guide: The switch and RADIUS may be connected via Ethernet or PPP. If an Ethernet connection exists between the switch and RADIUS server, the switch needs to authenticate the user by EAP relay (EAPoR authentication); if the switch connects to the RADIUS server by PPP, the switch will use EAP local end authentication (CHAP authentication). The switch should use different authentication methods according to the connection between the switch and the authentication server.
Example: Setting EAP local end authentication for the switch.
Switch(config)#no dot1x eapor enable

7.3.8 dot1x enable

Command: dot1x enable
no dot1x enable
Function: Enables the 802.1x function in the switch and ports: the 'no **dot1x enable'** command disables the 802.1x function.
Command mode: Global Mode and Port Mode.
Default: 802.1x function is **not enabled** in global mode by default; **if** 802.1x is enabled under Global Mode, 802.1x will not be enabled for the ports by default.
Usage Guide: The 802.1x authentication for the switch must be enabled first to enable 802.1x authentication for the respective ports. If Spanning Tree or MAC binding is enabled on the port, or the port is a Trunk port or member of port aggregation group, 802.1x function cannot be enabled for that port unless such conditions are removed.
Example: Enabling the 802.1x function of the switch and enable 802.1x for port1/0/12.
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/12
Switch(Config-If-Ethernet1/0/12)#dot1x enable

7.3.9 dot1x ipv6 passthrough

This command is not supported by the switch.

7.3.10 dot1x guest-vlan

Command: dot1x guest-vlan <*vlanid*>
no dot1x guest-vlan

Function: Set the guest-vlan of the specified port; the "**no dot1x guest-vlan**" command is used to delete the guest-vlan.
Parameters: ***<vlanid>*** the specified VLAN id, ranging from 1 to 4094.
Command Mode: Port Mode.
Default Settings: There is no 802.1x guest-vlan function on the port.
User Guide: The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.
In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications (such as anti-virus software, the patches of operating system). When a user of a port within Guest VLAN starts an authentication, the port will remain in Guest VLAN in the case of a failed authentication. If the authentication finishes successfully, there are two possible results:

- The authentication server assigns an Auto VLAN, causing the port to leave Guest VLAN to join the assigned Auto VLAN. After the user gets offline, the port will be allocated back into the specified Guest VLAN.
- The authentication server assigns an Auto VLAN, then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.

Attention:

- There can be different Guest VLAN set on different ports, while only one Guest VLAN is allowed on one port.
- Only when the access control mode is portbased, the Guest VLAN can take effect. If the access control mode of the port is macbased or userbased, the Guest VLAN can be successfully set without taking effect.

Examples： Set Guest-VLAN of port Ethernet1/0/3 as VLAN 10.
Switch(Config-If-Ethernet1/0/3)#dot1xguest-vlan 10

7.3.11 dot1x macfilter enable

Command: dot1x macfilter enable
no dot1x macfilter enable
Function: Enables the dot1x address filter function in the switch; the 'no dot1x macfilter enable' command disables the dot1x address filter function.
Command mode: Global Mode
Default: dot1x address filter is disabled by default.
Usage Guide: When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted.
Example: Enabling dot1x address filter function for the switch.
Switch(config)#dot1x macfilter enable

7.3.12 dot1x macbased guest-vlan

Command: dot1x macbased guest-vlan <vlanid>
no dot1x macbased guest-vlan
Function: Configure to appoint the port's guest-vlan based on the mac authentication; the no command deletes this guest-vlan.
Parameters: <vlanid>: the configured vlan id, the range is from 1 to 4094.
Command mode: Port Mode.
Default: Do not configure 802.1x macbased guest-vlan.
Usage Guide: If there is no dedicated authentication client or the client version was too low, and it makes no clients authenticate successfully on the port in some time, then the access device will make this user join to the guest VLAN. User can get the 802.1x client software in guest VLAN, update the client or do other updating things (such as anti-virus software, system patches and etc.) When the user under the port in Guest VLAN issues the authentication, this port will be stay in guest VLAN if the authentication failed; if it was successful, there are two situations as below:
1. The authentication server issues an auto VLAN, in this time, the user left the guest VLAN and joined to the auto VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.
2. The authentication server did not issue the VLAN, in this time, the user left the guest VLAN and joined to the configured native VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.
Notice:
1. dot1x macbased guest-vlan can be configured only on the port based on mac authentication and in HYBRID mode.
2. Different macbased guestVLAN can be configured on different ports, but only one macbased guestVLAN can be configured on one port.
Example: Configure the guest-vlan of Ethernet1/0/3 as Vlan 10.
Switch(Config-If-Ethernet1/0/3)#dot1x macbased guest-vlan 10

7.3.13 dot1x macbased port-down-flush

Command: dot1x macbased port-down-flush
no dot1x macbased port-down-flush
Function: Enables this command, when the dot1x certification according to mac is down, delete the user who passed the certification of the port; The no command does not make the down operation.
Command mode: Global Mode
Default: The command is not enabled by default.
Usage Guide: When users who passed the certification according to mac changed among different ports, delete the user for the new certification. The command should be enable to delete the user.
Example: When the dot1x certification according to mac is down, delete the user who passed the certification of the port.

Switch(config)#dot1x macbased port-down-flush

7.3.14 dot1x max-req

Command: dot1x max-req <*count*>
no dot1x max-req
Function: Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response; the "no dot1x max-req" command restores the default setting.
Parameters: ***<count>*** is the times to re-transfer EAP request/ MD5 frames, the valid range is 1 to 10.
Command mode: Global Mode.
Default: The default maximum for retransmission is 2.
Usage Guide: The default value is recommended in setting the EAP request/ MD5 retransmission times.
Example: Changing the maximum retransmission times for EAP request/ MD5 frames to 5 times.
Switch(config)#dot1x max-req 5

7.3.15 dot1x user allow-movement

Command: dot1x user allow-movement
no dot1x user allow-movement
Function: Enable the authentication function after the user moves the port, the no command disables the function.
Command Mode: Global mode
Default: Disable the authentication function after the user moves the port.
Usage Guide: Enable the authentication function after the user moves the port, so the switch allows user to process this authentication. In the condition that the switch connects with hub, when the user will be moved to other port, dot1x user allow-movement command should be enabled.
Example: Enable the authentication function after the user moves the port.
Switch(config)#dot1x user allow-movement

7.3.16 dot1x user free-resource

Command: dot1x user free-resource <*prefix*> <*mask*>
no dot1x user free-resource
Function: To configure 802.1x free resource; the no form command closes this function.
Parameter: <*prefix*> is the segment for limited resource, in dotted decimal format;
<*mask*> is the mask for limited resource, in dotted decimal format.
Command Mode: Global Mode.
Default: There is no free resource by default.
Usage Guide: This command is available only if user based access control is applied. If user based

access control has been applied, this command configures the limited resources which can be accessed by the un-authenticated users. For port based and MAC based access control, users could access no network resources before authentication.

If TrustView management system is available, the free resource can be configured in TrustView server, and the TrustView server will distribute the configuration to the switches.

To be noticed, only one free resource can be configured for the overall network.

Example: To configure the free resource segment as 1.1.1.0, the mask is 255.255.255.0.

Switch(Config)#dot1x user free-resource 1.1.1.0 255.255.255.0

7.3.17 free-resource destination

Command: free-resource destination {ipv4 | ipv6]} <**prefix>/<*mask*>**

no free-resource destination [ipv4 | ipv6] <prefix>/<*mask*>

Function: To configure global ipv4 or ipv6 free resource; the no form command deletes it.

Parameter: <*prefix*> is the segment for limited resource, ipv4 address is in dotted decimal format and ipv6 address is in colon hexadecimal format;

<*mask*> is the mask places for limited resource.

Command Mode: Global Mode.

Default: There is no free resource by default.

Usage Guide: After configured the free resource, the user who does not pass the 802.1x authentication can visit the free resource configured by this command.

Example: To configure the free resource segment as 100.1.1.0, the mask is 255.255.255.0.

Switch (config): free-resource destination ipv4 100.1.1.0/24

7.3.18 dot1x max-user macbased

Command: dot1x max-user macbased <*number*>

no dot1x max-user macbased

Function: Sets the maximum users allowed connect to the port; the 'no dot1x max-user' command restores the default setting.

Parameters: <*number*> is the maximum users allowed, the valid range is 1 to 256.

Command mode: Port configuration Mode.

Default: The default maximum user allowed is 1.

Usage Guide: This command is available for ports using MAC-based access management, if MAC address authenticated exceeds the number of allowed user, additional users will not be able to access the network.

Example: Setting port 1/0/3 to allow 5 users.

Switch(Config-If-Ethernet1/0/3)#dot1x max-user macbased 5

7.3.19 dot1x max-user userbased

Command: dot1x max-user userbased <number>

no dot1x max-user userbased

Function: Set the upper limit of the number of users allowed access the specified port when using user-based access control mode; the no command is used to reset the default value.
Parameters: *<number>* the maximum number of users allowed to access the network, ranging from 1 to 1~256.
Command Mode: Port Mode.
Default Settings: The maximum number of users allowed to access each port is 10 by default.
User Guide: This command can only take effect when the port adopts user-based access control mode. If the number of authenticated users exceeds the upper limit of the number of users allowed access the network, those extra users can not access the network.
Examples: Setting port 1/0/3 to allow 5 users.
Switch(Config-If-Ethernet1/0/3)#dot1x max-user userbased 5

7.3.20 dot1x portbased mode single-mode

Command: dot1x portbased mode single-mode
no dot1x portbased mode single-mode
Function: Set the single-mode based on portbase authentication mode; the no command disables this function.
Parameters: None.
Command mode: Port Mode
Default: Disable the single-mode.
Usage Guide: This command takes effect when the access mode of the port is set as portbase only. Before configuring the single-mode, if the port has enabled dot1x port-method portbased command and exist online users, the switch will enforce all users of this port are offline. After that, this port only allows a user to pass the authentication, the user can access the specified network resource, but other authentication users of this port will be denied and can not access the network. After disabling the single-mode, the switch also enforce the authenticated user is offline.
Example:
Switch(Config-If-Ethernet1/0/1)#dot1x portbased mode single-mode

7.3.21 dot1x port-control

Command: dot1x port-control {auto | force-authorized | **force-unauthorized}**
no dot1x port-control
Function: Sets the 802.1x authentication status; the 'no dot1x port-control' command restores the default setting.
Parameters: auto enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant; **force-authorized** sets port to authorized status, unauthenticated data is allowed to pass through the port; **force-unauthorized** will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port.
Command mode: Port configuration Mode

Default: When 802.1x is enabled for the port, **auto** is set by default.

Usage Guide: If the port needs to provide 802.1x authentication for the user, the port authentication mode should be set to auto.

Example: Setting port1/0/1 to require 802.1x authentication mode.

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#dot1x port-control auto

7.3.22 dot1x port-method

Command: dot1x port-method {macbased | portbased | userbased {standard | advanced}}

no dot1x port-method

Function: To configure the access control method of appointed interface. The no form command restores the default access control method.

Parameter: macbased means the access control method based on MAC address

portbased means the access control method based on port

userbased means the access control method based on user, it can be divided into two types, one is standard access control method, and the other is advanced access control method

Command mode: Port Configuration Mode.

Default: Advanced access control method based on user is used by default.

Usage Guide: This command is used to configure the dot1x authentication method for the specified port. When port based authentication is applied, only one host can authenticate itself through one port. And after authentication, the host will be able to access all the resources. When MAC based authentication is applied, multiple host which are connected to one port can access all the network resources after authentication. When either of the above two kinds of access control is applied, un-authenticated host cannot access any resources in the network.

When user based access control is applied, un-authenticated users can only access limited resources of the network. The user based access control falls into two kinds – the standard access control and the advanced access control. The standard user based access control does not limit the access to the limited resources when the host is not authenticated yet. While the user based advanced access control can control the access to the limited resources before authentication is done.

Notes: For standard control method based on user, the 802.1x free resource must be configured first, and it needs to be used with dot1x privateclient enable.

Example: To configure the access control method based on port for Etherent1/0/4.

Switch(Config-If-Ethernet1/0/4)#dot1x port-method portbased

7.3.23 dot1x privateclient enable

Command: dot1x privateclient enable

no dot1x privateclient enable

Function: To configure the switch to force the authentication client to use Digital China

Networks's private 802.1x authentication protocol. The no prefix will disable the command and allow the authentication client to use the standard 802.1x authentication protocol.
Command Mode: Global Mode.
Default: Private 802.1x authentication packet format is disabled by default.
Usage Guide: To implement Digital China Networks's integrated solution, the switch must be enabled to use DCN's private 802.1x protocol, or many applications will not be able to function. For detailed information, please refer to Digital China Networks's DCBI integrated solution. If the switch forces the authentication client to use Digital China Networks's private 802.1x protocol, the standard client will not be able to work.
Example: To force the authentication client to use Digital China Networks's private 802.1x authentication protocol.
Switch(config)#dot1x privateclient enable

7.3.24 dot1x privateclient protect enable

Command: dot1x privateclient protect enable
no dot1x privateclient protect enable
Function: Enable the privateclient protect function of the switch, the no command disables the protect function.
Parameter: None.
Command mode: Global Mode
Default: Disable the privateclient protect function.
Usage Guide: Support the partial encryption of the privateclient protocol to advance the security of the privateclient.
Example: Enable the privateclient protect function of the switch.
Switch(config)#dot1x privateclient protect enable

7.3.25 dot1x re-authenticate

Command: dot1x re-authenticate [interface <*interface-name*>] | port-channel <interface-name>
Function: Enables real-time 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.
Parameters: ***<interface-name>*** stands for port number, omitting the parameter for all ports.
Command mode: Global Mode.
Usage Guide: This command is a Global Mode command. It makes the switch to re-authenticate the client at once without waiting for re-authentication timer timeout. This command is no longer valid after authentication.
Example: Enabling real-time re-authentication on port1/0/8.
Switch(config)#dot1x re-authenticate interface ethernet 1/0/8

7.3.26 dot1x re-authentication

Command: dot1x re-authentication
no dot1x re-authentication
Function: Enables periodical supplicant authentication; the "no dot1x re-authentication" command disables this function.
Command mode: Global Mode.
Default: Periodical re-authentication is disabled by default.
Usage Guide: When periodical re-authentication for supplicant is enabled, the switch will re-authenticate the supplicant at regular interval. This function is not recommended for common use.
Example: Enabling the periodical re-authentication for authenticated users.
Switch(config)#dot1x re-authentication

7.3.27 dot1x timeout quiet-period

Command: dot1x timeout quiet-period <*seconds*>
no dot1x timeout quiet-period
Function: Sets time to keep silent on supplicant authentication failure; the "**no dot1x timeout quiet-period**" command restores the default value.
Parameters: ***<seconds>*** is the silent time for the port in seconds, the valid range is 1 to 65535.
Command mode: Global Mode.
Default: The default value is 10 seconds.
Usage Guide: Default value is recommended.
Example: Setting the silent time to 120 seconds.
Switch(config)#dot1x timeout quiet-period 120

7.3.28 dot1x timeout re-authperiod

Command: dot1x timeout re-authperiod <*seconds*>
no dot1x timeout re-authperiod
Function: Sets the supplicant re-authentication interval; the "**no dot1x timeout re-authperiod**" command restores the default setting.
Parameters: ***<seconds>*** is the interval for re-authentication, in seconds, the valid range is 1 to 65535.
Command mode: Global Mode.
Default: The default value is 3600 seconds.
Usage Guide: dot1x re-authentication must be enabled first before supplicant re-authentication interval can be modified. If authentication is not enabled for the switch, the supplicant re-authentication interval set will not take effect.
Example: Setting the re-authentication time to 1200 seconds.
Switch(config)#dot1x timeout re-authperiod 1200

7.3.29 dot1x timeout tx-period

Command: dot1x timeout tx-period <*seconds*>
no dot1x timeout tx-period
Function: Sets the interval for the supplicant to re-transmit EAP request/identity frame; the "**no dot1x timeout tx-period**" command restores the default setting.
Parameters: ***<seconds>*** is the interval for re-transmission of EAP request frames, in seconds; the valid range is 1 to 65535.
Command mode: Global Mode.
Default: The default value is 30 seconds.
Usage Guide: Default value is recommended.
Example: Setting the EAP request frame re-transmission interval to 1200 seconds.
Switch(config)#dot1x timeout tx-period 1200

7.3.30 dot1x unicast enable

Command: dot1x unicast enable
no dot1x unicast enable
Function: Enable the 802.1x unicast passthrough function of switch; the no operation of this command will disable this function.
Command mode: Global Configuration Mode.
Default: The 802.1x unicast passthrough function is not enabled in global mode.
Usage Guide: The 802.1x unicast passthrough authentication for the switch must be enabled first to enable the 802.1x unicast passthrough function, then the 802.1x function is configured.
Example: Enabling the 802.1x unicast passthrough function of the switch and enable the 802.1x for port 1/0/1.
Switch(config)#dot1x enable
Switch(config)# dot1x unicast enable
Switch(config)#interface ethernet1/0/1
Switch(Config-If-Ethernet1/0/1)#dot1x enable

7.3.31 dot1x web authentication enable

This command is not supported by switch.

7.3.32 dot1x web authentication ipv6 passthrough

This command is not supported by switch.

7.3.33 dot1x web redirect

This command is not supported by switch.

7.3.34 dot1x web redirect enable

This command is not supported by switch.

7.3.35 free-mac

Command: free-mac <source mac><wildcard bits>

no free-mac <source mac><wildcard bits>

Function: Add the free-authentication mac for the switch. The no command deletes it.

Parameters: <source mac> is the mac address of the free authentication user.

<wildcard bits> is the mask of the mac address of the free authentication user.

Command Mode: Global Mode.

Default: No configuration.

Usage Guide: For the special users, the free authentication mac can be used to allow the users. As the free authentication users, they can visit the resources without authentication. The mac address of the user can be appointed for no authentication and configure the mask as ff-ff-ff-ff-ff-ff. It can also configure the free authentication mac of multiple users and configure the mask as 0.

Example: Configure the free authentication MAC as 00-01-11-11-11-11.

Switch(config)# free-mac 00-01-11-11-11-11 ff-ff-ff-ff-ff-ff

7.3.36 show dot1x

Command**: show dot1x [interface <*interface-list*>]**

Function: Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.

Parameters: *<interface-list>* is the port list. If no parameter is specified, information for all ports is displayed.

Command mode: Admin and Configuration Mode.

Usage Guide: The dot1x related parameter and dot1x information can be displayed with 'show dot1x' command.

Example:

1. Display information about dot1x global parameter for the switch.

```
Switch#show dot1x
Global 802.1x Parameters
   reauth-enabled          no
   reauth-period           3600
   quiet-period            10
   tx-period               30
   max-req                 2
   authenticator mode      passive

Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable
```

dot1x-privateclient Disable
dot1x-unicast Disable

802.1x is enabled on ethernet Ethernet1/0/1
Authentication Method:Port based
Max User Number:1
  Status Authorized
  Port-control Auto
  Supplicant 00-03-0F-FE-2E-D3

Authenticator State Machine
  State Authenticated
Backend State Machine
  State Idle
Reauthentication State Machine
  State Stop

Displayed information	Explanation
Global 802.1x Parameters	Global 802.1x parameter information
reauth-enabled	Whether re-authentication is enabled or not
reauth-period	Re-authentication interval
quiet-period	Silent interval
tx-period	EAP retransmission interval
max-req	EAP packet retransmission interval
authenticator mode	Switch authentication mode
Mac Filter	Enables dot1x address filter or not
MacAccessList	Dot1x address filter table
dot1x-EAPoR	Authentication method used by the switch (EAP relay, EAP local end)
dot1x-privateclient	Whether the switch supports the privateclient
802.1x is enabled on ethernet Ethernet1/0/1	Indicates whether dot1x is enabled for the port
Authentication Method:	Port authentication method (MAC-based, port-based, user-based)
Status	Port authentication status
Port-control	Port authorization status
Supplicant	Authenticator MAC address
Authenticator State Machine	Authenticator state machine status
Backend State Machine	Backend state machine status
Reauthentication State Machine	Re-authentication state machine status

7.3.37 show dot1x user

Command: show dot1x user

Function: Show online users, who had passed the dot1x certification, information.

Command Mode: Admin and Configuration Mode.

Usage Gudie: Usually caring about online users information, other information used for technical support person to fault diagnose and troubleshooting.

Example: Show the information of online users who had passed dot1x certification.

Switch**(**config)# show dot1x user

---------- total authenticated users: 0 ----------

UserName	Port	OnTime(sec)	MAC	UserIP	UserIPv6

---------- total authenticated users: 0----------

7.3.38 clear dot1x all

Command: clear dot1x {all |interface <ethernet **IFNAME | IFNAME>|mac WORD |user WORD }**

Function: Delete the online users who had passed dot1x certification.

Parameters: <all>: Delete all dot1x online users

<IFNAME>: Delete dot1x online users in the specific port.

mac <WORD>: Delete dot1x online users in the specific mac address.

user <WORD>: Delete dot1x online users in the specific user name.

Command Mode: Admin Mode.

Usage Gudie: Users use this command can delete the specific mac address, port , user name or all dot1x online users from switch.

Example: Delete all online dot1x users.

Switch#clear dot1x all

7.3.39 user-control limit ipv4

This command is not supported by the switch.

7.3.40 user-control limit ipv6

This command is not supported by the switch.

7.3.41 vlan-pool

This command is not supported by the switch.

7.4 The Number Limitation Function of MAC and IP in Port, VLAN

7.4.1 debug ip arp count

Command: debug ip arp count

no debug ip arp count

Function: When the number limitation function debug of ARP in the VLAN, if the number of dynamic ARP and the number of ARP in the VLAN is larger than the max number allowed, users will see debug information. "**no debug ip arp count**" command is used to disable the number limitation function debug of ARP in the VLAN.

Parameters: None.

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide: Display the debug information of the number of dynamic ARP in the VLAN.

Examples:

Switch#debug vlan mac count

%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in vlan 1!!

%Jun 14 16:04:40 2007Arp learning will be stopped and some arp will be delete !!

7.4.2 debug ipv6 nd count

Command: debug ipv6 nd count

no debug ipv6 nd count

Function: When the number limitation function debug of neighbor in the VLAN, if the number of dynamic neighbor and the number of neighbor in the VLAN is larger than the max number allowed, users will see debug information. "**no debug ip neighbor count**" command is used to disable the number limitation function debug of neighbor in the VLAN.

Parameters: None.

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide: Display the debug information of the number of dynamic neighbor in the VLAN.

Examples:

Switch#debug vlan mac count

%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in vlan 1!!

7.4.3 debug switchport arp count

Command: debug switchport arp count

no debug switchport arp count

Function: When the number limitation function debug of ARP on the port, if the number of dynamic ARP and the number of ARP on the port is larger than the max number allowed, users will see debug information. "**no debug switchport arp count**" command is used to disable the number limitation function debug of ARP on the port.

Parameters: None

Command Mode: Admin Mode

Default Settings: None

Usage Guide: Display the debug information of the number of dynamic ARP on the port.

Examples:

Switch#debug switchport arp count

%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in port Ethernet1/0/1

!!%Jun 14 16:04:40 2007 Arp learning will be stopped and some mac will be delete !!

7.4.4 debug switchport mac count

Command: debug switchport mac count

no debug switchport **mac count**

Function: When the number limitation function debug of MAC on the port, if the number of dynamic MAC and the number of MAC on the port is larger than the max number allowed, users will see debug information. 'no **debug switchport mac count'** command is used to disable the number limitation function debug of MAC on the port.

Parameters: None

Command Mode: Admin Mode

Default Settings: None

Usage Guide: Display the debug information of the number of dynamic MAC on the port.

Examples:

Switch#debug switchport mac count

%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in port Ethernet1/0/1

!!%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!

7.4.5 debug switchport nd count

Command: debug switchport nd count

no debug switchport nd count

Function: When the number limitation function debug of ND on the port, if the number of dynamic ND and the number of ND on the port is larger than the max number allowed, users will see debug information. "**no debug switchport nd count**" command is used to disable the number limitation function debug of ND on the port.

Parameters: None
Command Mode: Admin Mode
Default Settings: None
Usage Guide: Display the debug information of the number of dynamic ND on the port
Examples:
Switch#debug switchport arp count
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in port Ethernet1/0/1
!!%Jun 14 16:04:40 2007 Neighbor learning will be stopped and some mac will be delete !!

7.4.6 debug vlan mac count

Command: debug vlan mac count
no debug vlan **mac count**
Function: When the number limitation function debug of MAC in the VLAN, if the number of dynamic MAC and the number of MAC in the VLAN is larger than the max number allowed, users will see debug information. 'no **debug vlan mac count'** command is used to disable the number limitation function debug of MAC in the VLAN.
Parameters: None.
Command Mode: Admin Mode.
Default Settings: None.
Usage Guide: Display the debug information of the number of dynamic MAC in the VLAN.
Examples:
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in vlan 1!!
%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!

7.4.7 ip arp dynamic maximum

Command: ip arp dynamic maximum *<value>*
no ip arp dynamic maximum
Function: Set the max number of dynamic ARP allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic ARP in the VLAN; "**no ip arp dynamic maximum**" command is used to disable the number limitation function of dynamic ARP in the VLAN.
Parameters: *<value>* upper limit of the number of dynamic ARP in the VLAN, ranging from 1 to 4096.
Default Settings: The number limitation function of dynamic ARP in the VLAN is disabled.
Command Mode: Interface Configuration Mode.
Usage Guide: When configuring the max number of dynamic ARP allowed in the VLAN, if the

number of dynamically learnt ARP in the VLAN is already larger than the max number to be set, the extra dynamic ARP will be deleted.

Examples:

Enable the number limitation function of dynamic ARP in VLAN 1, the max number to be set is 50.

Switch(config)#interface ethernet

Switch(Config-if-Vlan1)# ip arp dynamic maximum 50

Disable the number limitation function of dynamic ARP in VLAN 1.

Switch(Config-if-Vlan1)#no ip arp dynamic maximum

7.4.8 ipv6 nd dynamic maximum

Command: ipv6 nd dynamic maximum *<value>*

no ipv6 nd dynamic maximum

Function: Set the max number of dynamic NEIGHBOR allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic NEIGHBOR in the VLAN; "**no ipv6 nd dynamic maximum**" command is used to disable the number limitation function of dynamic NEIGHBOR in the VLAN.

Parameters: *<value>* upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic NEIGHBOR in the VLAN is disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: When configuring the max number of dynamic NEIGHBOR allowed in the VLAN, if the number of dynamically learnt NEIGHBOR in the VLAN is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted.

Examples:

Enable the number limitation function of dynamic NEIGHBOR in VLAN 1, the max number to be set is 50.

Switch(config)#interface ethernet

Switch(Config-if-Vlan1)# ipv6 nd dynamic maximum 50

Disable the number limitation function of dynamic NEIGHBOR in VLAN 1.

Switch(Config-if-Vlan1)#no ipv6 nd dynamic maximum

7.4.9 mac-address query timeout

Command: mac-address query timeout <seconds>

Function: Set the timeout value of querying dynamic MAC.

Parameter: *<seconds>* is timeout value, in second, ranging from 30 to 300.

Default Settings: Default value is 60 seconds.

Command Mode: Global mode

Usage Guide: After enabling the number limitation of MAC, users can use this command to configure the timeout value of querying dynamic MAC. If the data traffic is very large, the timeout value can be shorter, otherwise, it can be longer. Users can set it according to actual

situation.

Examples:

Set the timeout value of quering dynamic MAC as 30 seconds.

Switch(config)#mac-address query timeout 30

7.4.10 show arp-dynamic count

Command: show arp-dynamic count {(vlan <1-4096>)| interface ethernet *<portName>*}

Function: Display the number of dynamic ARP of corresponding port and VLAN.

Parameters: *<vlan-id>* is the specified vlan ID.

<portName> is the name of layer-2 port.

Command Mode: Admin and Configuration Mode.

Usage Guide: Use this command to display the number of dynamic ARP of corresponding port and VLAN.

Examples: Display the number of dynamic ARP of the port and VLAN which are configured with number limitation function of ARP.

Switch(config)# show arp-dynamic count interface ethernet 1/0/3

Port	MaxCount	CurrentCount
Ethernet1/0/3	5	1

Switch(config)# show arp-dynamic count vlan 1

Vlan	MaxCount	CurrentCount
1	55	15

7.4.11 show mac-address dynamic count

Command: show mac-address dynamic count { (vlan <1-4096>)| interface ethernet *<portName>*}

Function: Display the number of dynamic MAC of corresponding port and VLAN.

Parameters: *<vlan-id>* display the specified VLAN ID.

<portName> is the name of layer-2 port.

Command Mode: Admin and Configuration Mode

Usage Guide: Use this command to display the number of dynamic MAC of corresponding port and VLAN.

Examples: Display the number of dynamic MAC of the port and VLAN which are configured with number limitation function of MAC.

Switch(config)# show mac-address dynamic count interface ethernet 1/0/3

Port	MaxCount	CurrentCount

```
 Ethernet1/0/3                5                    1
-----------------------------------------------------------------------------------------------
Switch(config)# show mac-address dynamic count vlan 1
 Vlan                MaxCount                CurrentCount
-----------------------------------------------------------------------------------------------
 1                      55                    15
-----------------------------------------------------------------------------------------------
```

7.4.12 show nd-dynamic count

Command: show nd-dynamic count {(vlan <1-4096>)| interface ethernet *<portName>*}

Function: Display the number of dynamic ND of corresponding port and VLAN.

Parameters: ***<vlan-id>*** is play the specified vlan ID. ***<portName>*** is the name of layer-2 port.

Command Mode: Admin and Configuration Mode.

Usage Guide: Use this command to display the number of dynamic ND of corresponding port and VLAN.

Examples: Display the number of dynamic ND of the port and VLAN which are configured with number limitation function of ND.

```
Switch(config)# show nd-dynamic count interface ethernet 1/0/3
 Port                MaxCount                CurrentCount
-----------------------------------------------------------------------------------------------
 Ethernet1/0/3                5                    1
-----------------------------------------------------------------------------------------------
Switch(config)# show nd-dynamic count vlan 1
 Vlan                MaxCount                CurrentCount
-----------------------------------------------------------------------------------------------
 1                      55                    15
-----------------------------------------------------------------------------------------------
```

7.4.13 switchport arp dynamic maximum

Command: switchport arp dynamic maximum *<value>*

no switchport arp dynamic maximum

Function: Set the max number of dynamic ARP allowed by the port, and, at the same time, enable the number limitation function of dynamic ARP on the port; "**no switchport arp dynamic maximum**" command is used to disable the number limitation function of dynamic ARP on the port.

Parameters: ***<value>*** upper limit of the number of dynamic ARP of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic ARP allowed by the port, if the number of dynamically learnt ARP on the port is already larger than the max number to be set,

the extra dynamic ARP will be deleted. TRUNK ports do not supports this function.

Examples:

Enable the number limitation function of dynamic ARP in port 1/0/2 mode, the max number to be set is 20

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# switchport arp dynamic maximum 20

Disable the number limitation function of dynamic ARP in port 1/0/2 mode

Switch(Config-If-Ethernet1/0/2)#no switchport arp dynamic maximum

7.4.14 switchport mac-address dynamic maximum

Command: switchport mac-address dynamic maximum <value>

no **switchport mac-address dynamic maximum**

Function: Set the max number of dynamic MAC address allowed by the port, and, at the same time, enable the number limitation function of dynamic MAC address on the port; 'no **switchport mac-address dynamic maximum'** command is used to disable the number limitation function of dynamic MAC address on the port.

Parameters: <*value*> upper limit of the number of dynamic MAC address of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic MAC address on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic MAC address allowed by the port, if the number of dynamically learnt MAC address on the port is already larger than the max number of dynamic MAC address to be set, the extra dynamic MAC addresses will be deleted. This function is mutually exclusive to functions such as dot1x, MAC binding, if the functions of dot1x, MAC binding or TRUNK are enabled on the port, this function will not be allowed.

Examples:

Enable the number limitation function of dynamic MAC address in port 1/0/2 mode, the max number to be set is 20

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# switchport mac-address dynamic maximum 20

Disable the number limitation function of dynamic MAC address in port 1/0/2 mode

Switch(Config-If-Ethernet1/0/2)#no switchport mac-address dynamic maximum

7.4.15 switchport mac-address violation

Command: switchport mac-address violation {protect | shutdown**}** [recovery <5-3600>]

no switchport mac-address violation

Function: Set the violation mode of the port, the no command restores the violation mode to protect.

Parameters: protect: protect mode

shutdown: shutdown mode

recovery: Configure the border port to automatically restore after execute shutdown violation mode

<5-3600>: Recovery time, do not restore by default

Command Mode: Port mode

Default: protect mode

Usage Guide: The port sets the violation mode after enable the number limit function of MAC only. If the violation mode is protect, the port only disable the dynamic MAC address learning function when the MAC address number of the port exceeds the upper limit of secure MAC. If the violation mode is shutdown, the port will be disabled when the MAC address number exceeds the upper limit of secure MAC, and the user can enable the port by configuring no shutdown command manually or the automatic recovery timeout.

Example: Set the violation mode as shutdown, the recovery time as 60s for port1.

Switch(config)#interface Ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#switchport mac-address violation shutdown recovery 60

7.4.16 switchport nd dynamic maximum

Command: switchport nd dynamic maximum *<value>*

no switchport nd dynamic maximum

Function: Set the max number of dynamic NEIGHBOR allowed by the port, and, at the same time, enable the number limitation function of dynamic NEIGHBOR on the port; "**no switchport nd dynamic maximum**" command is used to disable the number limitation function of dynamic NEIGHBOR on the port.

Parameters: *<value>* upper limit of the number of dynamic NEIGHBOR of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic NEIGHBOR allowed by the port, if the number of dynamically learnt NEIGHBOR on the port is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. TRUNK ports do not supports this function.

Examples:

Enable the number limitation function of dynamic NEIGHBOR in port 1/0/2 mode, the max number to be 20.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# switchport nd dynamic maximum 20

Disable the number limitation function of dynamic NEIGHBOR in port 1/0/2 mode

Switch(Config-If-Ethernet1/0/2)#no switchport nd dynamic maximum

7.4.17 vlan mac-address dynamic maximum

Command: vlan mac-address dynamic maximum <*value*>

no **vlan mac-address dynamic maximum**

Function: Set the max number of dynamic MAC address allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic MAC address in the VLAN; 'no **ip mac-address dynamic maximum'** command is used to disable the number limitation function of dynamic MAC address in the VLAN.

Parameters: <*value*> upper limit of the number of MAC address in the VLAN, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic MAC address in the VLAN is disabled.

Command Mode: VLAN Configuration Mode.

Usage Guide: When configuring the max number of dynamic MAC allowed in the VLAN, if the number of dynamically learnt MAC address in the VLAN is already larger than the max number to be set, the extra dynamic MAC addresses will be deleted. After enabling number limitation function of dynamic MAC in the VLAN, the number limitation of MAC is only applied to general access port, the number of MAC on TURNK ports and special ports which has enabled dot1x, MAC binding function will not be limited or counted.

Examples: Enable the number limitation function of dynamic MAC address in VLAN 1, the max number to be set is 50.

Switch(config)#vlan1

Switch(Config-if-Vlan1)#vlan mac-address dynamic maximum 50

Enable the number limitation function of dynamic MAC address in VLAN 1.

Switch(Config-if-Vlan1)#no vlan mac-address dynamic maximum

7.5 AM

7.5.1 am enable

Command: am enable

no am enable

Function: Globally enable/disable AM function.

Parameters: None.

Default: AM function is disabled by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: Enable AM function on the switch.

Switch(config)#am enable

Disable AM function on the switch.

Switch(config)#no am enable

7.5.2 am port

Command: am iport

no am port

Function: Enable/disable AM function on port.

Parameters: None.

Default: AM function is disabled on all port.

Command Mode: Port Mode.

Example: Enable AM function on interface 1/0/3 of the switch.

Switch(Config-If-Ethernet 1/0/3)#am port

Disable AM function on interface 1/0/3 of the switch.

Switch(Config-If-Ethernet 1/0/3)#no am port

7.5.3 am ip-pool

Command: am ip-pool *<ip-address> <num>*

no am ip-pool *<ip-address> <num>*

Function: Set the AM IP segment of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.

Parameters: ***<ip-address>*** the starting address of an address segment in the IP address pool; ***<num>*** is the number of consecutive addresses following ip-address, less than or equal with 32.

Default: IP address pool is empty.

Command Mode: Port Mode.

Usage Guide: None.

Example: Configure that interface 1/0/3 of the switch will forward data packets from an IP address which is one of 10 consecutive IP addresses starting from 10.10.10.1.

Switch(Config-If-Ethernet 1/0/3)#am ip-pool 10.10.10.1 10

7.5.4 am mac-ip-pool

Command: am mac-ip-pool *<mac-address> <ip-address>*

no am mac-ip-pool *<mac-address> <ip-address>*

Function: Set the AM MAC-IP address of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.

Parameter: ***<mac-address>*** is the source MAC address; ***<ip-address>*** is the source IP address of the packets, which is a 32 bit binary number represented in four decimal numbers.

Default: MAC-IP address pool is empty.

Command Mode: Port Mode.

Usage Guide: None.

Example: Configure that the interface 1/0/3 of the switch will allow data packets with a source MAC address of 11-22-22-11-11-11 and a source IP address of 10.10.10.1 to be forwarded.

Switch(Config-If-Ethernet1/0/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1

7.5.5 no am all

Command: no am all [ip-pool | mac-ip-pool]
Function: Delete MAC-IP address pool or IP address pool or both pools configured by all users.
Parameters: ip-pool is the IP address pool; **mac-ip-pool** is the MAC-IP address pool; no parameter means both address pools.
Default: Both address pools are empty at the beginning.
Command Mode: Global Mode
Usage Guide: None.
Example: Delete all configured IP address pools.
Switch(config)#no am all ip-pool

7.5.6 show am

Command: show am [interface *<interface-name>*]
Function: Display the configured AM entries.
Parameters: ***<interface-name>*** is the name of the interface of which the configuration information will be displayed. No parameter means to display the AM configuration information of all interfaces.
Command Mode: Admin and Configuration Mode.
Example: Display all configured AM entries.
Switch#show am
AM is enabled

Interface Ethernet1/0/3
    am interface
    am ip-pool 30.10.10.1 20
Interface Ethernet1/0/5
  am port
  am ip-pool 50.10.10.1 30
  am mac-ip-pool 00-02-04-06-08-09 20.10.10.5
  am ip-pool 50.20.10.1 20
Interface Ethernet1/0/6
  am port
Interface Ethernet1/0/1
    am interface
    am ip-pool 10.10.10.1 20
    am ip-pool 10.20.10.1 20

Display the AM configuration entries of ehternet1/0/5 of the switch.
Switch#show am interface ethernet 1/0/5
AM is enabled

Interface Etherne1/0/5
    am interface

```
        am ip-pool 50.10.10.1    30
        am mac-ip-pool    00-02-04-06-08-09 20.10.10.5
am ip-pool 50.20.10.1    20
```

7.6 Security Feature

7.6.1 dosattack-check srcip-equal-dstip enable

Command: [no] dosattack-check srcip-equal-dstip enable

Function: Enable the function by which the switch checks if the source IP address is equal to the destination IP address; the “no” form of this command disables this function.

Parameter: None

Default: Disable the function by which the switch checks if the source IP address is equal to the destination IP address.

Command Mode: Global Mode

Usage Guide: By enabling this function, data packet whose source IP address is equal to its destination address will be dropped.

Example: Drop the data packet whose source IP address is equal to its destination address.l

Switch(config)# dosattack-check srcip-equal-dstip enable

7.6.2 dosattack-check ipv4-first-fragment enable

This command is not supported by switch.

7.6.3 dosattack-check tcp-flags enable

Command: [no] dosattack-check tcp-flags enable

Function: Enable the function by which the switch will check the unauthorized TCP label function; the “no” form of this command will disable this function.

Parameter: None

Default: This function disable on the switch by default

Command Mode: Global Mode

Usage Guide: With this function enabled, the switch will be able to drop follow four data packets containing unauthorized TCP label: SYN=1 while source port is smaller than 1024;TCP label positions are all 0 while its serial No. =0;FIN=1,URG=1,PSH=1 and the TCP serial No.=0;SYN=1 and FIN=1. This function can be used associating the “dosattack-check ipv4-first-fragment enable” command.

Example: Drop one or more types of above four packet types.

Switch(config)#dosattack-check tcp-flags enable

7.6.4 dosattack-check srcport-equal-dstport enable

Command: dosattack-check srcport-equal-dstport enable

no dosattack-check srcport-equal-dstport enable

Function: Enable the function by which the switch will check if the source port is equal to the destination port; the no command disables this function.

Parameter: None

Default: Disable the function by which the switch will check if the source port is equal to the destination port.

Command Mode: Global Mode

Usage Guide: With this function enabled, the switch will be able to drop TCP and UDP data packet whose destination port is equal to the source port. This function can be used associating the “dosattack-check ipv4-first-fragment enable” function so to block the IPv4 fragment TCP and UDP data packet whose destination port is equal to the source port.

Example: Drop the non-fragment TCP and UDP data packet whose destination port is equal to the source port.

Switch(config)#dosattack-check srcport-equal-dstport enable

7.6.5 dosattack-check tcp-fragment enable

This command is not supported by switch.

7.6.6 dosattack-check tcp-segment

This command is not supported by switch.

7.6.7 dosattack-check icmp-attacking enable

Command: [no] dosattack-check icmp-attacking enable

Function: Enable the ICMP fragment attack checking function on the switch; the “no” form of this command disables this function.

Parameter: None

Default: Disable the ICMP fragment attack checking function on the switch

Command Mode: Global Mode

Usage Guide: With this function enabled the switch will be protected from the ICMP fragment attacks, dropping the fragment ICMPv4/v6 data packets whose net length is smaller than the specified value.

Example: Enable the ICMP fragment attack checking function.

Switch(config)#dosattack-check icmp-attacking enable

7.6.8 dosattack-check icmpV4-size

This command is not supported by switch.

7.6.9 dosattack-check icmpv6-size

This command is not supported by switch.

7.6.10 invalid-dip-drop

Command: invalid-dip-drop {enable|disable}
Function: IPv4 destination IP checking for illegal function, Illegal IP will be drop and sent to the CPU to record information.
Parameter: enable enable function**, disable** disable function.
Default: The value is **disable** by default。
Command Mode: Global Mode。
Usage Guide: Illegal destination IP includes X.X.X. 0, 127.X.X.X, 240.0.0.0~255.255.255.254.
Example: Enable function.
Switch(config)#invalid-dip-drop enable

7.7 TACACS+

7.7.1 tacacs-server authentication host

Command: tacacs-server authentication host {{vrf <vrf-name>| } <ip-address>} [port <*port-number*>] [timeout <*seconds*>] [key {0 | 7} <*string*>] [primary]
no tacacs-server authentication host <*ip-address*>
Function: Configure the IP address, listening port number, the value of timeout timer and the key string of the TACACS+ server; the no form of this command deletes TACACS+ authentication server.
Parameter: <vrf-name> is the specific VRF name；*<ip-address>* is the IP address of the server; ***<port-number>*** is the listening port number of the server, the valid range is 0~65535, amongst 0 indicates it will not be an authentication server; ***<seconds>*** is the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60; ***<string>*** is the key string, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters; **primary** indicates it's a primary server.

Command Mode: Global Mode

Default: No TACACS+ authentication configured on the system by default.

Usage Guide: This command is for specifying the IP address, port number, timeout timer value and the key string of the TACACS+ server used on authenticating with the switch. The parameter port is for define an authentication port number which must be in accordance with the authentication port number of specified TACACS+ server which is 49 by default. The parameters key and timeout is used to configure the self-key and self-timeout, if the switch is not configure the timeout<*seconds*> and key<string>, it will use the global value and key by command tacacs-server timeout<*seconds*> and tacacs-server key <string>. This command can configure several TACACS+ servers communicate with the switch. The configuration sequence will be used as authentication server sequence. And in case **primary** is configured on one TACACS+ server, the server will be the primary server.

Example: Configure the TACACS+ authentication server address to 192.168.1.2, and use the global configured key.

Switch(config)#tacacs-server authentication host 192.168.1.2

7.7.2 tacacs-server key

Command: tacacs-server key {0 | 7} *<string>*

no tacacs-server key

Function: Configure the key of TACACS+ authentication server; the "**no tacacs-server key**" command deletes the TACACS+ server key.

Parameter: *<string>* is the key string of the TACACS+ server. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters.

Command Mode: Global Mode

Usage Guide: The key is used on encrypted packet communication between the switch and the TACACS+ server. The configured key must be in accordance with the one on the TACACS+ server or else no correct TACACS+ authentication will be performed. It is recommended to configure the authentication server key to ensure the data security.

Example: Configure test as the TACACS+ server authentication key.

Switch(config)#tacacs-server key 0 test

7.7.3 tacacs-server nas-ipv4

Command: tacacs-server nas-ipv4 <ip-address>

no tacacs-server nas-ipv4

Function: Configure the source IP address of TACACS+ packet sent by the switch; the "**no tacacs-server nas-ipv4**" command deletes the configuration.

Parameter: <ip-address> is the source IP address of TACACS+ packet, in dotted decimal notation, it must be a valid unicast IP address.

Default: No specific source IP address for TACACS+ packet is configured, the IP address of the interface from which the TACACS+ packets are sent is used as source IP address of TACACS+

packet.

Command Mode: Global Mode

Usage Guide: The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send TACACS+ packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from TACACS+ server are dropped when the interface link-down.

Example: Configure the source ip address of TACACS+ packet as 192.168.2.254.

Switch#tacacs-server nas-ipv4 192.168.2.254

7.7.4 tacacs-server timeout

Command: tacacs-server timeout *<seconds>*

no tacacs-server timeout

Function: Configure a TACACS+ server authentication timeout timer; the "**no tacacs-server timeout**" command restores the default configuration.

Parameter: ***<seconds>*** is the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60.

Command Mode: Global Mode

Default: 3 seconds by default.

Usage Guide: The command specifies the period the switch wait for the authentication through TACACS+ server. When connected to the TACACS+, and after sent the authentication query data packet to the TACACS+ server, the switch waits for the response. If no replay is received during specified period, the authentication is considered failed.

Example: Configure the timeout timer of the tacacs+ server to 30 seconds.

Switch(config)#tacacs-server timeout 30

7.7.5 debug tacacs-server

Command: debug tacacs-server

no debug tacacs-server

Function: Open the debug message of the TACACS+; the "**no debug tacacs-server**" command closes the TACACS+ debugging messages.

Command Mode: Admin Mode

Parameter: None.

Usage Guide: Enable the TACACS+ debugging messages to check the negotiation process of the TACACS+ protocol which can help detecting the failure.

Example: Enable the debugging messages of the TACACS+ protocol.

Switch#debug tacacs-server

7.8 RADIUS

7.8.1 aaa enable

Command: aaa enable

no aaa enable

Function: Enables the AAA authentication function in the switch; the "no AAA enable" command disables the AAA authentication function.

Command mode: Global Mode.

Parameters: No.

Default: AAA authentication is not enabled by default.

Usage Guide: The AAA authentication for the switch must be enabled first to enable IEEE 802.1x authentication for the switch.

Example: Enabling AAA function for the switch.

Switch(config)#aaa enable

7.8.2 aaa-accounting enable

Command: aaa-accounting enable

no aaa-accounting enable

Function: Enables the AAA accounting function in the switch: the "no aaa-accounting enable" command disables the AAA accounting function.

Command mode: Global Mode

Default: AAA accounting is not enabled by default.

Usage Guide: When accounting is enabled in the switch, accounting will be performed according to the traffic or online time for port the authenticated user is using. The switch will send an “accounting started” message to the RADIUS accounting server on starting the accounting, and an accounting packet for the online user to the RADIUS accounting server every five seconds, and an “accounting stopped” message is sent to the RADIUS accounting server on accounting end. Note: The switch send the “user offline” message to the RADIUS accounting server only when accounting is enabled, the “user offline” message will not be sent to the RADIUS authentication server.

Example: Enabling AAA accounting for the switch.

Switch(config)#aaa-accounting enable

7.8.3 aaa-accounting update

Command: aaa-accounting update {enable | disable}

Function: Enable or disable the AAA update accounting function.

Command Mode: Global Mode.

Default: Enable the AAA update accounting function.

Usage Guide: After the update accounting function is enabled, the switch will sending accounting

message to each online user on time.

Example: Disable the AAA update accounting function for switch.

Switch(config)#aaa-accounting update disable

7.8.4 aaa group server radius

This command is not supported by the switch.

7.8.5 debug aaa packet

Command: debug aaa packet {send | receive | all} interface {ethernet *<interface-number>* | *<interface-name>*}

no debug aaa packet {send | receive | all} interface {ethernet *<interface-number>* | *<interface-name>*}

Function: Enable the debug information of AAA about receiving and sending packets; the no operation of this command will disable such debug information.

Parameters: send: Enable the debug information of AAA about sending packets.

receive: Enable the debug information of AAA about receiving packets.

all: Enable the debug information of AAA about both sending and receiving packets.

***<interface-number>*:** the number of interface.

***<interface-name>*:** the name of interface.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of AAA about sending and receiving packets, users can check the messages received and sent by Radius protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of AAA about sending and receiving packets on interface1/0/1.

Switch#debug aaa packet all interface Ethernet 1/0/1

7.8.6 debug aaa detail attribute

Command: debug aaa detail attribute interface {ethernet *<interface-number>* | *<interface-name>*}

no debug aaa detail attribute interface {ethernet *<interface-number>* | *<interface-name>*}

Function: Enable the debug information of AAA about Radius attribute details; the no operation of this command will disable that debug information.

Parameters: *<interface-number>*: the number of the interface.

***<interface-name>*:** the name of the interface.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of AAA about Radius attribute details, users can check Radius attribute details of Radius messages, which might help diagnose the cause of faults

if there is any.

Example: Enable the debug information of aaa about Radius attribute details on interface 1/0/1.

Switch#debug aaa detail attribute interface Ethernet 1/0/1

7.8.7 debug aaa detail connection

Command: debug aaa detail connection

no debug aaa detail connection

Function: Enable the debug information of aaa about connection details; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of aaa about connection details, users can check connection details of aaa, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of aaa about connection details.

Switch#debug aaa detail connection

7.8.8 debug aaa detail escape

This command is not supported by the switch.

7.8.9 debug aaa detail event

Command: debug aaa detail event

no debug detail event

Function: Enable the debug information of aaa about events; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of aaa about events, users can check the information of all kinds of event generated in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of aaa about events.

Switch#debug aaa detail event

7.8.10 debug aaa error

Command: debug aaa error

no debug error

Function: Enable the debug information of aaa about errors; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of aaa about errors, users can check the information of all kinds of errors that occurs in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of aaa about errors.

Switch#debug aaa error

7.8.11 radius nas-ipv4

Command: radius nas-ipv4 <*ip-address*>

no radius nas-ipv4

Function: Configure the source IP address for RADIUS packet sent by the switch. The "**no radius nas-ipv4**" command deletes the configuration.

Parameter: ***<ip-address>*** is the source IP address of the RADIUS packet, in dotted decimal notation, it must be a valid unicast IP address.

Default: No specific source IP address for RADIUS packet is configured, the IP address of the interface from which the RADIUS packets are sent is used as source IP address of RADIUS packet.

Command mode: Global Mode.

Usage guide: The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send RADIUS packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from RADIUS server are dropped when the interface link-down.

Example: Configure the source ip address of RADIUS packet as 192.168.2.254.

Switch#radius nas-ipv4 192.168.2.254

7.8.12 radius nas-ipv6

Command: radius nas-ipv6 <ipv6-address>

no radius nas-ipv6

Function: Configure the source IPv6 address for RADIUS packet sent by the switch. The no command deletes the configuration.

Parameter: ***<ipv6-address>*** is the source IPv6 address of the RADIUS packet, it must be a valid unicast IPv6 address.

Default: No specific source IPv6 address for RADIUS packet is configured, the IPv6 address of the interface from which the RADIUS packets are sent is used as source IPv6 address of RADIUS packet.

Command mode: Global Mode.

Usage guide: The source IPv6 address must belongs to one of the IPv6 interface of the switch, otherwise a failure message of binding IPv6 address will be returned when the switch send RADIUS packet. We suggest using the IPv6 address of loopback interface as source IPv6 address, it avoids that the packets from RADIUS server are dropped when the interface link-down.

Example: Configure the source ipv6 address of RADIUS packet as 2001:da8:456::1.

Switch#radius nas-ipv6 2001:da8:456::1

7.8.13 radius-server accounting host

Command: radius-server accounting host (vrf <vrfname>){<*ipv4-address*> | <*ipv6-address*>} [port <*port-number*>] [key {0 | 7} <*string*>] [primary]

no radius-server accounting host {<*ipv4-address*> | <*ipv6-address*>}

Function: Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server; the no command deletes the RADIUS accounting server.

Parameters: ***<ipv4-address> | <ipv6-address>*** stands for the server IPv4/IPv6 address;

<port-number> for server listening port number from 0 to 65535;

<vrfname> Vrf instance name

<string> is the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters;

primary for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if **primary** is not configured, otherwise, the specified RADIUS server will be used first.

Command Mode: Global Mode

Default: No RADIUS accounting server is configured by default.

Usage Guide: This command is used to specify the IPv4/IPv6 address and port number of the specified RADIUS server for switch accounting, multiple command instances can be configured. The ***<port-number>*** parameter is used to specify accounting port number, which must be the same as the specified accounting port in the RADIUS server; the default port number is 1813. If this port number is set to 0, accounting port number will be generated at random and can result in invalid configuration. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the switch will send accounting packets to all the configured accounting servers, and all the accounting servers can be backup servers for each other. If **primary** is specified, then the specified RADIUS server will be the primary server. It only configures a RADIUS primary server whether the server use IPv4 address or IPv6 address.

Example: Sets the RADIUS accounting server of IPv6 address to 2004:1:2:3::2, as the primary server, with the accounting port number as 3000.

Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary

7.8.14 radius-server authentication host

Command: radius-server authentication host {{vrf <vrf-name>| }<*ipv4-address*> | <*ipv6-address*>} [port <port-number>] [key *{0* | 7} <string>] [primary] [access-mode {dot1x | telnet}]

no radius-server authentication host {<*ipv4-address*> | <*ipv6-address*>}

Function: Specifies the IPv4 address or IPv6 address and listening port number, cipher key, whether be primary server or not and access mode for the RADIUS server; the no command deletes the RADIUS authentication server.

Parameters: <vrf-name> is the specific VRF name；

<ipv4-address> | <ipv6-address> stands for the server IPv4/IPv6 address;

<port-number> for listening port number, from 0 to 65535, where 0 stands for non-authentication server usage;

<string> is the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters;

primary for primary server. Multiple RADIUS Sever can be configured and would be available. RADIUS Server will be searched by the configured order if **primary** is not configured, otherwise, the specified RADIUS server will be used last.

[access-mode *{dot1x*/telnet}] designates the current RADIUS server only use 802.1x authentication or telnet authentication, all services can use current RADIUS server by default.

Command mode: Global Mode

Default: No RADIUS authentication server is configured by default.

Usage Guide: This command is used to specify the IPv4 address or IPv6 address and port number, cipher key string and access mode of the specified RADIUS server for switch authentication, multiple command instances can be configured. The port parameter is used to specify authentication port number, which must be the same as the specified authentication port in the RADIUS server, the default port number is 1812. If this port number is set to 0, the specified server is regard as non-authenticating. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the configured order is used as the priority for the switch authentication server. When the first server has responded (whether the authentication is successed or failed), switch does not send the authentication request to the next. If **primary** is specified, then the specified RADIUS server will be the primary server. It **will *use the* cipher key which be configured by radius-server key <string>** global command if the current RADIUS server not configure key<string>. Besides, it can designate the current RADIUS server only use 802.1x authentication or telnet authentication via access-mode option. It is not configure access-mode option and all services can use current RADIUS server by default.

Example: Setting the RADIUS authentication server address as 2004:1:2:3::2.

Switch(config)#radius-server authentication host 2004:1:2:3::2

7.8.15 radius-server dead-time

Command: radius-server dead-time <*minutes*>

no radius-server dead-time

Function: Configures the restore time when RADIUS server is down; the "**no radius-server dead-time**" command restores the default setting.

Parameters: *<minute>* is the down -restore time for RADIUS server in minutes, the valid range is 1 to 255.

Command mode: Global Mode

Default: The default value is 5 minutes.

Usage Guide: This command specifies the time to wait for the RADIUS server to recover from inaccessible to accessible. When the switch acknowledges a server to be inaccessible, it marks that server as having invalid status, after the interval specified by this command; the system

resets the status for that server to valid.

Example: Setting the down-restore time for RADIUS server to 3 minutes.

Switch(config)#radius-server dead-time 3

7.8.16 radius-server key

Command: radius-server key {0 | 7} <*string*>

no radius-server key

Function: Specifies the key for the RADIUS server (authentication and accounting); the "no radius-server key" command deletes the key for RADIUS server.

Parameters: ***<string>*** is a key string for RADIUS server, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters.

Command mode: Global Mode

Usage Guide: The key is used in the encrypted communication between the switch and the specified RADIUS server. The key set must be the same as the RADIUS server set, otherwise, proper RADIUS authentication and accounting will not perform properly.

Example: Setting the RADIUS authentication key to be "test".

Switch(config)#radius-server key 0 test

7.8.17 radius-server retransmit

Command: radius-server retransmit <*retries*>

no radius-server retransmit

Function: Configures the re-transmission times for RADIUS authentication packets; the "**no radius-server retransmit**" command restores the default setting.

Parameters: ***<retries>*** is a retransmission times for RADIUS server, the valid range is 0 to 100.

Command mode: Global Mode

Default: The default value is 3 times.

Usage Guide: This command specifies the retransmission time for a packet without a RADIUS server response after the switch sends the packet to the RADIUS server. If authentication information is missing from the authentication server, AAA authentication request will need to be re-transmitted to the authentication server. If AAA request retransmission count reaches the retransmission time threshold without the server responding, the server will be considered to as not work, the switch sets the server as invalid.

Example: Setting the RADIUS authentication packet retransmission time to five times.

Switch(config)#radius-server retransmit 5

7.8.18 radius-server timeout

Command: radius-server timeout <*seconds*>

no radius-server timeout

Function: Configures the timeout timer for RADIUS server; the "**no radius-server timeout**"

command restores the default setting.

Parameters: ***<seconds>*** is the timer value (second) for RADIUS server timeout, the valid range is 1 to 1000.

Command mode: Global Mode

Default: The default value is 3 seconds.

Usage Guide: This command specifies the interval for the switch to wait RADIUS server response. The switch waits for corresponding response packets after sending RADIUS Server request packets. If RADIUS server response is not received in the specified waiting time, the switch resends the request packet or sets the server as invalid according to the current conditions.

Example: Setting the RADIUS authentication timeout timer value to 30 seconds.

Switch(config)#radius-server timeout 30

7.8.19 radius-server accounting-interim-update timeout

Command: radius-server accounting-interim-update timeout <*seconds*>

no radius-server accounting-interim-update timeout

Function: Set the interval of sending fee-counting update messages; the no operation of this command will reset to the default configuration.

Parameters: ***<seconds>*** is the interval of sending fee-counting update messages, in seconds, ranging from 60 to 3600.

Command Mode: Global Mode.

Default: The default interval of sending fee-counting update messages is 300 seconds.

User Guide: This command set the interval at which NAS sends fee-counting update messages. In order to realize the real time fee-counting of users, from the moment the user becomes online, NAS will send a fee-counting update message of this user to the RADIUS server at the configured interval.

The interval of sending fee-counting update messages is relative to the maximum number of users supported by NAS. The smaller the interval, the less the maximum number of the users supported by NAS; the bigger the interval, the more the maximum number of the users supported by NAS. The following is the recommended ratio of interval of sending fee-counting update messages to the maximum number of the users supported by NAS:

Table 8-1 The recommended ratio of the interval of sending fee-counting update messages to the maximum number of the users supported by NAS

The maximum number of users	The interval of sending fee-counting update messages(in seconds)
1~299	300（default value）
300~599	600
600~1199	1200
1200~1799	1800
≥1800	3600

Example: The maximum number of users supported by NAS is 700, the interval of sending

fee-counting update messages 1200 seconds.
Switch(config)#radius-server accounting-interim-update timeout 1200

7.8.20 server

This command is not supported by the switch.

7.8.21 show aaa authenticated-user

Command: show aaa authenticated-user
Function: Displays the authenticated users online.
Command mode: Admin and Configuration Mode.
Usage Guide: Usually the administrator concerns only information about the online user, the other information displayed is used for troubleshooting by technical support.
Example:
Switch#show aaa authenticated-user
---------- authenticated users ----------
UserName Retry RadID Port EapID ChapID OnTime UserIP MAC

---------- total: 0 ----------

7.8.22 show aaa authenticating-user

Command: show aaa authenticating-user
Function: Display the authenticating users.
Command mode: Admin and Configuration Mode.
Usage Guide: Usually the administrator concerns only information about the authenticating user, the other information displays is used for troubleshooting by the technical support.
Example:
Switch#show aaa authenticating-user

---------- authenticating users ----------
User-name Retry-time Radius-ID Port Eap-ID Chap-ID Mem-Addr State
---

---------- total: 0 ----------

7.8.23 show aaa config

Command: show aaa config
Function: Displays the configured commands for the switch as a RADIUS client.
Command mode: Admin and Configuration Mode.

Usage Guide: Displays whether aaa authentication, accounting are enabled and information for key, authentication and accounting server specified.

Example:

Switch#show aaa config（For Boolean value, 1 stands for TRUE and 0 for FALSE）

---------- AAA config data ----------

Is Aaa Enabled = 1 :1 means AAA authentication is enabled, 0 means is not enabled

Is Account Enabled= 1 :1 means AAA account is enabled, 0 means is not enabled

MD5 Server Key = yangshifeng : Authentication key

authentication server sum = 2 :Configure the number of authentication server

authentication server[0].sock_addr = 2:100.100.100.60.1812 :The address protocol group, IP and interface number of the first authentication server

.Is Primary = 1 :Is the primary server

.Is Server Dead = 0 :The server whether dead

.Socket No = 0 :The local socket number lead to this server

authentication server[1].sock_addr = 10:2004:1:2::2.1812

.Is Primary = 0

.Is Server Dead = 0

.Socket No = 0

accounting server sum = 2 :Configure the number of the accounting server

accounting server[0].sock_addr = 2:100.100.100.65.1813 :The address protocol group, IP and interface number of the accounting server

.Is Primary = 1 :Is primary server

.Is Server Dead = 0 :This server whether dead

.Socket No = 0 :The local socket number lead to this server

accounting server[1].sock_addr = 10:2004::7.1813

.Is Primary = 1

.Is Server Dead = 0

.Socket No = 0

Time Out = 5s :After send the require packets, wait for response time out

Retransmit = 3 :The number of retransmit

Dead Time = 5min :The tautology interval of the dead server

Account Time Interval = 0min :The account time interval

7.8.24 show radius authenticated-user count

Command: show radius authenticated-user count

Function: Show the number of on-line users who have already passed the authentication.

Parameter: None.

Command mode: Admin and configuration mode

Default: None.
Usage guide: None.
Example:
Switch#show radius authenticated-user count
The authenticated online user num is: 105

7.8.25 show radius authenticating-user count

Command: show radius authenticating-user count
Function: Show the number of the authenticating-user.
Parameter: None.
Command mode: Admin and configuration mode.
Default: None.
Usage Guide: None.
Example:
Switch#show radius authenticating-user count
The authenticating user num is: 10

7.8.26 show radius count

Command: show radius {authenticated-user|authenticating-user} count
Function**:** Displays the statistics for users of RADIUS authentication.
Parameters: authenticated-user displays the authenticated users online; **authenticating-user** displays the authenticating users.
Command mode: Admin and Configuration Mode.
Usage Guide: The statistics for RADIUS authentication users can be displayed with the 'show **radius count'** command.
Example:
1. Display the statistics for RADIUS authenticated users.
Switch#show radius authenticated-user count
The authenticated online user num is: 0
2. Display the statistics for RADIUS authenticated users and others.
Switch#show radius authenticating-user count

7.8.27 Radius Escaping

7.8.27.1 radius-server escape { enable | disable}

Command: radius-server escape enable
radius-server escape disable
Function: Enable the AAA radius server escaping function.

Parameters: None.
Default: Disable.
Command Mode: Global Mode.
Usage Guide: After enabled the radius server escaping function, the flow of dot1x or portal authentication client can be allowed when the configured radius server on them is inaccessible. When the configured authentication server is accessible again, the flow allowing rule will be deleted.
Example: Enable the global authentication function.
Switch (Config)# radius-server escape enable

7.8.27.2 radius-server escape detection-interval

Command: radius-server escape detection-interval {default| < second >)}
Function: Configure the detection interval of radius server escaping.
Parameters: default: the default interval is 3 minutes.
second: the interval whose range is 1-1800 seconds.
Default: 180s.
Command Mode: Global Mode.
Usage Guide: The shorter the configured interval is, the radius server escaping function is more flexible. The configured interval should be longer than (Retransmit+1)* Time Out.
Example: Configure the detection interval of radius server escaping as 120s.
Switch(config)#radius-server escape detection-interval 120

7.9 SSL

7.9.1 ip http secure-server

Command: ip http secure-server
no ip http secure-server
Function: Enable/disable SSL function.
Parameter: None.
Command Mode: Global Mode.
Default: Disabled.
Usage Guide: This command is used for enable and disable SSL function. After enable SSL function, the users visit the switch through https client, switch and client use SSL connect, can form safety SSL connect channel. After that, all the data which transmit of the application layer will be encrypted, then ensure the privacy of the communication.
Example: Enable SSL function.
Switch(config)#ip http secure-server

7.9.2 ip http secure-port

Command: ip http secure-port *<port-number>*

no ip http secure-port

Function: Configure/delete port number by SSL used.

Parameter: ***<port-number>*** means configured port number, range between 1025 and 65535. 443 is for default.

Command Mode: Global Mode.

Default: Not configure.

Usage Guide: If this command is used to configure the port number, then the configured port number is used to monitor. If the port number for https is changed, when users try to use https to connect, must use the changed one. For example: https://device:port_number. SSL function must reboot after every change.

Example: Configure the port number is 1028.

Switch(config)#ip http secure-port 1028

7.9.3 ip http secure- ciphersuite

Command: ip http secure-ciphersuite {aes128-gcm-sha256|aes128-sha|aes128-sha256|aes256-sha|aes256-sha256|ecdhe-rsa-aes128-gcm-sha256|ecdhe-rsa-aes128-sha|ecdhe-rsa-aes256-sha}

no ip http secure-ciphersuite

Function: Configure/delete secure cipher suite by SSL used.

Parameter: aes128-gcm-sha256encrypted algorithm **aes128-gcm**，encrypted algorithm sha256。

aes128-shaencrypted algorithm **aes128**，encrypted algorithm sha。

aes128-sha256encrypted algorithm **aes128**，encrypted algorithm sha256。

aes256-shaencrypted algorithm **aes256**，encrypted algorithm sha。

aes256-sha256encrypted algorithm **aes256**，encrypted algorithm sha256。

ecdhe-rsa-aes128-gcm-sha256encrypted algorithm **ecdhe-rsa-aes128-gcm**，encrypted algorithm sha256。

ecdhe-rsa-aes128-shaencrypted algorithm **ecdhe-rsa-aes128**，encrypted algorithm sha。

ecdhe-rsa-aes256-shaencrypted algorithm **ecdhe-rsa-aes256**，encrypted algorithm sha。

Command Mode: Global Mode.

Default: Not configure.

Usage Guide: If this command is used to configure the secure cipher suite, specified encryption method will be used. The SSL should be restarted to take effect after changes on configuration. When des-cbc-sha is configured, IE 7.0 or above is required.

Example: Configure the secure cipher suite is rc4-128-sha.

Switch(config)# ip http secure- ciphersuite rc4-128-sha

7.9.4 show ip http secure-server status

Command: show ip http secure-server status

Function: Show the status for the configured SSL.

Parameter: None.
Command Mode: Admin and Configuration Mode.
Example:
Switch# show ip http secure-server status
HTTP secure server status: Enabled
HTTP secure server port: 1028
HTTP secure server ciphersuite: rc4-128-sha

7.9.5 debug ssl

Command: debug ssl
no debug ssl
Function: Show the configured SSL information, the no command closes the DEBUG.
Parameter: None.
Command Mode: Admin Mode.
Example:
Switch# debug ssl
%Jan 01 01:02:05 2006 ssl will to connect to web server 127.0.0.1:9998
%Jan 01 01:02:05 2006 connect to http security server success!

7.10 VLAN-ACL

7.10.1 clear vacl statistic vlan

Command: clear vacl [in | out] statistic vlan [<*1-4094*>]
Function: This command can clear the statistic information of VACL.
Parameter: in | out: Clear the traffic statistic of the ingress/egress.
vlan <*1-4094*>: The VLAN which needs to clear the VACL statistic information. If do not input VLAN ID, then clear all VLAN statistic information.
Command mode: Admin Mode.
Default: None.
Usage Guide: None.
Example:
Clear VACL statistic information of Vlan1.
Switch#clear vacl statistic vlan 1

7.10.2 show vacl vlan

Command: show vacl [in | out] vlan [*<1-4094>*] | [begin | include | exclude *<regular-expression>*]

Function: This command shows the configuration and the statistic information of VACL.

Parameter: in | out: Show ingress/egress configuration and statistic

vlan *<1-4094>*: The VLAN which needs to show the configuration and the statistic information of VACL. If do not input VLAN ID, then show VACL configuration and statistic information of all VLANs.

begin | include | exclude *<regular-expression>*: the regular expression

. match any characters except the line feed character

^ match the beginning of the row

$ match the end of the row

| match the character string at the left or right of upright line

[0-9] match the number 0 to the number 9

[a-z] match the lowercase a to z

[aeiou] match any letter in “aeiou”

\ Escape Character is used to match the intervocalic character, for example, \$ will match the $ character, but it is not match the end of the character string

\w match the letter, the number or the underline

\b match the beginning or the end of the words

\W match any characters which are not alphabet letter, number and underline

\B match the locations which are not the begin or end of the word

[^x] match any characters except x

[^aeiou] match any characters except including aeiou letters

* repeat zero time or many times

+ repeat one time or many times

(n) repeat n times

(n,) repeat n or more times

(n, m) repeat n to m times

At present, the regular expression used does not support the following syntaxes:

\s match the blank character

\d match the number

\S match any characters except blank character

\D match non-number character

? repeat zero time or one time

Command mode: Admin Mode.

Default: None.

Usage Guide: None..

Example:

Switch (config)#show vacl vlan 2

Vlan 2:

IP Ingress access-list used is 100, traffic-statistics Disable.

Switch (config)# show vacl vlan 3

Vlan 3:

IP Ingress access-list used is myacl, packet(s) number is 5.

Displayed Information	Explanation
Vlan 2	The name of VLAN
100, myacl	The name of VACL
traffic-statistics Disable	Disable VACL statistic function
packet(s) number is 5	The sum of out-profile data packets matching this VACL

7.10.3 vacl ip access-group

Command: vacl ip access-group {<1-299> | WORD} {in | out} [traffic-statistic] vlan WORD

no vacl ip access-group {<1-299> | WORD} {in | out} vlan WORD

Function: This command configure VACL of IP type on the specific VLAN.

Parameter: <1-299> | WORD: Configure the numeric IP ACL (include: standard ACL rule <1-99>, extended ACL rule <100-299>) or the named ACL.

in | out: Filter the ingress/egress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.

Default: None.

Usage **Guide:** Use ';' or '-' to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length can not exceed 80 characters. At present, IP ACL that match tcp/udp range can not be bound to VLAN Egress direction.

Example: Configure the numeric IP ACL and enable the statistic function for Vlan 1-5, 6, 7-9.

Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9

7.10.4 vacl ipv6 access-group

Command: vacl ipv6 access-group (<500-699> | WORD) {in | out} (traffic-statistic|) vlan WORD

no ipv6 access-group {<500-699> | WORD} {in | out} vlan WORD

Function: This command configure VACL of IPv6 on the specific VLAN.

Parameter: <500-699> | WORD: Configure the numeric IP ACL (include: IPv6 standard ACL rule <500-599>, IPv6 extended ACL rule <600-699>) or the named ACL.

in | out: Filter the ingress/egress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.

Default: None.

Usage Guide: Use ';' or '-' to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length can not exceed 80 characters. At present, IPv6 ACL that match flowlabel can not be bound to VLAN Egress direction.

Example: Configure the numeric IPv6 ACL for Vlan 5.

Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5

7.10.5 vacl mac access-group

Command: vacl mac access-group {<700-1199> | WORD} {in | out} [traffic-statistic] vlan WORD

no vacl mac access-group {<700-1199> | WORD} {in | out} vlan WORD

Function: This command configure VACL of MAC type on the specific VLAN.

Parameter: <700-1199> | WORD: Configure the numeric IP ACL (include: <700-799> MAC standard access list, <1100-1199> MAC extended access list) or the named ACL.

in | out: Filter the ingress/egress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.

Default: None.

Usage Guide: Use ';' or '-' to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length can not exceed 80 characters. None.

Example: Configure the numeric MAC ACL for Vlan 1-5.

Switch(config)#vacl mac access-group 700 in traffic-statistic vlan 1-5

7.10.6 vacl mac-ip access-group

Command: vacl mac-ip access-group {<3100-3299> | WORD} {in | out} [traffic-statistic] vlan WORD

no vacl mac-ip access-group {<3100-3299> | WORD} {in | out} vlan WORD

Function: This command configure VACL of MAC-IP type on the specific VLAN.

Parameter: <3100-3299> | WORD: Configure the numeric IP ACL or the named ACL.

in | out: Filter the ingress/egress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.

Default: None.

Usage Guide: Use ';' or '-' to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length can not exceed 80 characters. At present, MAC-IP ACL that match tcp/udp range can not be bound to VLAN Egress direction.

Example: Configure the numeric MAC-IP ACL for Vlan 1, 2, 5.

Switch(config)#vacl mac-ip access-group 3100 in traffic-statistic vlan 1;2;5

7.11 Captive Portal Authentication

7.11.1 Authentication

7.11.1.1 ac-name

Command: ac-name <word>

no ac-name

Function: Configure the parameter of acname in the redirect url. The no command deletes it.

Parameters: <word>, it is the value of acname including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guide: This command is used to configure the parameter of acname in the redirect url. Some portal servers can pass the authentication only with the specific ac-name. So this command should be configured according to the requirement of the portal server.

Example: Configure the ac-name in the redirect url as 0100.0010.010.00 according to the standard of the mobile portal server, and the format is ACN.CTY.PRO.OPE.

Switch(config-cp-instance)#ac-name 0100.0010.010.00

7.11.1.2 captive-portal

Command: captive-portal

Function: Use this command to enter Captive Portal configuration mode.

Parameter: None.

Default: None.

Command Mode: Global configuration mode.

Usage Guide: Use this command to enter Captive Portal configuration mode.

Example: Enter into the global configuration mode for configuring.

Switch(config)#captive-portal

7.11.1.3 captive-portal binding arp

This command is not supported by the switch.

7.11.1.4 captive-portal client deauthenticate

Command: captive-portal client deauthenticate {<*1-10*> / <*FF-FF-FF-FF-FF-FF*> { ipv4 | ipv6} <*ip-addr*>}

Function: Deauthenticate the specific Captive Portal client.

Parameters: <*1-10*> is the ID of Captive Portal;

<*FF-FF-FF-FF-FF-FF*> is the MAC address of client;

ipv4 is the ipv4 address of user;

ipv6 is the ipv6 address of user;

<ip-addr> is the user address, ipv4 address is dotted decimal format, ipv6 address is the format of X:X::X:X.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Deauthenticate the specific Captive Portal client with the specific MAC address, it can also deauthenticate all the users or a single user under the specific captive portal configuration. When there is no parameters, deauthenticate all users.
Example: Deauthenticate the specific Captive Portal client
Switch #captive-portal client deauthenticate (force all the portal users on this controller get down the line)
The specified clients will be deauthenticated. Are you sure you want to deauthenticated clients? [Y/N]
Switch #captive-portal client deauthenticate 1 (force all the users of instance 1 get down the line)
Switch #captive-portal client deauthenticate 34-08-04-30-07-ca ipv4 100.1.1.1 (force one user get down the line)

7.11.1.5 captive-portal client keep-alive flow-detection enable

Command: captive-portal client keep-alive flow-detection enable
no captive-portal client keep-alive flow-detection enable
Function: Enable the keep-alive function of user. The no command disables this function.
Parameters: None.
Default: Disable.
Command Mode: captive portal mode.
Usage Guide: After enabled this function, it can keep alive for the user when the user is on line.
Example: Enter into the captive portal mode and configure it.
Switch (config-cp)#captive-portal client keep-alive flow-detection enable

7.11.1.6 captive-portal client keep-alive flow-detection interval

Command: captive-portal client keep-alive flow-detection interval <3-120>
no captive-portal client keep-alive flow-detection interval
Function: Configure the inquiring interval of user keep-alive. The no command configures the interval to be the default value.
Parameters: <3-120>: the range is 3-120 minutes.
Default: 5 minutes.
Command Mode: captive portal mode.
Usage Guide: After configured this command, the keep-alive timer inquires the user online status every once in a interval.
Example: Enter into the captive portal mode and configure it.
Switch (config-cp)# captive-portal client keep-alive flow-detection interval 3

7.11.1.7 captive-portal client keep-alive flow-detection number

Command: captive-portal client keep-alive flow-detection number <1-10>
no captive-portal client keep-alive flow-detection number
Function: Configure the times of continuous failed query that the keep-alive timer is allowed. The

no command configures it to be the default value.

Parameters: <1-10>: the range is from 1 to 10.

Default: 3 times.

Command Mode: captive portal mode.

Usage Guide: After configured this command, the keep-alive timer can inquire the user online status for configured times, if the user is no online always, it judges the user is down the line. Otherwise, the user is online once in the times of query, it judges the user is online. The times will be configured again.

Example: Enter into the captive portal mode and configure it.

Switch (config-cp)# captive-portal client keep-alive flow-detection interval 3

7.11.1.8 clear

This command is not supported by switch.

7.11.1.9 configuration

Command: configuration *<cp-id>*

no configuration *<cp-id>*

Function: Use this command to enter Captive Portal instances Mode. The no command will delete the Portal Captive instance configuration..

Parameter: *<cp-id>* is the number of Captive Portal instances, range is 1 to 10.

Default: None.

Command Mode: Captive Portal global configuration mode.

Usage Guide: This configuration is used to configure Captive Portal instances. Each instance represents a class of users, users under the same instance have the same flow and rate configuration, etc., and vice versa. No command will delete a captive portal configuration. If there is an interface associated with a instance, then the no command will be invalid.

Example: Set the ID parameter as 4.

Switch(config-cp)#configuration 4

7.11.1.10 debug captive-portal packet

Command: debug captive-portal packet {send|receive|dump|all}

no debug captive-portal packet {send|receive|dump|all}

Function: Enable the packet debugging on-off of the captive portal authentication. The no command disables it.

Parameters: send: enables the debugging information of sending packet of captive portal;

receive: enables the debugging information of receiving packet of captive portal;

Dump: enables the packet parsing and debugging information of the captive portal

all: enables the debugging information of sending, receiving and dumping packet of captive portal.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the packet debugging on-off of the captive portal authentication.

Example: Enable all the packets debugging information of the captive portal authentication.

Switch#debug captive-portal packet all

7.11.1.11 debug captive-portal trace

Command: debug captive-portal trace

no debug captive-portal trace

Function: Enable the tracing debugging of the captive portal authentication. The no command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the tracing debugging of the captive portal authentication.

Example: Enable the tracing debugging of the captive portal authentication.

Switch#debug captive-portal trace

7.11.1.12 debug captive-portal error

Command: debug captive-portal error

no debug captive-portal error

Function: Enable the error debugging of the captive portal authentication. The no command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the error debugging of the captive portal authentication.

Example: Enable the error debugging of the captive portal authentication.

Switch#debug captive-portal error

7.11.1.13 enable (global)

Command: enable

disable

Function: Use this command to enable the Captive Portal function of the controller globally, use disable function to disable the Captive Portal function of the controller globally.

Parameter: None.

Default: Disable.

Command Mode: Captive Portal global configuration mode.

Usage Guide: Use this command to enable global Captive Portal characteristics on the controller.
Example: Enable the global Captive Portal function on the controller.
Switch(config-cp)#enable

7.11.1.14 enable (instance)

Command: enable
disable
Function: Enable Captive Portal configuration.
Parameter: None.
Default: Enable Captive Portal configuration.
Command Mode: Captive Portal Instance configuration mode.
Usage Guide: disable command will disable the captive-portal function, after disabling this command, the portal users will be forced offline.
Example: Enable captive-portal function.
Switch(config-cp-instance)#enable

7.11.1.15 external portal-server server-name

Command: external portal-server server-name <*name*> {ipv4 | ipv6} <*ipaddr*> [port <*1-65535*>]
no external portal-server {ipv4 | ipv6}server-name <*name*>
Function: Configure the external portal server. Launch the redirect page through this server, after inputting the correct user name and password, the authentication is successful and the client can access the outside network.
Parameter: <*name*> is name of external portal server.
<*ipaddr*> is ip address of external portal server.
ipv4 the configured portal server address is ipv4 address.
ipv6 the configured portal server address is ipv6 address.
<*1-65535*> is number of portal server.
Default: None.
Command Mode: Captive Portal global configuration mode.
Usage Guide: Configure external portal servers, 10 can be configured at most. Each cp configuration can be bound to one portal server.
Example: Configure a external portal server.
Switch(config-cp)# external portal-server server-name x1 ipv4 1.0.0.1 port 11111

7.11.1.16 http-redirect-filter <1-32>

Command: http-redirect-filter <1-32>
no http-redirect-filter <1-32>
Function: Bind a rule to a instance of the captive portal. The no command deletes the redirect binding.
Parameters: <1-32>: the ID number of the rule (index).

Default: This command is not configured as default.
Command Mode: Captive Portal instance mode.
Usage Guide: Bind a rule to a instance of the captive portal.
Example: Bind the rule to the instance.
Switch (config-cp-instance)# http-redirect-filter 1

7.11.1.17 name

Command: name *<cp-name>*
no name
Function: Define the name of Captive Portal configuration.
Parameter: *<cp-name>*, the name of Captive Portal configuration, 32 characters can be included at most and they can be numbers and letters.
Default: None.
Command Mode: Captive Portal Instance configuration mode.
Usage Guide: Define the name of Captive Portal configuration.
Example: Define the name of Captive Portal configuration as abc123.
Switch(config-cp-instance)#name abc123

7.11.1.18 nas-ipv4

Command: nas-ipv4 *< A.B.C.D>*
no nas-ipv4 *< A.B.C.D>*
Function: Define the Captive Portal nas-ip address.
Parameters: *< A.B.C.D >*: IPv4 address of NAS.
Default: None.
Command Mode: Captive Portal mode.
Usage Guide: Define the Captive Portal nas-ip address.
Example: Configure the Captive Portal nas-ip address as 10.1.1.1.
Switch (config-cp)#nas-ip 10.1.1.1

7.11.1.19 nas-ipv6

Command：nas-ipv6 *<ipv6-address>*
no nas-ipv6
Function: Define the Captive Portal nas-ipv6 address.
Parameters: *<ipv6-address>*: IPv6 address of NAS.
Default: None.
Command Mode: Captive Portal mode.
Usage Guide: Define the Captive Portal nas-ip address.
Example: Configure the Captive Portal nas-ipv6 address as 2000::1.
Switch (config-cp)#nas-ipv6 2000::1

7.11.1.20 portal-server

Command: portal-server {ipv4 | ipv6} <*name*>

no portal-server {ipv4 | ipv6}

Function: This command can bind specific external portal server for the CP configuration. Networks under this CP configuration all redirect authentication through this portal server.

Parameter: <name> binding Portal server name.

ipv4 the bond portal server address is ipv4 address.

ipv6 the bond portal server address is ipv6 address.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Use this command to bind specific external portal server for the CP configuration; it can also unbind the specific external portal server.

Example: Bind specific external portal server for the CP configuration.

Switch(config-cp -instance)#portal-server ipv4 x1

7.11.1.21 radius accounting

Command: radius accounting

no radius accounting

Function: Enable the accounting function of Captive Portal instance. The no command disables it.

Parameters: None.

Default: Disable.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Enable the accounting function of Captive Portal instance.

Example: Enable the accounting function of Captive Portal instance.

Switch (config-cp-instance)#radius accounting

7.11.1.22 radius-accounting update interval

Command: radius-accounting update interval <*60-3600*>

no radius-accounting update interval

Function: Configure the accounting updating interval of the portal user that the switch sends to radius. The no command recovers it to be the default value.

Parameters: <*60-3600*> is the interval, the unit is second.

Default: 300 seconds.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Configure the accounting updating interval of the portal user

Example: Configure the accounting updating interval of the portal user that the switch sends to radius as 60s.

Switch (config-cp-instance)# radius-accounting update interval 60

7.11.1.23 radius-acct-server

Command: radius-acct-server *<server-name>*

no radius-acct-server

Function: Define the radius accounting server name of the captive portal. The no command deletes it.

Parameters: <*server-name*>: name of radius accounting server.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Define the radius accounting server name of the captive portal.

Example: Define the radius accounting server name of the captive portal as radius_aaa_1.

Switch (config-cp-instance)#radius-acct-server radius_aaa_1

7.11.1.24 radius-auth-server

Command: radius-auth-server *<server-name>*

no radius-auth-server

Function: Use this command to define the RADIUS authentication server of the Captive Portal configuration. The no command deletes the configuration.

Parameter: *<server-name>*, RADIUS authentication server name of Captive Portal configured.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Define the RADIUS authentication server of the Captive Portal configuration.

Example: Define the RADIUS authentication server of the Captive Portal configuration as radius_aaa_1.

Switch(config-cp-instance)#radius-auth-server radius_aaa_1

7.11.1.25 redirect url-head <word>

Command: redirect url-head <word>

no redirect url-head

Function: Configure the redirect url-head including transmission protocol, host name, port and path. The no command deletes it.

Parameters: <word>, It is the redirect url-head such as https://200.101.13.4:8080/index.jsp or http:// www.portal.com/index.jsp. 128 characters can be input at most.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guide: This command is used to configure the redirect url-head including transmission protocol, host name, port and path. Configures according to the redirect url of the portal server. The transmission protocol, host name, port and path should be same for redirecting.

Example: Configure the redirect url-head as http://17.16.1.26/control.

Switch(config-cp-instance)#redirect url-head http://17.16.1.26/control

7.11.1.26 redirect attribute ssid enable

Command: redirect attribute ssid enable

no redirect attribute ssid enable

Function: Configure the redirect url to carry the parameter of ssid. The no command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disable.

Usage Guide: This command is used to configure the redirect url to carry the parameter of ssid. After enabled this command, the redirect url will carry the ssid associated with client when the client conducts the redirection.

Example: Configure the redirect url to carry the parameter of ssid.

Switch(config-cp-instance)#redirect attribute ssid enable

7.11.1.27 redirect attribute ssid name

Command: redirect attribute ssid name <word>

no redirect attribute ssid name

Function: Configure the name of the parameter of ssid carried in the redirect url. The no command recovers it to be the default value.

Parameters: <word>, it is the ssid name including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: ssid.

Usage Guide: This command is used to configure the name of the parameter of ssid carried in the redirect url.

Example: Configure the name of the parameter of ssid carried in the redirect url as ssid.

Switch(config-cp-instance)#redirect attribute ssid name ssid

7.11.1.28 redirect attribute nas-ip enable

Command: redirect attribute nas-ip enable

no redirect attribute nas-ip enable

Function: Configure the redirect url to carry the parameter of nas-ip. The no command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disable.

Usage Guide: This command is used to configure the redirect url to carry the parameter of nas-ip. After enabled this command, the redirect url will carry the IP address of switch associated with client when the client conducts the redirection.

Example: Configure the redirect url to carry the parameter of nas-ip.

Switch(config-cp-instance)#redirect attribute nas-ip enable

7.11.1.29 redirect attribute nas-ip name

Command: redirect attribute nas-ip name <word>

no redirect attribute nas-ip name

Function: Configure the name of the parameter of nas-ip carried in the redirect url. The no command recovers it to be the default value.

Parameters: <word>, it is the nas-ip name including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: acname.

Usage Guide: This command is used to configure the name of the parameter of nas-ip carried in the redirect url.

Example: Configure the name of the parameter of nas-ip carried in the redirect url as nasip.

Switch(config-cp-instance)#redirect attribute nas-ip name nasip

7.11.1.30 session-timeout

Command: session-timeout *<0-86400>*

no session-timeout

Function: Define the session timeout of the Captive Portal. The no command disables this function.

Parameters: <*0-86400*>: the session timeout, unit is second. 0 means the timeout function is not effective.

Default: 86400.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Define the session timeout of the Captive Portal.

Example: Define the session timeout of the Captive Portal as 100s.

Switch (config-cp-instance)# session-timeout 100

7.11.1.31 show captive-portal

Command: show captive-portal

Function: Shows the characteristics status of the Captive Portal.

Parameter: None.

Default: None.

Command Mode: Admin mode

Usage Guide: Show the relevant state parameters of the captive portal function on this switch.

Example: Show Captive Portal status of enable and disable.

captive portal enable:

Switch#show captive-portal

Administrative Mode..... Enable

Operational Status..... Enabled

CP IP Address..... 101.1.1.3

captive portal disable:

Switch#show captive-portal
Administrative Mode..... Disable
Operational Status..... Disabled
Disable Reason..... Administrator Disabled
CP IP Address..... 0.0.0.0

7.11.1.32 show captive-portal status

Command: show captive-portal status
Function: Shows the status of all the Captive Portal instance in the system.
Parameter: None.
Default: None.
Command Mode: Admin mode
Usage Guide: This command shows the captive portal configuration and the supported property parameters on this switch.
Example: Show the Captive Portal status of the controller.
Switch#show captive-portal status
Peer Switch Statistics Reporting Interval..... 120
Authentication Timeout..... 300
Authentication Type..... External
Supported Captive Portals..... 10
Configured Captive Portals..... 9
Active Captive Portals..... 0
Local Supported Users..... 128
Configured Local Users..... 0
System Supported Users..... 1024
Authenticated Users..... 0

7.11.1.33 show captive-portal configuration

Command: show captive-portal configuration *<cp-id>*
Function: Show the status of Captive Portal configuration.
Parameter: ***<cp-id>*** is the ID number of captive portal, range is 1 to 10.
Default: None.
Command Mode: Admin mode
Usage Guide: Show the configured parameters of portal instance.
Example: Show the configured situation of captive portal1.
Switch#show captive-portal configuration 1
CP ID..... 1
CP Name..... default
Operational Status..... Enabled
Block Status..... Not Blocked
Configured Locales..... 1

Authenticated Users..... 0
Permit-all Status..... Disabled

7.11.1.34 show captive-portal configuration interface

Command: show captive-portal configuration *<cp-id>* interface <IFNAME or ethernet>
Function: Shows all the interface information assigned to the captive portal configuration.
Parameter: *<cp-id>,* ID number of cp;
IFNAME ,Interface Name or number
Ethernet, Ethernet port
Default: None.
Command Mode: Admin mode
Usage Guide: Shows the interface state of the a portal instance.
Example: Shows all the interface information of Captive Portal configuration.
Switch # show captive-portal configuration 1 interface e1/0/1
CP ID..... 1
CP Name..... Default
Interface..... 1
Interface Description..... Ethernet1/0/1
Operational Status..... Enabled
Block Status..... Not Blocked
Authenticated Users..... 0

7.11.1.35 show captive-portal configuration status

Command: show captive-portal configuration [*<cp-id>*] status
Function: Shows the configuration information of all or specific Captive Portal.
Parameter: *<cp-id>*, ID number of cp, the parameter **<cp-id>** means the content of a instance, without the parameter to show all the current configured instance parameters.
Default: None.
Command Mode: Admin mode
Usage Guide: Show detailed configuration parameters of portal instance.
Example: Show all Captive Portal configuration information.
Show the status of all the instances:
Switch # show captive-portal configuration status

CP ID	CP Name	Mode	Protocol	Verification
1	Default	Enable	HTTP	RADIUS
2	Default	Enable	HTTP	RADIUS

7.11.1.36 show captive-portal client status

Command: show captive-portal client [<*FF-FF-FF-FF-FF-FF*> { ipv4 | ipv6} <*ip-addr*>] status

Function: This command shows detailed connection information or an overview of users connected to the captive portal.

Parameter: <*FF-FF-FF-FF-FF-FF*> is the MAC address of the user.

ipv4: user address is ipv4 address.

ipv6: user address is ipv6 address.

<*ip-addr*> is user address. Ipv4 address is decimal format with point and ipv6 address is the format of X:X::X:X.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the status of all or a portal user.

Example: Show detailed information of user1 connected to the captive portal.

Switch # show captive-portal client status

MAC Address	IP Address	User Name	Protocol	Mode	Session Time
20-6a-8a-65-0d-17	66.1.1.2	user1	HTTP	RADIUS	0d:00:00:47

7.11.1.37 show captive-portal configuration client

Command: show captive-portal configuration [<*cp-id*>] client status

Function: This command shows the client information through the portal authentication in an interface.

Parameter: <*cp-id*>, ID number of Captive Portal.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the user parameters of a portal instance.

Example: Show all the portal configuration information of the client passed authentication.

Switch #show captive-portal configuration 1 client status

CP ID..... 1

CP Name..... Default

Client MAC Address	Client IP Address	Interface	Interface Description
00-24-8c-00-99-27	10.1.1.51	1922	Port-Channel2

7.11.1.38 show captive-portal ext-portal-server status

Command: show captive-portal ext-portal-server status

Function: Use this command to check the status of the external portal server.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Check the status of the external portal server.

Example: Check the status of the external portal server.

Switch #show captive-portal ext-portal-server status

Server Name	Server IP Address	port	SocketNo
x1	100.1.1.2	7749	0
x2	100.1.1.1	7749	0

7.11.1.39 show captive-portal interface configuration status

Command: show captive-portal interface configuration [<*cp-id*>] status

Function: This command shows the interface information of all captive portal configuration or a specific configuration.

Parameter: <*cp-id*>, captive portal ID.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the binding relationship of all or a portal instances with interface.

Example: Show the interface information of all captive portal configuration.

Switch #show captive-portal interface configuration status

CP ID	CP Name	Interface	Interface Description	Type
1	Default	1	Ethernet1/0/1	Physical

7.11.2 Free-resource

7.11.2.1 free-resource

Command: free-resource destination { ipv4 | ipv6} <*ip-addr*><*netmask*> }

no free-resource destination { ipv4 | ipv6} <*ip-addr*><*netmask*> }

Function: Configure the free-resource rules, the client who conforms the source IP address in rules can access the resources of the destination IP address in rules, the switch does not redirect, the client can access directly without Portal authentication.

Parameter: ipv4 the configured free resource address is ipv4 address

ipv6 the configured free resource address is ipv6 address

<*ip-addr*> free-resource rules interviewees'/visitors' IP addresses.

<*netmask*> free-resource rules interviewees'/visitors' IP addresses.

Default: None.

Command Mode: cp configuration mode.

Usage Guide: Configure the client address segment (visitor) which can be free to access the resources and the address segment which is free to provide the resource (interviewee).

Example: Set free-resource rules.

Switch (config-cp)# free-resource 1 source any

7.11.3 Automatic Page Pushing after Successful Authentication

7.11.3.1 redirect attribute url-after-login enable

Command: redirect attribute url-after-login enable

no redirect attribute url-after-login enable

Function: Enable the function that the redirect url carrys the pushed url after the successful authentication. The no command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disable.

Usage Guide: This command is used to enable the function that the redirect url carrys the pushed url after the successful authentication. After enabled this command, the redirect url pushed by switch will carry the url which needs to be pushed after the successful authentication. At the same time, when the <url-value> of redirect attribute url-after-login value is configured as empty, the carried url is the page url that the user access before the authentication. If it is not empty, the carried url is the page url configured by <url-value>.

Example: Enable the function that the redirect url carrys the pushed url after the successful authentication.

Switch(config-cp-instance)#redirect attribute url-after-login enable

7.11.3.2 redirect attribute url-after-login name

Command: redirect attribute url-after-login name <name>

no redirect attribute url-after-login name

Function: Configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url. The no command recovers it to be the default value.

Parameters: <name>, it is the attribute name including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: The default name is srcurl.

Usage Guide: This command is used to configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url.

Example: Configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url as redirect.

Switch(config-cp-instance)#redirect attribute url-after-login name redirect

7.11.3.3 redirect attribute url-after-login encode

Command: redirect attribute url-after-login encode {plain-text|base64}

Function: Configure the encode of the pushed url after the successful authentication which is

carried in the redirect url.

Parameters: plain-text, it is the plain-text;

base64, It is the base64 encode.

Command Mode: Captive Portal Instance Mode.

Default: The default encode is plain-text.

Usage Guide: This command is used to configure the encode of the pushed url after the successful authentication which is carried in the redirect url. It can be configured according to the encode supported by the portal server.

Example: Configure the encode of the pushed url after the successful authentication which is carried in the redirect url as base64.

Switch(config-cp-instance)#redirect attribute url-after-login encode base64

7.11.3.4 redirect attribute url-after-login value

Command: redirect attribute url-after-login value <url-value>

no redirect attribute url-after-login value

Function: Configure the appointed url which is popped up after the success authentication. The no command deletes it.

Parameters: <url-value>, it is the configured appointed url including 512 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guide: This command is used to configure the appointed url which is popped up after the success authentication. If enable the function that the redirect url carries the pushed url after the successful authentication, the redirect url will carry the url with the <url-value>.

Example: Configure the appointed url which is popped up after the success authentication as http://www.test.com.

Switch(config-cp-instance)#redirect attribute url-after-login value http://www.test.com

7.11.4 Portal Escaping

7.11.4.1 show captive-portal ext-portal-server server-name <name> status

Command: show captive-portal ext-portal-server server-name <name> status

Function: Show the portal server status including the server address and if the portal escaping function is enabled.

Parameters: <name> is the Portal server name, it is the string including 1 to 32 characters and the upper and lower case letters should be distinguished.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Checking the server status is the important method to check the fault. When the portal escaping function is not effective, the configuration may be wrong; the command can be modified to help the administrator to remove the fault. If there is not the parameter of <name>, the status of all the servers will be shown. If there is the parameter of <name>, the detailed status information of the server will be shown.

Example: Show the status of all the ext-portal-server.

Show the detailed status of the server named as Portaltest.

Switch (config-cp)#show captive-portal ext-portal-server server-name Portaltest status

Server Name..... portaltest

Server IP..... 101.1.1.6

Server Port..... 7749

Server Key.....

Detect Mode..... Enable

Detect Interval..... 20

Detect Retries..... 3

Detect Trap Mode..... Disable

Detect Log Mode..... Disable

Detect Permit-all Mode..... Enable

Detect Operational Mode..... Enable

Detect Operational Status..... Down

Detect Operational Fails..... 1

Detect Operational Time..... 0d:00:00:11

7.12 MAB

7.12.1 authentication mab

Command: authentication mab {radius|local} (none|)

no authentication mab

Function: Configure the authentication mode and priority of MAC address authentication, the no command restores the default authentication mode.

Parameters: radius means RADIUS authentication mode; local means the local authentication; none means the authentication is needless.

Default: Using RADIUS authentication mode.

Command Mode: Global mode

Usage Guide: none option is used to the fleeing function of MAC address authentication. If all configured RADIUS servers don't respond, switch will adopt none authentication mode to allow that MAC address authentication users access the network directly. The option of local is used for the local authentication of MAC address, it authenticates through the local user name and password. If configured as the method of **authentication mab radius local none**, judge if configured the user name and password used in mab authentication in local when the radius

server has no response. If it has been configured, use the local authentication, if not, use the backup none authentication.

Example: Configure the local authentication and the fleeing function of MAC address authentication.

Switch(config)#authentication mab radius local none

7.12.2 clear mac-authentication-bypass binding

Command: clear mac-authentication-bypass binding {mac WORD | interface (ethernet IFNAME | IFNAME) | all}

Function: Clear MAB binding information.

Parameters: MAC: Delete MAB binding of the specified MAC address

IFNAME: Delete MAB binding of the specified port

all: Delete all MAB binding

Command Mode: Admin Mode

Default: None.

Usage Guide: None.

Example: Delete all MAB binding.

Switch#clear mac-authentication-bypass binding all

7.12.3 debug mac-authentication-bypass

Command: debug mac-authentication-bypass {packet | event | binding}

Function: Enable the debugging of the packet information, event information or binding information for MAB authentication.

Parameters: packet: Enable the debugging of the packet information for MAB authentication.

event: Enable the debugging of the event information for MAB authentication.

binding: Enable the debugging of the binding information for MAB authentication.

Command Mode: Admin Mode

Default: None.

Usage Guide: None.

Example: Enable the debugging of the packet information for MAB authentication.

Switch#debug mac-authentication-bypass packet

7.12.4 mac-authentication-bypass binding-limit

Command: mac-authentication-bypass binding-limit <*1-100*>

no mac-authentication-bypass binding-limit

Function: Set the max binding number of MAB. The no command will restore the default binding number as 3.

Parameters: <*1-100*> the max binding number of MAB, ranging from 1 to 100.

Command Mode: Port Mode

Default: The max binding number of MAB is 3.

Usage Guide: Set the max binding number of MAB. When the binding number reaches to the max value, the port will stop binding, if the max binding number is less than the current binding number of the port, the setting will be unsuccessful.

Example: Configure the max binding number as 10.

Switch(Config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#mac-authentication-bypass binding-limit 10

7.12.5 mac-authentication-bypass enable

Command: mac-authentication-bypass enable

no mac-authentication-bypass enable

Function: Enable the global and port MAB function. The no command disables MAB function.

Parameters: None.

Command Mode: Global Mode and Port Mode

Default: Disable the global and port MAB function.

Usage Guide: To process MAB authentication of a port, enable the global MAB function first, and then, enable the MAB function of the corresponding port.

Example: Enable the global and port Eth1/0/1 MAB function.

Switch(Config)#mac-authentication-bypass enable

Switch(Config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#mac-authentication-bypass enable

7.12.6 mac-authentication-bypass guest-vlan

Command: mac-authentication-bypass guest-vlan <1-4094>

no mac-authentication-bypass guest-vlan

Function: Set guest vlan of MAB authentication. The no command deletes guest vlan.

Parameters: <*1-4094*>: guest vlan ID, ranging from 1 to 4094.

Command Mode: Port Mode

Default: None.

Usage Guide: Set guest vlan of MAB authentication, only Hybrid port use this command, it is not take effect on access port. After MAB authentication is failing, if the existent guest vlan is configured by the port connecting to the MAB user, the MAB user can join and access guest vlan.

Example: Configure guest vlan of MAB authentication for port 1/0/1

Switch(Config)#interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)#mac-authentication-bypass guest-vlan 10

7.12.7 mac-authentication-bypass spoofing-garp-check

7.12.8 mac-authentication-bypass timeout linkup-period

Command: mac-authentication-bypass timeout linkup-period <0-30>

no mac-authentication-bypass timeout linkup-period

Function: Set the interval between down and up when VLAN binding in a port is changing to assure the user can obtain IP again.

Parameters: <*0-30*>: After the port is shutdown automatically, the interval before it up again, the unit is second, 0 means there is no down/up operation.

Command Mode: Global Mode

Default: The interval is 0.

Usage Guide: When MAB authentication is successful, belong to vlan according to auto-vlan setting, when MAB authentication is failing, belong to vlan according to guest-vlan setting. After linkup-period is set, when VLAN binding of a port is changing, the port will be shutdown automatically, and will be up again after linkup-period to assure the client obtain IP.

Example: Configure down/up time as 12s.

Switch(Config)#mac-authentication-bypass timeout linkup-period 12

7.12.9 mac-authentication-bypass timeout offline-detect

Command: mac-authentication-bypass timeout offline-detect (0 | <60-7200>)

no mac-authentication-bypass timeout offline-detect

Function: Configure offline-detect time. The no command restores the default value.

Parameters: (0 | <60-43200>): offline-detect time, the range is 0 or 60 to 43200s.

Command Mode: Global Mode

Default: offline-detect time is 180s.

Usage Guide: When offline-detect time is 0, the switch does not detect MAB binding, when offline-detect time is 60s to 7200s, the switch timely detects the flow corresponding to the MAB binding. If there is no flow in the period of offline-detect time, it will delete this binding and forbid the flow to pass.

Example: Configure offline-detect time as 200s.

Switch(Config)#mac-authentication-bypass timeout offline-detect 200

7.12.10 mac-authentication-bypass timeout quiet-period

Command: mac-authentication-bypass timeout quiet-period <1-60>

no mac-authentication-bypass timeout quiet-period

Function: Set quiet-period of MAB authentication. The no command restores quiet-period as the

default value.

Parameters: <*1-60*>: quiet-period, ranging from 1 to 60s.

Command Mode: Global Mode

Default: quiet-period is 30s.

Usage Guide: If MAB authentication is failing, within the quiet-period the switch will not respond the authentication request of this MAC, after quiet-period, it will respond the request again.

Example: Configure quiet-period of MAB authentication as 60s.

Switch(Config)#mac-authentication-bypass timeout quiet-period 60

7.12.11 mac-authentication-bypass timeout reauth-period

Command: mac-authentication-bypass timeout reauth-period <1-3600>

no mac-authentication-bypass timeout reauth-period

Function: Set the reauthentication interval at failing authentication state. The no command restores the default value.

Parameters: <*1-3600*>: reauthentication interval, ranging from 1 to 3600s.

Command Mode: Global Mode

Default: reauthentication interval is 30s.

Usage Guide: At failing authentication state, the user processes the reauthentication timely until the authentication is successful; at the successful state, the user can access the network resources.

Example: Configure reauthentication time as 20s.

Switch(Config)#mac-authentication-bypass timeout reauth-period 20

7.12.12 mac-authentication-bypass timeout stale-period

Command: mac-authentication-bypass timeout stale-period <0-60>

no mac-authentication-bypass timeout stale-period

Function: Set the time that delete the binding user after MAB port is down. The no command restores the default value.

Parameters: <*1-60*>: The time that delete the binding, ranging from 0 to 60s.

Command Mode: Global Mode

Default: 30s.

Usage Guide: If the time that delete the binding as 0, delete all user binding of this port as soon as the MAB port is down, if the time is bigger than 0, delete the user binding with a delay after the MAB port is down.

Example: Configure the deletion time as 40s.

Switch(Config)#mac-authentication-bypass timeout stale-period 40

7.12.13 mac-authentication-bypass username-format

Command: mac-authentication-bypass username-format {mac-address | {fixed username WORD password WORD}}

Function: Set the authenticate method of MAB authentication.

Parameters: mac-address: Use MAC address of MAB user as username and password to authenticate.

fixed username WORD password WORD: Use the specified username and password to authenticate, the length of username and password ranges between 1 and 32 characters.

Command Mode: Global Mode

Default: Use MAC address of MAB user as username and password to authenticate.

Usage Guide: There are two methods for MAB authentication: use MAC address of MAB user as username and password to authenticate or use the specified username and password to authenticate. If there is no specified username and password, the device uses the first method to authenticate by default.

Example: All MAB users use the same username and password to authenticate, the username is mab-user, the password is mab-pwd.

Switch(Config)#mac-authentication-bypass username-format fixed username mab-user password mab-pwd

7.12.14 show mac-authentication-bypass

Command: show mac-authentication-bypass {interface {ethernet IFNAME | IFNAME) |}

Function: Show the binding information of MAB authentication.

Parameters: interface {ethernet IFNAME|IFNAME}: The port name.

Command Mode: Admin Mode

Default: None.

Usage Guide: None.

Example: Show the binding information of all MAB users.

Switch#show mac-authentication-bypass

The Number of all binding is 5

MAC	Interface	Vlan ID	State
05-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET
04-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET
03-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET
02-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_AUTHENTICATED

00-0a-eb-6a-7f-8e Ethernet1/0/1 1 MAB_AUTHENTICATED

Displayed information	Explanation
The Number of all binding	The binding number of all MAB users, include the successful authentication user and the failing authentication user at quiet-period state
MAC	MAC address
Interface	The binding port
Vlan	The VLAN that MAB user belongs
State	Authentication state

Switch(config)#show mac-authentication-bypass int e1/0/1

Interface Ethernet1/0/1 user config:

MAB enable: Enable

Binding info: 1

MAB Binding built at SUN JAN 01 01:14:48 2006

VID 1, Port: Ethernet1/0/1

Client MAC: 00-0a-eb-6a-7f-8e

Binding State: MAB_AUTHENTICATED

Binding State Lease: 164 seconds left

Displayed information	Explanation
MAB enable	MAB function enabled or not
Binding info	The MAB binding number of the specified port
MAB Binding built at	The time when the user binding was created
VID	The VLAN that MAB user belongs
Port	The binding port
Client MAC	MAC address
Binding State	Authentication state
Binding State Lease	Remain time before the binding release

7.13 PPPoE Intermediate Agent

7.13.1 debug pppoe packet {receive | send} interface ethernet <interface-name>

Command: debug pppoe packet (receive | send|) interface ethernet <interface-name>

no debug pppoe packet (receive | send|) interface ethernet <interface-name>

Function: Enable PPPoE packet debug for the specified port, the no command disables it.

Parameter: receive: Enable the debug that receive PPPoE packet.

send: Enable the debug that send PPPoE packet.

ehernet: Physical port

interface-name: Port name

Command Mode: Admin mode

Default: Disable PPPoE packet debug for the specified port.

Usage Guide: Enable PPPoE packet debug for the specified port to show PPPoE packet received and sent by this port.

Example: Enable PPPoE intermediate debug for port ethernet1/0/2.

Switch#debug pppoe intermediate send interface ethernet 1/0/2

7.13.2 pppoe intermediate-agent

Command: pppoe intermediate-agent

no pppoe intermediate-agent

Function: Enable global PPPoE intermediate agent function. The no command disables global PPPoE intermediate agent function.

Parameter: None.

Command Mode: Global mode.

Default: Disable global PPPoE intermediate agent function.

Usage Guide: After enable global PPPoE IA function, process the packet of PPPoE discovery stage according to the related configuration.

Example: Enable global PPPoE intermediate agent function.

Switch(config)#pppoe intermediate agent

7.13.3 pppoe intermediate-agent (Port)

Command: pppoe intermediate-agent

no pppoe intermediate-agent

Function: Enable PPPoE intermediate agent function of the port. The no command disables PPPoE intermediate agent function of the port.

Parameter: None.

Command Mode: Port mode

Default: Disable PPPoE intermediate agent function of the port.

Usage Guide: After enable PPPoE IA function of the port, add vendor tag for PPPoE packet of the port.

Note: 1. It must enable global pppoe intermediate-agent function.

2. At least one port is connected to PPPoE server, and the port mode is trust.

Example: Enable PPPoE intermediate agent function of the port ethernet 1/0/2.

Switch(config-if-ethernet1/0/2)#pppoe intermediate agent

7.13.4 pppoe intermediate-agent circuit-id

Command: pppoe intermediate-agent circuit-id <string>

no pppoe intermediate-agent circuit-id <string>

Function: Configure circuit ID of the port, the no command cancels this configuration.

Parameter: <string>: circuit-id, the max character number is 63 bytes.

Command Mode: Port mode

Default: This configuration is null.

Usage Guide: This command configures circuit-id alone for each port, the priority is higher than pppoe intermediate-agent identifier-string command.

Example: Configure circuit-id as abcd/efgh on port ethernet1/0/3 of vlan3.

Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id abcd/efgh

After port ethernet1/0/3 of vlan3 receives PPPoE packet, circuit-id value of the added vendor tag as ”abcd/efgh”.

7.13.5 pppoe intermediate-agent delimiter

Command: pppoe intermediate-agent delimiter <WORD>

no pppoe intermediate-agent delimiter

Function: Configure the delimiter among the fields in circuit-id and remote-id, the no command cancels the configuration.

Parameter: <WORD>: the delimiter, its range is (#|.|,|;|:|/|space).

Command Mode: Global mode

Default: The fields is comparted with ’\0’.

Usage Guide: After configuring the delimiter, the added fields of circuit-id and remote-id use the configured delimiter to compart. Notice: The global **pppoe intermediate-agent** function must be enabled.

Example: Configure the delimiter.

Switch(config)#pppoe intermediate-agent delimiter space

7.13.6 pppoe intermediate-agent format

Command: pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii)
no pppoe intermediate-agent format (circuit-id | remote-id)

Function: Configure the format with hex or ASCII for circuit-id and remote-id, the no command cancels the configuration.

Parameter: hex: hexadecimal
ascii: ASCII code

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: Encapsulation circuit-id and remote-id with hex ASCII format to vendor tag. Notice: The global **pppoe intermediate-agent** function must be enabled.

Example: Configure the trust port 1/0/1 to enable vendor-tag strip function.

Switch(config)#pppoe intermediate-agent format remote-id ascii

7.13.7 pppoe intermediate-agent remote-id

Command: pppoe intermediate-agent remote-id <string>
no pppoe intermediate-agent remote-id <string>

Function: Configure remote-id of the port, the no command cancels this configuration.

Parameter: <string>: remote-id, the max character number is 63 bytes.

Command Mode: Port mode

Default: This configuration is null.

Usage Guide: Configure remote-id for each port, if there is no configuration, use switch's MAC as remote-id value.

Example: Configure remote-id as abcd on port ethernet1/0/2.

Switch(config-if-ethernet1/0/2)# pppoe intermediate-agent remote-id abcd

7.13.8 pppoe intermediate-agent trust

Command: pppoe intermediate-agent trust
no pppoe intermediate-agent trust

Function: Configure the port as trust port, the no command configures the port as untrust port.

Parameter: None.

Command Mode: Port mode

Default: Untrust port.

Usage Guide: The port which connect to server must be configured as trust port. Note: At least one trust port is connected to PPPoE server.

Example: Configure port ethernet1/0/1 as trust port.

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

7.13.9 pppoe intermediate-agent type self-defined circuit-id

Command: pppoe intermediate-agent type self-defined circuit-id {vlan | port | id (switch-id (mac | hostname) | remote-mac) | string WORD}

no pppoe intermediate-agent type self-defined circuit-id

Function: Configure the self-defined circuit-id, the no command cancels the configuration.

Parameter: vlan: VLAN ID

port: Port ID

id switch-id mac: the local MAC address

id switch-id hostname: the local host name

id remote-mac: the remote MAC address

string WORD: the specified keyword

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: This configuration and type tr-101 circuit-id are mutually exclusive, it will clear the corresponding configuration of type tr-101 circuit-id.

Example: Configure the self-defined circuit-id as vlan port id switch-id hostname.

Switch(config)#pppoe intermediate-agent type self-defined circuit-id vlan port id switch-id hostname

7.13.10 pppoe intermediate-agent type self-defined remoteid

Command: pppoe intermediate-agent type self-defined remoteid {mac | vlan-mac | hostname | string WORD}

no pppoe intermediate-agent type self-defined remote-id

Function: Configure the self-defined remote-id, the no command cancels the configuration.

Parameter: mac: Ethernet port MAC address

vlan-mac: IP interface MAC address

hostname: the local host name

string WORD: the specified keyword

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: Configuration order of this command according to the fields order in remote-id.

Example: Configure the self-defined remote-id as string abcd mac hostname.

Switch(config)#pppoe intermediate-agent type self-defined remoteid string abcd mac hostname

7.13.11 pppoe intermediate-agent type tr-101 circuit-id access-node-id

Command: pppoe intermediate-agent type tr-101 circuit-id access-node-id <string>

no pppoe intermediate-agent type tr-101 circuit-id access-node-id

Function: Configure access-node-id field value of circuit ID in the added vendor tag with tr-101 standard.

Parameter: <string>: access-node-id, the max character number is 47 bytes.

Command Mode: Global mode

Default: MAC address of the switch

Usage Guide: Use this configuration to create access-node-id of circuit ID in vendor tag. circuit-id value is access-node-id +" eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n<48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte. In default state, access-node-id value of circuit-id is switch's MAC, it occupies 6 bytes. For example: MAC address is "0a0b0c0d0e0f", Slot ID is 12, Port Index is 34, Vlan ID is 567, the default circuit-id value is "0a0b0c0d0e0f eth 12/034:0567".

Example: Configure access-node-id value of circuit ID as abcd in vendor tag.

Switch(config)#pppoe intermediate-agent access-node-id abcd

After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "abcd eth 01/003:0003".

7.13.12 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Command: pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp | sv | pv | spv} delimiter <WORD> [delimiter <WORD>]

no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Function: Configure circuit-id of the added vendor tag with tr-101 standard, the no command deletes this configuration.

Parameter: <string>: identifier-string, the max character number is 47 bytes.

{sp | sv | pv | spv}: This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan.

<WORD>: The delimiter between slot, port and vlan, the range is (# | . | , | ; | : | / | space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan.

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: This command is used to configure global circuit id, the priority is higher than

pppoe intermediate-agent access-node-id command. circuit-id value is access-node-id +" eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n<48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte.

Example: Configure access-node-id as xyz, use spv combination mode, delimiter with "#"between Slot ID and Port ID, delimiter with "/"between Port ID and Vlan ID.

Switch(config)#pppoe intermediate-agent identifier-string xyz option spv delimiter # delimiter /

Switch# show pppoe intermediate-agent identifier-string option delimiter

config identifier string is : xyz

config option is : slot , port and vlan

the first delimiter is : "# "

the second delimiter is : "/ "

After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "xyz eth 01#003/0003".

7.13.13 pppoe intermediate-agent vendor-tag strip

Command: pppoe intermediate-agent vendor-tag strip

no pppoe intermediate-agent vendor-tag strip

Function: Enable vendor-tag strip function of the port, the no command cancels this function.

Parameter: None.

Command Mode: Port mode

Default: Disable vendor-tag strip function of the port.

Usage Guide: If the received packet includes vendor tag from server to client, strip this vendor tag.

Note: 1. Must enable global pppoe intermediate-agent function.

2. It must be configured on trust port.

Example: Trust port ethernet1/0/1 enables vendor tag strip function.

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip

7.13.14 show pppoe intermediate-agent access-node-id

Command: show pppoe intermediate-agent access-node-id

Function: Show the configured access node ID.

Parameter: None.

Command Mode: Admin mode

Default: The configuration information is null.

Usage Guide: This command is used to show access-node-id configured by user.

Example: Show access-node-id configuration information.

Switch#pppoe intermediate-agent access-node-id abcd

Switch#show pppoe intermediate-agent access-node-id
pppoe intermediate-agent access-node-id is : abcd

7.13.15 show pppoe intermediate-agent identifier-string option delimiter

Command: show pppoe intermediate-agent identifier-string option delimiter
Function: Show the configured identifier-string, the combination format and delimiter of slot, port and vlan.
Parameter: None.
Command Mode: Admin mode
Default: The configuration information is null.
Usage Guide: Show the configured identifier-string, the combo format and delimiter of slot, port and vlan.
Example: Show the configuration information for pppoe intermediate-agent identifier-string.
Switch#pppoe intermediate-agent identifier-string abcd option spv delimiter # delimiter /
Switch# show pppoe intermediate-agent identifier-string option delimiter
config identifier string is : abcd
config option is : slot , port and vlan
the first delimiter is : "# "
the second delimiter is : "/ "

7.13.16 show pppoe intermediate-agent info

Command: show pppoe intermediate-agent info [interface ethernet <interface-name>]
Function: Show the related PPPoE IA configuration information of all ports or the specified port.
Parameter: ehernet: physical port
interface-name: port name
Command Mode: Admin mode
Default: The configuration information is null.
Usage Guide: Check the configuration information of the corresponding port, show whether the port is trust port, strip function is enabled, rate limit is enabled, show the configured circuit ID and remote ID.
Example: Show pppoe intermediate-agent configuration information of port ethernet1/0/2.
Switch# show pppoe intermediate-agent info interface ethernet 1/0/2

Interface	IA	Trusted	vendor Strip	Rate limit	circuit id	remote id
Ethernet1/0/2	yes	no	no	no	test1/port1	host1

7.14 QoS

7.14.1 accounting

Command: accounting

no accounting

Function: Set statistic function for the classified traffic.

Parameter: None.

Command mode: Policy map configuration mode

Default: Do not set statistic function.

Usage Guide: After enable this function, add statistic function to the traffic of the policy class map. In single bucket mode, the messages can only red or green when passing police. In the print information, in-profile means green and out-profile means red. In dual bucket mode, there are three colors of messages. In the print information, in-profile means green **and out-profile means** red and yellow.

Example: Count the packets which satisfy c1 rule.

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class **c1**

Switch(Config-PolicyMap-p1-Class-c1)#accounting

Switch(Config-PolicyMap-p1-Class-c1)#exit

Switch(Config-PolicyMap-p1)#exit

7.14.2 class

Command: class <*class-map-name*> [insert-before <*class-map-name*>]

no class <*class-map-name*>

Function: Associates a class to a policy map and enters the policy class map mode; the no command deletes the specified class.

Parameters: <*class-map-name*> is the class map name used by the class.

insert-before <*class-map-name*> insert a new configured class to the front of a existent class to improve the priority of the new class.

Default: No policy class is configured by default.

Command mode: Policy map configuration mode

Usage Guide: Before setting up a policy class, a policy map should be created and the policy map mode entered. In the policy map mode, classification and nexthop configuration can be performed on packet traffic classified by class map.

Example: After add a policy class map c1 to the policy map, add a policy class map c2 and insert it to the front of c1.

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#exit

Switch(Config-PolicyMap-p1)#class c2 insert-before c1
Switch(Config-PolicyMap-p1-Class-c2)#exit

7.14.3 class-map

Command: class-map <*class-map-name*>
no class-map <*class-map-name*>
Function: Creates a class map and enters class map mode; the no command deletes the specified class map.
Parameters: <*class-map-name*> is the class map name.
Default: No class map is configured by default.
Command mode: Global Mode
Usage Guide:
Example: Creating and then deleting a class map named "c1".
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#exit
Switch(config)#no class-map c1

7.14.4 clear mls qos statistics

Command: clear mls qos statistics [in / *out*] {interface *<interface-name>* | vlan <vlan-id>}
Function: Clear the in or out accounting data of the specified ports or VLAN Policy Map.
Parameters: [in | out]: the in or out direction of the port or vlan.
<vlan-id>: VLAN ID
<interface-name**>:** The interface name
Default: Do not set action.
Command mode: Admin Mode
Usage Guide**:** Clear the in or out accounting data of the specified ports or VLAN Policy Map.
Example: Clear the Policy Map statistic of VLAN 100.
Switch#Clear mls qos **statistics** vlan 100

7.14.5 drop

Command: drop
no drop
Function: Drop data package that match the class, the no command cancels the assigned action.
Parameters: None.
Default: Do not set the action.
Command mode: Policy class map configuration mode
Usage Guide: Drop the specified packet after configure this command.
Example: Drop the packet which satisfy c1.
Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#drop
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit

7.14.6 match

Command: match {access-group *<acl-index-or-name>* | ip dscp *<dscp-list>* | ip precedence *<ip-precedence-list>* | ipv6 access-group *<acl-index-or-name>* | ipv6 dscp *<dscp-list>* | ipv6 flowlabel *<flowlabel-list>* | vlan *<vlan-list>* | cos *<cos-list>*}
no match {access-group | ip dscp | ip precedence| ipv6 access-group| ipv6 dscp | ipv6 flowlabel | vlan | cos}
Function: Configure the match standard of the class map; the no form of this command deletes the specified match standard.
Parameter: **access-group *<acl-index-or-name>*** match specified IP ACL, MAC ACL or IPv6 standard ACL , the parameters are the number or name of the ACL;
ip dscp <dscp-list> and ipv6 dscp <dscp-list> match specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the range is 0~63;
ip **precedence** <***ip-precedence-list>*** match specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0~7;
ipv6 access-group <acl-index-or-name> match specified IPv6 ACL, the parameter is the number or name of the IPv6 ACL;
ipv6 flowlabel <flowlabel-list> match specified IPv6 flow label, the parameter is IPv6 flow label value, the range is 0~1048575;
vlan **<vlan-list**> ***match*** specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the range is 1~4094;
cos <cos-list> match specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS, the range is 0~7.
Default: No match standard by **default**
Command Mode*: Class-map* Mode
Usage Guide: Only one match standard can be configured in a class map. When configuring the match ACL, permit rule as the match option, apply Policy Map action. Deny rule as the excluding option, do not apply Policy Map action. (The deny rule is not supported issuing in PBR, please pay attention to avoid it.) If configure another match rule after one was configured, the operation fails, but configure the same match rule will cover the previous.
Example: Create a class-map named c1, and configure the class rule of this class-map to match packets with IP Precedence of 0.
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match ip precedence 0
Switch(Config-ClassMap-c1)#exit

7.14.7 mls qos aggregate-policy

Command:

Single Bucket Mode:

mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> [{conform-action ACTION | exceed-action ACTION }]

Dual Bucket Mode:

mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> (pir <peak_rate_bps> | <maximum_burst_bytes>) ({conform-action ACTION | exceed-action ACTION | violate-action ACTION)

ACTION definition:

drop | transmit | set-internal-priority <intp_value> | set-cos-transmit <new-cos> | set-dscp-transmit <new-dscp> | set-prec-transmit <ip-precedence> | set-drop-precedence < new-drop-priority>

[no] mls qos aggregate-policy <policer_name>

Function: Define an aggregate policy command, analyze the working mode of the token bucket, whether it is single rate singe bucket, singe rate dual bucket or dual rate dual bucket, and set the corresponding action for different color packets. The no operation will delete the mode configuration.

Parameters: policer_name: the name of aggregation policy;

bits_per_second: the committed information rate - CIR , in Kbps, ranging from 1 to 10000000;

normal_burst_bytes: the committed burst size – CBS, in kb, ranging from 1 to 1000000. When the configured CBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt;

maximum_burst_bytes: the peak burst size - PBS, in kb, ranging from 1to 1000000. When the configured PBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt. Notice: this configuration only exists in dual bucket mode;

pir peak_rate_bps: the peak information rate - PIR, in kbps, ranging from 1to 10000000. Without configuring PIR, the Police works in the single rate dual bucket mode; otherwise in the dual rate dual bucket mode. Notice: this configuration only exist in the dual bucket mode.

conform-action: When it does not exceed CIR rate and the packet is green, the default action is transmit.

exceed-action: the actions to take when the CIR is exceeded but PIR isn't, which means the messages are yellow, the default is Drop;

violate-action: the actions to take when the PIR is exceeded, which means the messages are red, the default is Drop.

ACTION:

drop/transmit: Drop/transmit the packets

set-internal-priority **<intp_value>:** Modify the internal priority of the packets

set-cos-transmit< new-cos >: Modify the L2 COS value of the packets

set-drop-precedence < new-drop-priority >: Modify the drop priority of the packets
set-dscp-transmit <new-dscp> : Modify dscp
set-prec-transmit< ip-precedence > : Modify TOS
Default: No aggregation Policy is defined by default; the default action of exceed-action and violate-action both is drop.
Command mode: Global Mode
Usage Guide: The CLI can support both singe bucket and dual bucket configuration, and determine which one by checking whether PIR or PBS is configured. When configuring with CLI, after configuring CBS, if the action is directly configured, the mode is single rate single bucket; if only PBS is configured, the mode is single rate dual bucket three colors; if PIR and PBS are configured, the mode is dual rate dual bucket three **colors**. The actions of set and policy selected by policy map are same, the action of policy can cover the action of the set. Furthermore, If the actions of exceed-action and violate-action are set-internal-priority in policy, <intp_value> must be same.
Example: Set the dual bucket mode, CIR is 1000, CBS is 1000, PIR is 20000, PBS is 10000. The action is transmit when CIR is exceeded but PIR isn't, which means the messages are yellow.
Switch(config)#mls qos aggregate-policy color 10000 1000 pir 20000 10000 exceed-action transmit

7.14.8 mls qos cos

Command: mls qos cos {*<default-cos>*}
no mls qos cos
Function: Configures the default CoS value of the port; the 'no **mls qos cos'** command restores the default setting.
Parameters: *<default-cos>* is the default CoS value for the port, the valid range is 0 to 7.
Default: The default CoS value is 0.
Command mode: Port Configuration Mode.
Usage Guide: Configure the default CoS value for switch port. In default configuration, the message ingress cos from this port are default value whether the message with tag. If the message without tag, the message cos value for tag is enactmented.
Example: Setting the default CoS value of ethernet port 1/0/1 to **7,** i.e., packets coming in through this port will be assigned a default CoS value of 7 if no CoS value present .
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mls qos cos 7

7.14.9 mls qos internal-priority

Command: mls qos internal-priority {*<default-intp>* }
no mls qos internal-priority

Function: Configure the default internal priority of the port, the no command restores the default.

Parameter: ***<default-intp>*** the default internal priority of the port, ranging from 0 to 119.

Default: The default intp value is 0.

Command Mode: Port mode

Usage Guide: Configure the default internal priority of the port. If there is no dscp and cos fields of the trust packets, the ingress packet of the port will obtain a default internal priority. The packet's internal priority may be reset according to the configured QoS policy.

Example: Configure the default intp value as 40 on ethernet 1/0/1.

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#mls qos internal-priority 40

7.14.10 mls qos map

Command: mls qos map (cos-intp < in-cos list > | dscp-dscp <in-dscp list> to <out-dscp> | dscp-intp <in-dscp list> to <intp> | intp-exp <exp1。。。exp8>|exp-intp <intp>| intp-cos <intp> to <in-cos list>|intp-dp <intp> to <dp1…dp8> |intp-dscp <intp> to <in-dscp list|intp-quene <intp> to <quene>)

no mls qos map (cos-intp | dscp-dscp | dscp-intp | dscp-dp| intp-exp | exp-intp| intp-cos|intp-dp|intp-dscp|intp-quene)

mls qos map intp-exp <exp1。。。exp8>no mls qos map intp-exp

Function: Set the priority mapping of QoS, the no command restores the default mapping.

Parameters**: cos-dp <dp1…dp8>** defines the mapping from CoS to dp (drop precedence) value, <dp1..dp8> are 8 dp value corresponding to the 0 to 7 CoS value, each dp value is delimited with space, ranging from 0 to 2;

cos-intp < in-cos list > defines the mapping from ingress L2 COS value to the internal priority, <in-cos list> are 8 internal priority values, corresponding to the cos value from 0 to 7 respectively. each internal priority value is delimited with space**,** ranging from 0 to 7.

dscp-dscp defines the mapping from ingress DSCP to egress DSCP, <in-dscp ***list***> stand for incoming DSCP values, up to 8 values are supported, each DSCP value is delimited with space, ranging from 0 *to* 63, <out-dscp> is the output DSCP value, ranging from 0 to 63;

dscp-intp defines the mapping from DSCP to intp;

dscp-dp defines the mapping from DSCP to dp;

intp-exp < exp1。。。exp8> defines the mapping from intp to exp, <exp1…exp8> are 8 exp value corresponding to the 0 to 7 intp value, each exp value is delimited with space, ranging from 0 to 7.

Default: Default mapping values are:

Ingress COS-TO-Drop-Precedence map:

COS:	0	1	2	3	4	5	6	7
DP:	**0**	**0**	**0**	0	0	0	0	0

Ingress COS-TO-Internal-Priority map:

COS: 0 1 2 3 4 5 6 7

INTP: 0 1 2 3 4 5 6 7

Ingress DSCP-TO-Internal-Priority map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

0: **0** 0 0 0 0 0 0 0 1 1

1: 1 1 1 1 1 *1* 2 2 2 2

2: 2 2 2 2 3 3 3 3 3 3

3: 3 3 4 4 4 4 4 4 4 4

4: 5 5 5 5 5 5 5 5 6 6

5: 6 6 6 6 6 6 7 7 *7* 7

*6***:** 7 7 7 7

Ingress DSCP-TO-DSCP map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

0: 0 0 0 0 0 0 0 0 8 8

1: 8 8 8 8 8 8 16 16 16 16

2: 16 16 16 16 24 24 24 24 24 24

3: 24 24 32 32 32 32 32 32 32 32

4: 40 40 40 40 40 40 40 40 48 48

5: 48 48 48 48 48 48 56 56 56 56

6: 56 56 56 56

Ingress DSCP-TO-Drop-Precedence map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

0: 0 0 0 0 0 0 0 0 0 0

1: 0 0 0 0 0 0 0 0 0 0

2: 0 0 0 0 0 0 0 0 0 0

3: 0 0 0 0 0 0 0 0 0 0

4: 0 0 0 0 0 0 0 0 0 0

5: 0 0 0 0 0 0 0 0 0 0

6: 0 0 0 0

Egress Internal-Priority-TO-EXP map:

INTP: 0 1 2 3 4 5 6 7

EXP: 0 1 2 3 4 5 6 7

Command mode: Global Mode

Usage Guide: INTP means the chip internal priority setting, DP means the drop precedence. Because of the internal DSCP value have 64 and the chip internal priority only 8, the dscp-cos

mapping need 8 continuum dscp-inside mapping to the same INTP or DP.
Example: 1. Setting the CoS-to-dp mapping value to 1 1 1 1 1 1 1 1 from the default.
Switch(config)#mls qos map cos-dp 1 1 1 1 1 1 1 1
2. Mapping DSCP 1 to dp 2.
Switch(config)#mls qos map dscp-dp 1 to 2

7.14.11 mls qos queue weight

Command: mls qos queue weight <weight0..weight7>
no mls qos queue weight
Function: After configure this command, the queue weight is set.
Parameters: <weight0..weight7> defines the queue weight, for WDRR algorithm, this configuration is valid, for SP algorithm, this configuration is invalid, weight ranging from 0 to 255. The absolute value of weight is meaningless. WDRR allocates bandwidth by using 8 weight values.
Default: The queue weight is 1 1 1 1 1 1 1 0, and the seventh queue weight is the users configured.
Command mode: Global Mode.
Usage Guide: If the queue weight is configured as 0, join the queue to SP algorithm. If the queue weight is not configured as 0, join the queue to WDRR, and turns into SP+WDRR. When managing the queue, select a queue according to WDRR algorithm in WDRR group, WDRR and SP queues execute the strict priority management mode.
Example: Configure the queue weight as 1 2 3 4 5 6 7 8.
Switch(config)#mls qos queue weight 1 2 3 4 5 6 7 8

7.14.12 mls qos queue wred

This command is not supported by switch.

7.14.13 mls qos queue wdrr weight

This command is not supported by switch.

7.14.14 mls qos trust

Command: mls qos trust {cos | dscp|exp}
no mls qos trust {cos | dscp|exp}
Function: Configures port trust; the no **command disables** the current trust status of the port.
Parameters: cos configures the port to trust CoS value; dscp configures the port to trust DSCP value; exp configures the port to trust EXP value.

Default: Trust CoS value.

Command mode: Port Configuration Mode.

Usage Guide:

trust dscp mode: can set the intp field based dscp-to-intp mapping, set the dp value based dscp-to-dp mapping, set DSCP value based dscp-to-dscp mapping.

Example:

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0)# mls qos trust dscp

7.14.15 pass-through-cos

command：pass-through-cos

no pass-through-cos

Fcuntion: It is prohibited to rewrite L2 cos value when message exits。

Parameters:

Default： The L2 CoS value can be rewritten when the default message exits。

Command mode： Port Configuration Mode。

Usage Guide:

When the default message exits, the L2 CoS value can be rewritten. Configure pass through cos on the inbound port, and the message will be prohibited from rewriting the L2 CoS value on the outbound port. This command can be used with other QoS commands, such as mls qos trust. After other QoS actions take effect, the CoS value carried at the initial entry is retained at the message exit。

Example: Configure the trust dscp value on port ethernet1/0/1, that is, the messages are classified according to the dscp value, but the CoS value of the message is not changed.

switch(config-if-ethernet1/0/1)#pass-through-cos

7.14.16 pass-through-dscp-exp

Command: pass-through-dscp

no pass-through-dscp

Function: Forbid the egress packets rewriting DSCP value.

Parameter: None.

Default: The egress packets rewrite DSCP value.

Command Mode: Port Mode

Usage Guide: The egress packets can not rewrite DSCP value when configuring pass-through-dscp on the ingress. This command may associate with other commands of QoS, such as mls qos trust command. After QoS actions are valid, the egress packets save the original DSCP value.

Example: Configuring ethernet port 1/0/1 to trust CoS value, i.e., classifying the packets according to CoS value.

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#mls qos trust cos
Switch(config-if-ethernet1/0/1)#pass-through-dscp

7.14.17 policy

Command:
Single Bucket Mode:
policy <bits_per_second> <normal_burst_bytes> ({conform-action ACTION | exceed-action ACTION})
Dual Bucket Mode:
policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] | **<maximum_burst_bytes> [{conform-action ACTION | exceed-action ACTION | violate-action ACTION }]**

ACTION definition:
drop | transmit | set-dscp-transmit <dscp_value> | set-prec-transmit <**ip_precedence_value**> | set-cos-transmit <cos_value> | **set-internal-priority <inp_value> | set-Drop-Precedence <dp_value>**

no policy

Function: The non-aggregation policy command supporting three colors. Determine whether the working mode of token bucket is singe rage single bucket, single rate dual bucket or dual rate dual bucket, set the corresponding action to the different color packets. The no command will delete the mode configuration.

Parameters: bits_per_second: The committed information rate – CIR (Committed Information Rate), in Kbps, ranging from 1 to 10000000;

normal_burst_bytes: The committed burst size – CBS (Committed Burst Size), in byte, ranging from 1 to 1000000. When the configured CBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt;

maximum_burst_bytes**: The peak burst size – PBS (Peak Burst Size), in byte,** ranging from 1 to 10000000. When the configured PBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt. Notice: this configuration only exists in dual bucket mode;

pir peak_rate_bps: The peak information rate – PIR (Peak Information Rate), in kbps, ranging from 1 to 10000000. Without configuring PIR, the Police works in the single rate dual bucket mode; otherwise in the dual rate dual bucket mode. Notice: this configuration only exists in dual bucket mode;

violate-action: The actions to take when the PIR is exceeded, which means the messages are red, the default as drop;

conform-action: The action to take when the CIR is not exceeded, which means the messages are green, the default as transmit;

exceed-action: The actions to take when the CIR is exceeded but PIR isn't, which means the

messages are yellow, the default as drop.

ACTION include:
drop**/transmit:** Drop/transmit the packets
set-dscp-transmit sets DSCP, it is valid to IPv4 and IPv6 packets, only set-dscp-transmit or set-prec-transmit can be selected.
set-prec-transmit **sets TOS, only set-prec-transmit** or set-dscp-transmit can be selected
set-internal-priority sets the internal priority of the packets
set-Drop-Precedence sets the drop precedence of the packets
set-cos-transmit sets the CoS value of the L2 packets
Default: No policy action; the default action of conform-action is transmit, while that of exceed-action and violate-action are both drop.
Command mode: Policy class map configuration Mode
Usage Guide:
The CLI can support both singe bucket and dual bucket configuration, and determine which one to select by checking whether PIR or PBS is configured. When configuring with CLI, after configuring CBS, if the action is directly configured, the mode is single bucket dual color; if only PBS is configured, the mode is single rate dual bucket three color; if PIR and PBS are configured, the mode is dual rate dual bucket three color. 'set' and 'policy'（policy aggregate） are selected and have the same action in Policy Map, then the action selected by 'policy' will cover the action of 'set'.
Example: In the policy class table configuration mode, set the CIR as 1000, CBS as 2000 and the action when CIR is not exceeded as transmitting the messages after changing DSCP to 23, and the action triggered by exceeding CIR as transmit without changing the messages.
Switch(config)#class-map cm
Switch(config-classmap-cm)#match cos 0
Switch(config-classmap-cm)#exit
Switch(config)#policy-map 1
Switch(config-policymap-1)#class cm
Switch(config-policymap-1-class-cm)#policy 1000 2000 conform-action set-dscp-transmit 23

7.14.18 policy aggregate

Command: policy aggregate <*aggregate-policy-name*>
no policy aggregate <*aggregate-policy-name*>
Function: Police Map reference aggregate policy, applies an aggregate policy to classified traffic; the no command deletes the specified aggregate policy.
Parameters: <*aggregate-policy-name*> is the policy set name.
Default: No policy is configured by default.
Command mode: Policy class map configuration Mode
Usage Guide: The same policy set can be referred to by different policy class maps.
Example: Create class-map, the match rule is the cos value is 0; policy-map is 1, enter the policy

map mode, set the Policy and choose the color policy for the current list.
Switch(config)#class-map cm
Switch(config-classmap-cm)#match cos 0
Switch(config-classmap-cm)#exit
Switch(config)#policy-map 1
Switch(config-policymap-1)#class cm
Switch(config-policymap-1-class-cm)#policy aggregate color

7.14.19 policy-map

Command: policy-map <*policy-map-name*>
no policy-map <*policy-map-name*>
Function: Creates a policy map and enters the policy map mode; the 'no **policy-map <*policy-map-name*>**' command deletes the specified policy map.
Parameters: <*policy-map-name*> is the policy map name.
Default: No policy map is configured by default.
Command mode: Global Mode
Usage Guide: PBR classification matching and marking next hop operations can be done in policy map configuration mode.
Example: Creating and deleting a policy map named 'p1'.
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#exit
Switch(config)#no policy-map p1

7.14.20 service-policy input

Command: service-policy input <*policy-map-name*>
no service-policy input {<*policy-map-name*>}
Function: Applies a policy map to the specified port; the no command deletes the specified policy map applied to the port or deletes all the policy maps applied on the ingress direction of the port .
Parameters: input <*policy-map-name*> applies the specified policy map to the ingress direction of switch port.
no command will delete all the policy maps applied on the ingress direction of the port if there is not the specified policy map name.
Default: No policy map is bound to port by default.
Command mode: Port Configuration Mode.
Usage Guide: Only one policy map can be applied to each direction of each port or VLAN interface. It is not recommended to use policy map on VLAN and VLAN's port at the same time.
Example:
Bind policy p1 to ingress Ethernet port1/0/1.

Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#service-policy input p1
Bind policy p1 to ingress redirection of v1 interface.
Switch(config)#interface vlan 1
Switch(Config-If-vlan1)#service-policy input p1

7.14.21 service-policy input vlan

Command: service-policy input <*policy-map-name*> vlan <*vlan-list*>
no service-policy input {<*policy-map-name*>} vlan < *vlan-list*>
Function: Applies a policy map to the specified VLAN interface; the no command deletes the specified policy map applied to the VLAN interface or deletes all the policy maps applied in the ingress direction of the vlan interface .
Parameters: input <*policy-map-name*> applies the specified policy map to the ingress direction of switch VLAN interface.
vlan <vlan-list> the vlan list of binding policy map.
no command will deletes all the policy maps applied in the ingress direction of the vlan interface if there is not the specified policy map name.
Default: No policy map is bound to VLAN interface by default.
Command mode: Global Configuration Mode.
Usage Guide: Only one policy map can be applied to each direction of each port or VLAN interface. It is not recommended to use policy map on VLAN and VLAN's port at the same time.
Example:
Bind policy p1 to ingress of VLAN interface v2, v3, v4, v6.
Switch(config)# service-policy input p1 vlan 2-4;6

7.14.22 set

Command: set {ip dscp <new-dscp> | internal priority <new-inp> | ip [default] nexthop [vrf <vrf>] <ip-address> | ipv6 [default] nexthop [vrf <vrf>] <*nexthop-ip*> | cos <new-cos>}
no set {ip dscp | internal priority | ip *nexthop* | ipv6 nexthop | cos}
Function: **Assign a new DSCP** for the classified traffic; the no form of this command delete assigning the new values.
Parameter: ip dscp <new-dscp> new DSCP value, do not distinguish v4 and v6.
ipv6 flowlabel <new-flowlabel> new IPv6 FL value.
ip default nexthop [vrf <vrf>**] <*ip-address*>** next hop IP address, set the route of nexthop for PBR, default means a route of the lowest priority, it's priority is lower than route map and neighbor map, vrf means virtual route forwarding, the ranging from 0 to 252.
ipv6 default nexthop [vrf <vrf**>] <ip-address>** next hop IPv6 address, set the route of nexthop for IPv6 PBR, default means a route of the lowest priority, it's priority is lower than route map and

neighbor map, vrf means virtual route forwarding, the ranging from 0 to 252.
cos <new cos> new COS value.
Default: Not assigning by default.
Command Mode: Policy Class-map Mode
Usage Guide: Only the classified traffic which matches the matching standard will be assigned with the new values.
Example: Set the **IP** DSCP of the packets matching the c1 class rule to 3.
Switch(config)#*policy-map p1*
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip dscp 3
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit

7.14.23 show class-map

Command: show class-map [<*class-map-name*>]
Function: Displays class map of QoS.
Parameters: <*class-map-name*> is the class map name.
Default: N/A.
Command mode: Admin Mode.
Usage Guide: Displays all configured class-map or specified class-map information.
Example:
Switch # show class-map
Class map name:c1, used by 1 times
match acl name:1

Displayed information	Explanation
Class map name:c1	Name of the Class map
used by 1 times	Used times
match acl name:1	Classifying rule for the class map.

7.14.24 show policy-map

Command: show policy-map [<*policy-map-name*>]
Function: Displays policy map *of* QoS.
Parameters: <policy-map-name> is the policy map name.
Default: N*/A*.
Command mode: Admin Mode.
Usage Guide: Displays all configured policy-map or specified policy-map information.
Example:
Switch#show policy -map
Policy Map p1, used by 0 port

Class Map name: **c1**
policy CIR: 1000 CBS: 1000 PIR: 200 PBS: 3000
conform-action:
transmit
exceed-action:
drop
violate-action:
drop

Displayed information	Explanation
Policy Map p1	Name of policy map
Class map name:c1	Name of the class map referred to
policy CIR: 1000 CBS: 1000 PIR: 200 PBS: 3000 conform-action: transmit exceed-action: drop violate-action: drop	Policy implemented

7.14.25 show mls qos interface

Command: show mls qos {interface [<interface-id>] [policy | queuing] | vlan <vlan-id>} | [begin | include | exclude <regular-expression>]
Function: Displays QoS configuration information on a port.
Parameters: <interface-id> is the port ID; **<**vlan-id>: VLAN ID; policy is the policy setting on the port; queuing is the queue setting for the port.
Default: N/A.
Command mode: Admin Mode.
Usage Guide: In single rate single bucket mode, the messages can only red or green when passing police. In the print information, in-profile means green and out-profile means red. In dual bucket mode, there are three colors of messages. But the counter can only count two kinds of messages, the red and yellow ones will both be treated as out-profile. Only when configuring ingress policies, there is statistic information.
Example:
Switch#show mls qos interface ethernet 1/0/2
Ethernet 1/0/2
Default COS: 0
Trust: COS DSCP EXP
Attached Policy Map for Ingress: p1

```
Classmap      classified      in-profile      out-profile (in packets)
     c1            20                10                10
   c2            NA                NA                NA
（If there is no Accounting for Class Map, show NA）

Internal-Priority-TO-Queue map:
INTP      0       1       2       3       4       5       6       7
-----------------------------------------------------------------------
Queue        0       1       2       3       4       5       6       7

Queue Algorithm: WRR
Queue weights:
Queue        0       1       2       3       4       5       6       7
-----------------------------------------------------------------------------------------------
weight          1       2       3       4       5       6       7       8

Bandwidth Guarantee Configuration:
Queue        0       1       2       3       4       5       6       7
-----------------------------------------------------------------------------------------------
MinBW(K)      128         0           0       0       0       0       0       0
   MaxBW(K)   256    0  0       0       0       0       0       0
```

Display Information	Explanation
Ethernet1/0/2	Port name
default cos:0	Default CoS value of the port
Trust: COS DSCP EXP	The trust state of the port
Attached Policy Map for Ingress: p1	Policy name bound to port
ClassMap	ClassMap name
classified	Total data packets match this ClassMap. If there is no Accounting for Class Map, show NA
in-profile	Total in-profile data packets match this ClassMap. If there is no Accounting for Class Map, show NA
out-profile	Total out-profile data packets match this ClassMap. If there is no Accounting for Class Map, show NA
Internal-Priority-TO-Queue map::	Internal-Priority to queue mapping
Queue Algorithm:	WRR or PQ queue out method
Queue weights	Queue weights configuration
Bandwidth Guarantee Configuration	Bandwidth guarantee configuration

Switch(config)#show mls qos interface ethernet1/0/2 queuing

```
Ethernet1/0/2:
   Internal-Priority-TO-Queue map:
   INTP    0        1        2        3        4        5        6        7
   ---------------------------------------------------------------------------
   Queue     0        1        2        3        4        5        6        7

   Queue Algorithm: WRR
   Queue weights:
   Queue          0        1        2        3        4        5        6        7
-------------------------------------------------------------------------------------------------
   weight         1        2        3        4        5        6        7        8

   Bandwidth Guarantee Configuration:
   Queue          0        1        2        3        4        5        6        7
   ---------------------------------------------------------------------------------------------------
   MinBW(K)     128          0              0        0        0        0        0        0
   MaxBW(K)    256     0  0        0        0        0        0        0
```

Display Information	Explanation
Internal-Priority-TO-Queue map::	Internal-Priority to queue mapping
Queue Algorithm:	WRR or PQ queue out method
Queue weights	Queue weights configuration
Bandwidth Guarantee Configuration	Bandwidth guarantee configuration

```
Switch # show mls qos interface ethernet 1/0/2 policy
Ethernet1/0/2:
   Attached Policy Map for Ingress: p1
   Accounting: ON
   Classmap       classified       in-profile       out-profile (in packets)
     c1                0                0                0
```

Display Information	Explanation
Ethernet1/0/2	Port name
Attached Policy Map for Ingress: p1	Policy name bound to port
ClassMap	ClassMap name
classified	Total data packets match this ClassMap.
in-profile	Total in-profile data packets match this ClassMap.
out-profile	Total out-profile data packets match this ClassMap.

```
Switch #show mls qos vlan 100
```

Vlan 100:
Attached Policy Map for Ingress: p1
Classmap classified in-profile out-profile (in packets)
c1 20 10 10
c2 NA NA NA

7.14.26 show mls qos in {interface <interface-name> policy | vlan <vlan-id>

Command: show mls qos in {interface <interface-name> policy | vlan <vlan-id>
Function: Show the policy configuration information of the in direction of port or vlan.
Parameters: <interface-name>: port name.
Command Mode: Admin and configuration mode
Default: None.
Usage Guide: Show the policy configuration information of the in direction.
Example: Show the policy configuration information of the in direction.
Switch#show mls qos in interface ethernet1/0 policy
Ethernet1/0:
Attached Policy Map for Ingress: p

7.14.27 show mls qos maps

Command: show mls qos maps [cos-dp| cos-intp | dscp-dscp | dscp-intp | dscp-dp |intp-exp] | [begin | include | exclude <regular-expression>]
Function: Display the configuration of QoS mapping.
Parameters: cos-dp: The mapping from ingress L2 **CoS** to drop precedence
cos-intp: The mapping from ingress L2 COS to the internal priority
dscp-dscp**:** The mapping from ingress DSCP to DSCP
dscp-intp: The mapping from ingress DSCP to internal priority
dscp-dp: The mapping from ingress DSCP to drop precedence
intp-exp: **The** mapping from IntPrio to EXP
Default: None.
Command mode: Admin and Configuration Mode.
Usage Guide: Display the map configuration information of QoS.
Example: Display configuration information of the mapping table.
Switch (config)#show mls qos maps

Ingress COS-TO-Internal-Priority map:

COS: 0 1 2 3 4 5 6 7

INTP: 0 1 2 3 4 5 6 7

Ingress DSCP-TO-Internal-Priority map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	1	1
1:	1	1	1	1	1	1	2	2	2	2
2:	2	2	2	2	3	3	3	3	3	3
3:	3	3	4	4	4	4	4	4	4	4
4:	5	5	5	5	5	5	5	5	6	6
5:	6	6	6	6	6	6	7	7	7	7
6:	7	7	7	7						

Ingress COS-TO-Drop-Precedence map:

COS: 0 1 2 3 4 5 6 7

DP: 0 0 0 0 0 0 0 0

Ingress DSCP-TO-DSCP map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	8	8
1:	8	8	8	8	8	8	16	16	16	16
2:	16	16	16	16	24	24	24	24	24	24
3:	24	24	32	32	32	32	32	32	32	32
4:	40	40	40	40	40	40	40	40	48	48
5:	48	48	48	48	48	48	56	56	56	56
6:	56	56	56	56						

Ingress DSCP-TO-Drop-Precedence map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	0	0
1:	0	0	0	0	0	0	0	0	0	0
2:	0	0	0	0	0	0	0	0	0	0
3:	0	0	0	0	0	0	0	0	0	0
4:	0	0	0	0	0	0	0	0	0	0
5:	0	0	0	0	0	0	0	0	0	0
6:	0	0	0	0						

Ingress EXP-TO-Internal-Priority map:

EXP: 0 1 2 3 4 5 6 7

```
  ----------------------------------------
INTP: 0     1     2     3     4     5     6     7

Ingress EXP-TO-Drop-Precedence map:
EXP:   0     1     2     3     4     5     6     7
                  ----------------------------------------
               DP:     0     0     0     0     0     0     0     0

Egress Internal-Priority-TO-EXP map:
INTP: 0     1     2     3     4     5     6     7
  ----------------------------------------
EXP:   0     1     2     3     4     5     6     7
```

7.14.28 show mls qos vlan

Command: show mls qos vlan <v-id>
Parameters: v-id: the ranging from 1 to 4094.
Command Mode: Admin mode.
Default: None.
Example:
Switch#show mls qos vlan 1

7.14.29 show mls qos aggregate-policy

Command: show mls qos aggregate-policy [<aggregate-policy-name>]

Parameter: [policy-name] the policy name
Default: **None**.
Command Mode: Admin mode and configuration mode
Usage Guide**:** Show the aggregate-policy configuration.
Example:
Switch#**show** mls qos aggregate-policy
aggregate policy p
CIR: 1 CBS: 1 PBS: 1
conform-action:
transmit
exceed-action:
drop
violate-action:

drop
Not used by any policy map

7.14.30 transmit

Command: transmit
no transmit
Function: Transmit data package that match the class, the no command cancels the assigned action.
Parameters: None.
Default: Do not set the action.
Command mode: Policy class map configuration mode
Usage Guide: Send the packet directly after configure this command.
Example: Send the packet which satisfy c1.
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#transmit
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit

7.15 Flow-based Redirection

7.15.1 access-group redirect to interface ethernet

Command: access-group <*aclname*> redirect to interface [ethernet <*IFNAME*> | <*IFNAME*>]
no access-group <*aclname*> redirect
Function: Specify flow-based redirection*; 'no* access-group <aclname> redirect' command is used to delete flow-based redirection.
Parameters**: <aclname> name of** the flow , only supports digital standard IP ACL, digital extensive IP ACL, nomenclatural standard IP ACL, nomenclatural extensive IP ACL, digital standard IPv6 ACL, and nomenclatural standard IPv6 ACL. Parameters of **Timerange** and **Portrange** can not be set in ACL; the type of ACL should be Permit. ***<IFNAME>*** the destination port of redirection.
Command Mode: Physical Port Configuration Mode.
Usage Guide: 'no access-group <aclname> redirect' command is used to delete flow-based redirection. Flow-based redirection function enables the switch to transmit the data frames meeting some special condition to another specified port.
Examples: Redirecting the frames whose source IP is 192.168.1.111 received from port 1 to port 6,
Switch(config)#access-list 1 permit host 192.168.1.111

Switch(config)# interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# access-group 1 redirect to interface ethernet 1/0/6

7.15.2 match vlan <1-4096> redirect interface (ethernet|) IFNAME

Command: match vlan <1-4096> redirect interface **(ethernet|) IFNAME**

no match vlan <1-4096> redirect

Command Mode: Port Mode.

Function: Configure the vlan redirection function of the port.

Parameters: vlan <1-4096>: vlanID

IFNAME: Port name

Usage Guide: Redirect the flow which matches the packet of vid from the appointed port to another port.

Example: Redirect the flow of vlan1 of 1/0/1 to the port of 1/0/2.

(config-if-ethernet1/0/1)#match vlan 1 redirect interface ethernet 1/0/2

7.15.3 port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME

Command: port-redirect match vlan <1-4094> source-port **interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME**

no port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME

Function: Configure the vlan redirection function of the port.

Parameters: vlan <1-4094>: vlanID;

IFNAME: Port name.

Command Mode: Global Mode.

Usage Guide: This command can redirect the flow which is matching with the packet of vid to another port from the appointed port. The ports of source-port and destination-port must be the trunk port.

Example: Redirect the flow of vlan1 of port 1/0/1 to the port 1/0/2.

(config)#port-redirect match vlan 1 source-port interface ethernet 1/0/1 destination-port interface ethernet 1/0/2

7.15.4 show flow-based-redirect

Command: show flow-based-redirect {interface [ethernet <*IFNAME*> | <*IFNAME*>]}
Function: Display the information of current flow-based redirection in the system/port.
Parameters: 1. No specified port, display the information of all the flow-based redirection in the system.

2. Specify ports in ***<IFNAME>***, display the information of the flow-based redirection configured in the ports listed in the interface-list.

Command Mode: Admin Mode and Configuration Mode.
Usage Guide: This command is used to display the information of current flow-based redirection in the system/port.
Examples:
Switch(config)# show flow-based-redirect
Flow-based-redirect config on interface ethernet 1/0/1:
RX flow (access-list 1) is redirected to interface Ethernet1/0/6

7.15.5 vlan-port-redirect vlan maximum <1-1000>

Command: vlan-port-redirect vlan maximum <1-1000>
no **vlan-port-redirect vlan maximum**
Command Mode: Global Mode.
Function: Configure the maximum number of vlan of redirect on each port.
Default: 500
Parameters: maximum <1-1000>: maximum number of vlan
Usage Guide: Configure the maximum number of vlan of redirect on each port.
Example: Configure the maximum number of vlan of redirect on 1/0/1 as 600.
(config)# vlan-port-redirect vlan maximum 600

7.16 Egress QoS

7.16.1 mls qos egress green remark

Command: [no] mls qos egress green remark
Function: Set Egress QoS remarking to take effect for green packets, no command does not take effect to green packets.
Parameter: None.
Default: Do not modify green packets.
Command Mode: Global Mode

Usage Guide: QoS attribute of green packets will be modified by remark table after enable the global configuration.

Example: Egress remarking takes effect for green packets.

Switch(config)#mls qos egress green remark

7.16.2 mls qos map

Command: mls qos map cos-cos <color> <cos1…cos8>

mls qos map cos-dscp <color> <dscp1…dscp8>

mls qos map dscp-cos <color> <dscp list> to <cos>

mls qos map dscp-dscp <color> <dscp list> to <dscp>

no mls qos map (cos-cos | cos-dscp | dscp-cos | dscp-dscp) <color>

Function: Set mapping between Egress QoS remark tables, no command restores the default configuration.

Parameters: cos-cos：Set mapping from cos to cos for Egress remark cos table

cos-dscp：Set mapping from cos to dscp for Egress remark cos table

dscp-cos：Set mapping from dscp to cos for Egress remark dscp table

dscp-dscp：Set mapping from dscp to dscp for Egress remark dscp table

<color>：Packet's colors, including green、yellow、red

<cos>：cos value, its range from 0 to 7

<dscp>： dscp value, its range from 0 to 63

<dscp list>：1 to 8 dscp values

Default: default mapping:

COS-TO-COS-GREEN map:

COS: 0 1 2 3 4 5 6 7

COS: 0 1 2 3 4 5 6 7

COS-TO-COS-YELLOW map:

COS: 0 1 2 3 4 5 6 7

COS: 0 1 2 3 4 5 6 7

COS-TO-COS-RED map:

COS: 0 1 2 3 4 5 6 7

COS: 0 1 2 3 4 5 6 7

COS-TO-DSCP-GREEN map:

COS: 0 1 2 3 4 5 6 7

DSCP: 0 8 16 24 32 40 48 56

COS-TO-DSCP-YELLOW map:

COS:	0	1	2	3	4	5	6	7
DSCP:	0	8	16	24	32	40	48	56

COS-TO-DSCP-RED map:

COS:	0	1	2	3	4	5	6	7
DSCP:	0	8	16	24	32	40	48	56

DSCP-TO-COS-GREEN map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	1	1
1:	1	1	1	1	1	1	2	2	2	2
2:	2	2	2	2	3	3	3	3	3	3
3:	3	3	4	4	4	4	4	4	4	4
4:	5	5	5	5	5	5	5	5	6	6
5:	6	6	6	6	6	6	7	7	7	7
6:	7	7	7	7						

DSCP-TO-COS-YELLOW map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	1	1
1:	1	1	1	1	1	1	2	2	2	2
2:	2	2	2	2	3	3	3	3	3	3
3:	3	3	4	4	4	4	4	4	4	4
4:	5	5	5	5	5	5	5	5	6	6
5:	6	6	6	6	6	6	7	7	7	7
6:	7	7	7	7						

DSCP-TO-COS-RED map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	1	1
1:	1	1	1	1	1	1	2	2	2	2
2:	2	2	2	2	3	3	3	3	3	3
3:	3	3	4	4	4	4	4	4	4	4
4:	5	5	5	5	5	5	5	5	6	6
5:	6	6	6	6	6	6	7	7	7	7
6:	7	7	7	7						

DSCP-TO-DSCP-GREEN map:

d1 : d2	0	1	2	3	4	5	6	7	8	9

```
0:        0  10   2   3   4   5   6   7   8   9
1:       10  11  12  13  14  15  16  17  18  19
2:       20  21  22  23  24  25  26  27  28  29
3:       30  31  32  33  34  35  36  37  38  39
4:       40  41  42  43  44  45  46  47  48  49
5:       50  51  52  53  54  55  56  57  58  59
6:       60  61  62  63

DSCP-TO-DSCP-YELLOW map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:        0   9   2   3   4   5   6   7   8   9
1:       10  11  12  13  14  15  16  17  18  19
2:       20  21  22  23  24  25  26  27  28  29
3:       30  31  32  33  34  35  36  37  38  39
4:       40  41  42  43  44  45  46  47  48  49
5:       50  51  52  53  54  55  56  57  58  59
6:       60  61  62  63

DSCP-TO-DSCP-RED map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:        0   1   2   3   4   5   6   7   8   9
1:       10  11  12  13  14  15  16  17  18  19
2:       20  21  22  23  24  25  26  27  28  29
3:       30  31  32  33  34  35  36  37  38  39
4:       40  41  42  43  44  45  46  47  48  49
5:       50  51  52  53  54  55  56  57  58  59
6:       60  61  62  63
```

Command Mode: Global Mode

Usage Guide: Egress remark mapping table is a global table, it is used to distinguish QoS attributs for modifying packets with different colors.

Example: Set yellow packet's dscp of 0 to 3.

Switch(config)#mls qos map dscp-dscp yellow 0 to 3

7.16.3 service-policy output

Command: service-policy output <*policy-map-name*>

no service-policy output {<*policy-map-name*>}

Function: Applies a policy map to the egress of the port; no command deletes the specified policy map applied to the port or deletes all the policy maps applied on the egress direction of the port .

Parameters: output <*policy-map-name*> applies the specified policy map to the egress of the port.

no command will delete all the policy maps on the egress direction if there is not the specified policy map name.

Default: No policy map is bound to port.

Command mode: Port Mode.

Usage Guide: Only a policy map can be applied to each direction of each port. Policy may not be bound to the port if it uses the rule or action which is not supported by EFP.

Example: Bind policy-map p1 to egress Ethernet 1/0/1.

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#service-policy output p1

7.16.4 service-policy output vlan

Command: service-policy output <*policy-map-name*> vlan <*vlan-list*>

no service-policy output {<*policy-map-name*>} vlan <*vlan-list*>

Function: Applies a policy map to the VLAN interface; no command deletes the specified policy map applied to the VLAN interface or deletes all the policy maps applied in the egress direction of the vlan interface .

Parameters: output <*policy-map-name*> applies the specified policy map to the egress of VLAN interface.

no command will delete all the policy maps in the egress direction of vlan interface if there is not the specified policy map name.

Default: No policy map is bound to VLAN interface.

Command mode: Global Mode.

Usage Guide: Only a policy map can be applied to each direction of each VLAN. Policy may not be bound if it uses the rule or action which is not supported by EFP.

Example: Bind policy p1 to egress vlan1.

Switch(config)#service-policy output p1 vlan 1

7.16.5 set

Command: set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*> | cos <*new-cos*> | c-vid <*new-c-vid*> | s-vid <*new-s-vid*> | s-tpid <*new-s-tpid*>}

no set {ip dscp | ip precedence | cos | c-vid | s-vid | s-tpid}

Function: Assign a new DSCP, IP Precedence for the classified traffic; no command deletes the new value.

Parameter: ip dscp <*new-dscp*> new DSCP value of IPv4 and IPv6 packets.

ip precedence <*new-precedence*> new IPv4 Precedence, only one can be selected for IPv4 Precedence and IP DSCP.

cos <*new cos*> new CoS value.

c-vid <*new-c-vid*> new c-vid value.

s-vid <*new-s-vid*> new s-vid value.

s-tpid <*new-s-tpid*> new s-tpid value.

Default: Do not assign a new value.

Command Mode: Policy Class-map Mode
Usage Guide: Only the classified traffic matching the standard will be assigned the new values.
Example: Set IP Precedence of the packets which satisfy c1 class rule as 3.
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 3
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit

7.16.6 show mls qos egress green remark

Command: show mls qos egress green remark
Function**:** Show whether Egress remarking mapping takes effect for green packets.
Parameter: None.
Default: None.
Command Mode: Admin and configuration mode
Usage Guide: When show mapping relation between Egress remarking table and green packets, it will show whether map green.
Example: Show whether Egress remarking mapping takes effect for green packets.
Switch(config)#show mls qos egress green remark
Green remarking: Disable.

7.16.7 show mls qos maps

Command: show mls qos maps (cos-cos | cos-dscp | dscp-cos | dscp-dscp) <color>
Function: Show Egress remarking mapping.
Parameters: cos-cos：Set mapping from cos to cos for Egress remark cos table
cos-dscp：Set mapping from cos to dscp for Egress remark cos table
dscp-cos：Set mapping from dscp to cos for Egress remark dscp table
dscp-dscp：Set mapping from dscp to dscp for Egress remark dscp table
<color>：Packet's colors, including green、yellow、red
Default: None.
Command Mode: Admin and configuration mode
Usage Guide: Show mapping of Egress remarking table.
Example: Show mapping between cos-cos table and green packets.
Switch(config)#show mls qos maps cos-cos green
COS-TO-COS-GREEN map:
COS: 0 1 2 3 4 5 6 7

COS: 0 1 2 3 4 5 6 7

Green remarking: Disable.

7.17 Flexible QinQ

7.17.1 Add

Command: add s-vid <new-vid>

no add s-vid

Function: Add a specified external tag or inner tag for the packet which match the class map, no command cancels the operation.

Parameters: s-vid <new-vid> specifies VID of an external VLAN Tag.

Default: Do not add the tag.

Command **Mode:** Policy class-map configuration mode

Usage Guide: Add the external tag for **the** packet which match the class map after this command is configured.

Example: Add an external VLAN Tag with VID of 2 for the packet which satisfy c1 class rule.

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#add s-vid 2

7.17.2 delete

This command is not supported by the switch.

7.17.3 Match

Command: match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| ipv6 access-group <*acl-index-or-name*>| ipv6 dscp <*dscp-list*> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <*cos-list*>}

no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos}

Function: Configure the match standard of the class map; the no command deletes the specified match standard.

Parameter: access-group <acl-index-or-name> match the specified IP ACL or MAC ACL, the parameters are the number or name of ACL

ip dscp <dscp-list> and ipv6 dscp <dscp-list> match the specified DSCP value, the parameter is **a**

list of DSCP consisting of maximum 8 DSCP values, the ranging is 0 to 63

ip precedence <*ip-precedence-list*> match the specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0 to 7

ipv6 access-group <*acl-index-or-name*> match **the specified IPv6 *ACL,*** the parameter is the number or name of IPv6 ACL

ipv6 flowlabel <flowlabel-list> match the specified IPv6 flow label, the parameter is IPv6 flow label value, the ranging is 0 to 1048575

vlan **<vlan-list> *match the*** specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the ranging is 1 to 4094

<cost-list> match the specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS values, the ranging is 0 to 7

Default**: There is *no*** match standard.

Command Mode: Class-map Mode

Usage Guide: Only one match standard can be configured in a class map. When configuring the ACL match, permit rule is the match option, it will apply Policy Map action. Deny rule is the excluding option, it does not apply Policy Map action. If it has been configured other match rule, the operation is failure, but configuring the same match rule will cover the previous.

Example: Create a class-map named c1, and configure the class rule of the class-map to match packets with IP Precedence of 0.

Switch(config)#class-map c1

Switch(config-classmap-c1)#match ip precedence 0

Switch(config-classmap-c1)#exit

7.17.4 service-policy

Command: service-policy <*policy-map-name*> in

no service-policy <*policy-map-name*> in

Function: Bind the specified policy of flexible QinQ to the ingress of the port, the no command cancels the binding.

Parameters: service-policy <*policy-map-name*>: The specified policy-map name of flexible QinQ.

Default: No policy map is bound to port.

Command mode: Port Mode.

Usage Guide: Only one policy map can be bound to each port, the function takes effect after the policy map is bound to a port.

Example: Apply policy-map p1 to Ethernet port 1/0/1 for flexible QinQ.

Switch(Config-If-Ethernet1/0/1)#service-policy p1 in

7.17.5 set

Command: set s-vid <new-vid>

no set s-vid

Function: Assign the new cos and vid value to the packets which match the class map, no command cancels the operation.

Parameters: s-vid <new-vid> specifies VID of an external VLAN Tag

Default: Do not assign the value.

Command Mode: Policy class-map configuration mode

Usage Guide: Only assign the new value again for the classified flow that correspond the match standard.

Example: Set an external VLAN Tag' VID as 3 for the packet which satisfy c2 class **rule.**

Switch(config)#policy-map **p1**

Switch(Config-PolicyMap-p1)#class c2

Switch(Config-PolicyMap-p1-Class-c2)#set s-vid 3

Switch(Config-PolicyMap-p1-Class-c2)#exit

Chapter 8 Commands for Reliability

8.1 MSTP

8.1.1 MSTP

8.1.1.1 abort

Command: abort

Function: Abort the current MSTP region configuration, quit MSTP region mode and return to global mode.

Command mode: MSTP Region Mode.

Usage Guide: This command is to quit MSTP region mode without saving the current configuration. The previous MSTP region configuration is valid.

Example: Quit MSTP region mode without saving the current configuration.

Switch(Config-Mstp-Region)#abort

Switch(config)#

8.1.1.2 exit

Command: exit

Function: Save current MSTP region configuration, quit MSTP region mode and return to global mode.

Command mode: MSTP Region Mode

Usage Guide: This command is to quit MSTP region mode with saving the current configuration.

Example: Quit MSTP region mode with saving the current configuration.

Switch(Config-Mstp-Region)#exit

Switch(config)#

8.1.1.3 instance vlan

Command: instance *<instance-id>* vlan *<vlan-list>*

no instance *<instance-id>* [vlan *<vlan-list>*]

Function: In MSTP region mode, create the instance and set the mappings between VLANs and instances; the command "**no instance *<instance-id>* [vlan *<vlan-list>*]**" removes the specified instance and the specified mappings between the VLANs and instances.

Parameter: Normally, ***<instance-id>*** sets the instance number. The valid range is from 0 to 64; in the command "**no instance *<instance-id>* [vlan *<vlan-list>*]**", ***<instance-id>*** sets the instance number. The valid number is from 0 to 64. ***<vlan-list>*** sets consecutive or non-consecutive VLAN

numbers. "-" refers to consecutive numbers, and ";" refers to non-consecutive numbers.

Command mode: MSTP Region Mode

Default: Before creating any Instances, there is only the instance 0, and VLAN 1~4094 all belong to the instance 0.

Usage Guide: This command sets the mappings between VLANs and instances. Only if all the mapping relationships and other attributes are same, the switches are considered in the same MSTP region. Before setting any instances, all the VLANs belong to the instance 0. MSTP can support maximum 64 MSTIs (except for CISTs). CIST can be treated as MSTI 0. All the other instances are considered as instance 1 to 64.

Example: Map VLAN1-10 and VLAN 100-110 to Instance 1.

Switch(config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110

8.1.1.4 name

Command: name *<name>*

no name

Function: In MSTP region mode, set MSTP region name; the "**no name**" command restores the default setting.

Parameter: ***<name>*** is the MSTP region name. The length of the name should be less than 32 characters.

Command mode: MSTP Region Mode

Default: Default MSTP region name is the MAC address of this bridge.

Usage Guide: This command is to set MSTP region name. The bridges with same MSTP region name and same other attributes are considered in the same MSTP region.

Example: Set MSTP region name to mstp-test.

Switch(config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#name mstp-test

8.1.1.5 no

Command: no <*instance-id*> | <*name*> | <*revision-level*>

Function: Cancel one command or set it as initial value.

Parameter: ***<instance-id>*** instance number, ***<name>*** MSTP region name, ***<revision-level>*** is account the modify value of MST configuration caption.

Command mode: MSTP Region Mode

Default: The default revision level is 0.

Usage Guide: This command deletes the specified instance and MSTP region name, restore the default of modify value is 0.

Example: Delete instance 1.

Switch(Config-Mstp-Region)#no instance 1

8.1.1.6 revision-level

Command: revision-level *<level>*

no revision-level

Function: In MSTP region mode, this command is to set revision level for MSTP configuration; the command "**no revision-level**" restores the default setting to 0.

Parameter: ***<level>*** is revision level. The valid range is from 0 to 65535.

Command mode: MSTP Region Mode

Default: The default revision level is 0.

Usage Guide: This command is to set revision level for MSTP configuration. The bridges with same MSTP revision level and same other attributes are considered in the same MSTP region.

Example: Set revision level to 2000.

Switch(config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)# revision-level 2000

8.1.1.7 spanning-tree

Command: spanning-tree

no spanning-tree

Function: Enable MSTP in global mode and in Port Mode; The command "**no spanning-tree**" is to disable MSTP.

Command mode: Global Mode and Port Mode

Default: MSTP is not enabled by default.

Usage Guide: If the MSTP is enabled in global mode, the MSTP is enabled in all the ports except for the ports which are set to disable the MSTP explicitly.

Example: Enable the MSTP in global mode, and disable the MSTP in the interface1/0/2.

Switch(config)#spanning-tree

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#no spanning-tree

8.1.1.8 spanning-tree cost

Command: spanning-tree cost *<cost>*

no spanning-tree cost

Function: Sets path cost of the current port; the command "**no spanning-tree cost**" restores the default setting.

Parameter: ***<cost>*** sets path cost. The valid range is from 1 to 200,000,000.

Command mode: Port Mode

Default: By default, the port cost is relevant to the port bandwidth.

Port Type	Default Path Cost	Suggested Range
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000

1Gbps	20000	20000~200000
10Gbps	2000	2000~20000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N
10Gbps	N	2000/N

Usage Guide: By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of port and the designated port of the instance.
Example: On the port1/0/2, set the port cost is 3000000.
Switch(Config-If-Ethernet1/0/2)#spanning-tree cost 3000000

8.1.1.9 spanning-tree cost-format

This command is not supported by the switch.

8.1.1.10 spanning-tree digest-snooping

Command: spanning-tree digest-snooping
no spanning-tree digest-snooping
Function: Configure the port to use the authentication string of partner port; the command "**no spanning-tree digest-snooping**" restores to use the port generated authentication string.
Parameter: None
Command mode: Port Mode
Default: Don't use the authentication string of partner port.
Usage Guide: According to MSTP protocol, the region authentication string is generated by MD5 algorithm with public authentication key, intstance ID, VLAN ID. Some manufactory don't use the public authentication key, this causes the incompatibility. After the command is executed the port can use the authentication string of partner port, realize compatibility with these manufactories equipment.
Note: Because the authentication string is related to instance ID and VLAN ID, the command may cause recognizing the equipment that with different instance and VLAN relation as in the same region. Before the command is executed, make sure that instance and VLAN relation is accord for all the equipment. If there are more than one equipment connected, all the connected ports should execute this command.
Example: Configure the authentication string of partner port.
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree digest-snooping
Switch(Config-If-Ethernet1/0/2)#

8.1.1.11 spanning-tree format

Command: spanning-tree format {standard | privacy | auto}

no spanning-tree format

Function: Configure the format of the port packet so to be interactive with products of other companies. The no command restores the default format.

Parameter: standard: The packet format provided by IEEE

privacy: Privacy packet format, which is compatible with CISCO equipments.

auto: Auto identified packet format, which is determined by checking the format of the received packets.

Command Mode: Port Mode

Default: Auto Packet Format.

Usage Guide: As the CISCO has adopted the packet format different with the one provided by IEEE, while many companies also adopted the CISCO format to be CISCO compatible, we have to provide support to both formats. The standard format is originally the one provided by IEEE, and the privacy packet format is CISCO compatible. In case we are not sure about which the packet format is on partner, the AUTO configuration will be preferred so to identify the format by the packets they sent. The AUTO packet format is set by default in the concern of better compatibility with previous products and the leading companies. The packet format will be privacy format before receiving the partner packet when configured to AUTO.

When the format is not AUTO and the received packet format from the partner does not match the configured format, we set the state of the port which receives the unmatched packet to DISCARDING to prevent both sides consider themselves the root which leads to circuits.

When the AUTO format is set, and over one equipment which is not compatible with each other are connected on the port (e.g. a equipment running through a HUB or Transparent Transmission BPDU is connected with several equipments running MSTP), the format alter counts will be recorded and the port will be disabled at certain count threshold. The port can only be re-enabled by the administrator.

Example: Configure port message format as the message format of IEEE. Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree format standard

Switch(Config-If-Ethernet1/0/2)#

8.1.1.12 spanning-tree forward-time

Command: spanning-tree forward-time *<time>*

no spanning-tree forward-time

Function: Set the switch forward delay time; the command "**no spanning-tree forward-time**" restores the default setting.

Parameter: *<time>* is forward delay time in seconds. The valid range is from 4 to 30.

Command mode: Global Mode

Default: The forward delay time is 15 seconds by default.

Usage Guide: When the network topology changes, the status of the port is changed from blocking to forwarding. This delay is called the forward delay. The forward delay is co working with hello time and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example: In global mode, set MSTP forward delay time to 20 seconds.

Switch(config)#spanning-tree forward-time 20

8.1.1.13 spanning-tree hello-time

Command: spanning-tree hello-time *<time>*

no spanning-tree hello-time

Function: Set switch Hello time; The command "**no spanning-tree hello-time**" restores the default setting.

Parameter: *<time>* is Hello time in seconds. The valid range is from 1 to 10.

Command mode: Global Mode

Default: Hello Time is 2 seconds by default.

Usage Guide: Hello time is the interval that the switch sends BPDUs. Hello time is co working with forward delay and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example: Set MSTP hello time to 5 seconds in global mode.

Switch(config)#spanning-tree hello-time 5

8.1.1.14 spanning-tree link-type p2p

Command: spanning-tree link-type p2p {auto | force-true | force-false}

no spanning-tree link-type

Function: Set the link type of the current port; the command "**no spanning-tree link-type**" restores link type to auto-negotiation.

Parameter: auto sets auto-negotiation, **force-true** forces the link as point-to-point type, **force-false** forces the link as non point-to-point type.

Command mode: Port Mode

Default: The link type is auto by default; The MSTP detects the link type automatically.

Usage Guide: When the port is full-duplex, MSTP sets the port link type as point-to-point; When the port is half-duplex, MSTP sets the port link type as shared.

Example: Force the port 1/0/7-8 as point-to-point type.

Switch(config)#interface ethernet 1/0/7-8

Switch(Config-Port-Range)#spanning-tree link-type p2p force-true

8.1.1.15 spanning-tree maxage

Command: spanning-tree maxage *<time>*

no spanning-tree maxage

Function: Set the max aging time for BPDU; the command "**no spanning-tree maxage**" restores the default setting.

Parameter: *<time>* is max aging time in seconds. The valid range is from 6 to 40.

Command mode: Global Mode

Default: The max age is 20 seconds by default.

Usage Guide: The lifetime of BPDU is called max age time. The max age is co working with hello time and forward delay. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example: In global mode, set max age time to 25 seconds.

Switch(config)#spanning-tree maxage 25

8.1.1.16 spanning-tree max-hop

Command: spanning-tree max-hop *<hop-count>*

no spanning-tree max-hop

Function: Set maximum hops of BPDU in the MSTP region; the command "**no spanning-tree max-hop**" restores the default setting.

Parameter: *<hop-count>* sets maximum hops. The valid range is from 1 to 40.

Command mode: Global Mode

Default: The max hop is 20 by default.

Usage Guide: The MSTP uses max-age to count BPDU lifetime. In addition, MSTP also uses max-hop to count BPDU lifetime. The max-hop is degressive in the network. The BPDU has the max value when it initiates from MSTI root bridge. Once the BPDU is received, the value of the max-hop is reduced by 1. When a port receives the BPDU with max-hop as 0, it drops this BPDU and sets itself as designated port to send the BPDU.

Example: Set max hop to 32.

Switch(config)#spanning-tree max-hop 32

8.1.1.17 spanning-tree mcheck

Command: spanning-tree mcheck

Function: Force the port to run in the MSTP mode.

Command mode: Port Mode

Default: The port is in the MSTP mode by default.

Usage Guide: If a network which is attached to the current port is running IEEE 802.1D STP, the port converts itself to run in STP mode. The command is used to force the port to run in the MSTP mode. But once the port receives STP messages, it changes to work in the STP mode again.

This command can only be used when the switch is running in IEEE802.1s MSTP mode. If the switch is running in IEEE802.1D STP mode, this command is invalid.

Example: Force the port 1/0/2 to run in the MSTP mode.
Switch(Config-If-Ethernet1/0/2)#spanning-tree mcheck

8.1.1.18 spanning-tree mode

Command: spanning-tree mode {mstp | stp | rstp}
no spanning-tree mode
Function: Set the spanning-tree mode in the switch; the command "**no spanning-tree mode**" restores the default setting.
Parameter: mstp sets the switch in IEEE802.1s MSTP mode; **stp** sets the switch in IEEE802.1D STP mode; **rstp** sets the switch in IEEE802.1D RSTP mode.
Command mode: Global Mode
Default: The switch is in the MSTP mode by default.
Usage Guide: When the switch is in IEEE802.1D STP mode, it only sends standard IEEE802.1D BPDU and TCN BPDU. It drops any MSTP BPDUs.
Example: Set the switch in the STP mode.
Switch(config)#spanning-tree mode stp

8.1.1.19 spanning-tree mst configuration

Command: spanning-tree mst configuration
no spanning-tree mst configuration
Function: Enter the MSTP mode. Under the MSTP mode, the MSTP attributes can be set. The command "**no spanning-tree mst configuration**" restores the attributes of the MSTP to their default values.
Command mode: Global Mode
Default: The default values of the attributes of the MSTP region are listed as below:

Attribute of MSTP	Default Value
Instance	There is only the instance 0. All the VLANs (1~4094) are mapped to the instance 0.
Name	MAC address of the bridge
Revision	0

Usage Guide: Whether the switch is in the MSTP region mode or not, users can enter the MSTP mode, configure the attributes, and save the configuration. When the switch is running in the MSTP mode, the system will generate the MST configuration identifier according to the MSTP configuration. Only if the switches with the same MST configuration identifier are considered as in the same MSTP region.
Example: Enter MSTP region mode.
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#

8.1.1.20 spanning-tree mst cost

Command: spanning-tree mst *<instance-id> cost <cost>*

no spanning-tree mst <instance-id> cost

Function: Sets path cost of the current port in the specified instance; the command 'no **spanning-tree mst <instance-id> cost'** restores the default setting.

Parameter: *<instance-id>* sets the instance ID. The valid range is 0-64. <cost> sets ***path cost***, different cost formats have different ranges. For the default dot1t **mode** the valid range is 1-200,000,000, and for dot1d is 1-65535.

Command mode: Port Mode

Default: By default, the port cost is relevant to the port bandwidth.

Port Type	Default Path Cost	Suggested Range
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000
10Gbps	2000	2000~20000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N
10Gbps	N	2000/N

Port Speed	Port Type	Port Cost	
		802.1D-2008	802.1T
0		65535	200,000,000
10Mbps	Half- duplex	100	2,000,000
	Full- duplex	99	1,999,999
	aggregation link with 2 ports	95	1,000,000
		95	666,666
	aggregation link with 3 ports	95	500,000
	aggregation link with 4 ports		
100Mbps	Half- duplex	19	200,000
	Full- duplex	18	199,999
	aggregation link with 2 ports	15	100,000
		15	66,666
	aggregation link with 3 ports	15	50,000
	aggregation link with 4 ports		
1000Mbps	Full- duplex	4	20,000

	aggregation link with 2 ports aggregation link with 3 ports aggregation link with 4 ports	3 3 3	10,000 6,666 5,000
10Gbps	Full- duplex aggregation link with 2 ports aggregation link with 3 ports aggregation link with 4 ports	2 1 1 1	2,000 1,000 666 500

Usage Guide: By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of root port and the designated port of the instance.

Example: On the port1/0/2, set the MSTP port cost in the instance 2 to 3000000.

Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 2 cost 3000000

8.1.1.21 spanning-tree cost-format

Command: spanning-tree cost-format {dot1d | dot1t}

Function: In global mode, users can select path-cost format with dot1d or dot1t, the default format is dot1t.

Command Mode: Global mode.

Default: count path-cost with dot1t format.

Usage Guide: There are two formats about cost value: they are dot1d marked on IEEE802.1d-2008 and dot1t marked on IEEE802.1t, but path-cost ranges of them are different, dot1d range from 1 to 65535, and dot1t range from 1 to 200,000,000.

If users already configured the cost value of link with **spanning-tree cost** command manually, changing path-cost format with **cost-format** command is successful after the previous configuration is cleared only.

Example: Set the cost format in global mode

Switch(config)#spanning-tree cost-format dot1d

8.1.1.22 spanning-tree mst loopguard

Command: spanning-tree [mst <instance-id>] loopguard

no spanning-tree [mst <instance-id>] loopguard

Function: Enable the loopguard function for specified instance, the no command disables this function.

Parameter: ***<instance-id>***: MSTP instance ID.

Command mode: Port Mode.

Default: Disable loopguard function.

Usage Guide: The command can avoid root port or alternate port to be changed as designated port due to invalid unilateralism link. When the receiving timer is time, the configured port with loopguard is set as block state.

Example: Configure port 1/0/2 as loopguard mode for instance 0.

Switch(Config)#interface ethernet 1/0/2

Switch(Config-Ethernet-1/0/2)#spanning-tree mst 0 loopguard

Switch(Config-Ethernet-1/0/2)#

8.1.1.23 spanning-tree mst port-priority

Command: spanning-tree mst *<instance-id>* port-priority *<port-priority>*

no spanning-tree mst *<instance-id>* port-priority

Function: Set the current port priority for the specified instance; the command "**no spanning-tree mst *<instance-id>* port-priority**" restores the default setting.

Parameter: ***<instance-id>*** sets the instance ID. The valid range is from 0 to 64; ***<port-priority>*** sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32…240.

Command mode: Port Mode

Default: The default port priority is 128.

Usage Guide: By setting the port priority, users can control the port ID of the instance in order to control the root port and designated port of the instance. The lower the value of the port priority is, the higher the priority is.

Example: Set the port priority as 32 on the port 1/0/2 for the instance 1.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 1 port-priority 32

8.1.1.24 spanning-tree mst priority

Command: spanning-tree mst *<instance-id>* priority *<bridge-priority>*

no spanning-tree mst *<instance-id>* priority

Function: Set the bridge priority for the specified instance; the command "**no spanning-tree mst *<instance-id>* priority**" restores the default setting.

Parameter: ***<instance-id>*** sets instance ID. The valid range is from 0 to 64; ***<bridge-priority>*** sets the switch priority. The valid range is from 0 to 61440. The value should be the multiples of 4096, such as 0, 4096, 8192…61440.

Command mode: Global Mode

Default: The default bridge priority is 32768.

Usage Guide: By setting the bridge priority, users can change the bridge ID for the specified instance. And the bridge ID can influence the elections of root bridge and designated port for the specified instance.

Example: Set the priority for Instance 2 to 4096.
Switch(config)#spanning-tree mst 2 priority 4096

8.1.1.25 spanning-tree mst rootguard

Command: spanning-tree [mst *<instance-id>*] rootguard
no spanning-tree [mst *<instance-id>*] rootguard
Function: Enable the rootguard function for specified instance, the rootguard function forbid the port to be MSTP root port. "**no spanning-tree mst *<instance-id>* rootguard**" disable the rootguard function.
Parameter: *<instance-id>*: MSTP instance ID.
Command mode: Port Mode.
Default: Disable rootguard function.
Usage Guide: The command is used in Port Mode, if the port is configured to be a rootguand port, it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent (blocked).If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is added to the network.
Example: Enable rootguard function for port 1/0/2 in instance 0.
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 0 rootguard
Switch(Config-If-Ethernet1/0/2)#

8.1.1.26 spanning-tree portfast

Command: spanning-tree portfast [bpdufilter | bpduguard] [recovery <30-3600>]
no spanning-tree portfast
Function: Set the current port as boundary port, and BPDU filter、BPDU guard as specified mode or default mode; the command "**no spanning-tree portfast**" sets the current port as non-boundary port.
Parameter: bpdufilter: configure the border port mode as BPDU filter
bpduguard: configure the border port mode as BPDU guard
recovery: configure the border port can be recovered automatically after implement bpduguard violation operation
<30-3600>: the recovery time, do not recover it by default
Command mode: Port Mode
Default: All the ports are non-boundary ports by default when enabling MSTP.
Usage Guide: When a port is set to be a boundary port, the port converts its status from discarding to forwarding without bearing forward delay. Once the boundary port receives the BPDU, the port becomes a non-boundary port.
Example: Configure the border port mode as BPDU guard, the recovery time as 60s.
Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree portfast bpduguard recovery 60
Switch(Config-If-Ethernet1/0/2)#

8.1.1.27 spanning-tree port-priority

Command: spanning-tree port-priority *<port-priority>*

no spanning-tree port-priority

Function: Set the port priority; the command "**no spanning-tree port-priority**" restores the default setting.

Parameter: ***<port-priority>*** sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32, 48…240.

Command mode: Port Mode

Default: The default port priority is 32768.

Usage Guide: By setting the port priority to designated port. The lower the value of the port priority is, the higher the priority is.

Example: Set the port priority as 4096 on the port 1.

Switch(Config-If-Ethernet1/0/1)#spanning-tree port-priority 4096

8.1.1.28 spanning-tree priority

Command: spanning-tree priority *<bridge-priority>*

no spanning-tree priority

Function: Configure the spanning-tree priority; the "**no spanning-tree priority**" command restores the default priority.

Parameter: ***<bridge-priority>*** is the priority of the bridging switch. Its value should be round times of 4096 between 0 and 61440, such as 0, 4096, 8192… 61440.

Command Mode: Global Mode.

Default: Priority is 32768.

Usage Guide: The bridge ID can be altered by changing the priority of the switch. Further, the priority information can also be used for voting of the root bridge and the specified ports. The bridge priority value of the switch is smaller, however the priority is higher.

Example: Configure the priority is 4096.

Switch(config)#spanning-tree priority 4096

8.1.1.29 spanning-tree rootguard

Command: spanning-tree rootguard

no spanning-tree rootguard

Function: Set the port is root port, "**no spanning-tree rootguard**" command sets the port is non-root port.

Parameter: None.

Command mode: Port Mode.

Default: Port is non-root port.

Usage Guide: The command is used in Port Mode, if the port is configured to be a rootguand port, it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent (blocked). If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is added to the network.

Example: Set the port 1 is root port.

Switch(Config-If-Ethernet1/0/1)#spanning-tree rootguard

8.1.1.30 spanning-tree tcflush (Global mode)

Command: spanning-tree tcflush {enable| disable| protect}

no spanning-tree tcflush

Function: Configure the spanning-tree flush mode once the topology changes. “no spanning-tree tcflush” restores to default setting.

Parameter: enable: The spanning-tree flush once the topology changes.

disable: The spanning tree don’t flush when the topology changes.

protect: the spanning-tree flush not more than one time every ten seconds.

Command mode: Global mode

Default: Enable

Usage Guide: According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command

Note: For the complicated network, especially need to switch from one spanning tree branch to another rapidly, the disable mode is not recommended.

Example: Configure the spanning-tree flush mode once the topology changes is not flush to TC.

Switch(config)#spanning-tree tcflush disable

Switch(config)#

8.1.1.31 spanning-tree tcflush (Port mode)

Command: spanning-tree tcflush {enable| disable| protect}

no spanning-tree tcflush

Function: Configure the spanning-tree flush mode for port once the topology changes. “no spanning-tree tcflush” restores to default setting.

Parameter: enable: The spanning-tree flush once the topology changes.

disable: The spanning tree don’t flush when the topology changes.

protect: the spanning-tree flush not more than one time every ten seconds.

Command mode: Port Mode

Default: Global configuration

Usage Guide: According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command

Note: For the complicated network, especially need to switch from one spanning tree branch to another rapidly, the disable mode is not recommended.

Example: Configure the spanning-tree flush mode once the topology change is not flush to TC.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree tcflush disable

Switch(Config-If-Ethernet1/0/2)#

8.1.1.32 spanning-tree transmit-hold-count

Command: spanning-tree transmit-hold-count <*tx-hold-count-value*>

no spanning-tree transmit-hold-count

Function: Set the max transmit-hold-count of port.

Parameter: tx-hold-count-value: ranging from 1 to 255, the default value is 10.

Command mode: Global Mode

Default: 10.

Usage Guide: Set the max number for sending BPDU within the Hello Time interval to control BPDU flow. The variable is used to whole MST bridge.

Example: Set the max transmit-hold-count as 20.

Switch(config)#spanning-tree transmit-hold-count 20

8.1.2 Monitor and Debug

8.1.2.1 debug spanning-tree

Command: debug spanning-tree

no debug spanning-tree

Function: Enable the MSTP debugging information; the command "**no debug spanning-tree**" disables the MSTP debugging information.

Command mode: Admin Mode

Usage Guide: This command is the general switch for all the MSTP debugging. Users should enable the detailed debugging information, and then they can use this command to display the relevant debugging information. In general, this command is used by skilled technicians.

Example: Enable to receive the debugging information of BPDU messages on the port1/0/1.

Switch#debug spanning-tree

Switch#debug spanning-tree bpdu rx interface e1/0/1

8.1.2.2 show mst-pending

Command: show mst-pending

Function: In the MSTP region mode, display the configuration of the current MSTP region.

Command mode: Admin Mode

Usage Guide: In the MSTP region mode, display the configuration of the current MSTP region such as MSTP name, revision, VLAN and instance mapping.

Note: Before quitting the MSTP region mode, the displayed parameters may not be effective.

Example: Display the configuration of the current MSTP region.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#show mst-pending

Name          test
Revision      0
Instance      Vlans Mapped
---------------------------------
00              1-29, 31-39, 41-4093
03              30
04              40
05              4094
---------------------------------
Switch(Config-Mstp-Region)#
```

8.1.2.3 show spanning-tree

Command: show spanning-tree [mst [*<instance-id>*]] [interface *<interface-list>*] [detail]

Function: Display the MSTP Information.

Parameter: ***<interface-list>*** sets interface list; ***<instance-id>*** sets the instance ID. The valid range is from 0 to 64; **detail** sets the detailed spanning-tree information.

Command mode: Admin and Configuration Mode

Usage Guide: This command can display the MSTP information of the instances in the current bridge.

Example: Display the bridge MSTP.

```
Switch#sh spanning-tree

                        -- MSTP Bridge Config Info --

Standard        :   IEEE 802.1s
Bridge MAC      :   00: 03: 0f: 01: 0e: 30
Bridge Times :   Max Age 20, Hello Time 2, Forward Delay 15
Force Version:   3

############################## Instance 0 ##############################
Self Bridge Id     : 32768 -    00: 03: 0f: 01: 0e: 30
```

```
Root Id                 : 16384.00: 03: 0f: 01: 0f: 52
Ext.RootPathCost : 200000
Region Root Id      : this switch
Int.RootPathCost : 0
Root Port ID         : 128.1
Current port list in Instance 0:
Ethernet1/0/1 Ethernet1/0/2 (Total 2)

  PortName          ID          ExtRPC     IntRPC    State Role        DsgBridge        DsgPort
-------------- ------- --------- --------- --- ---- ------------------ -------
  Ethernet1/0/1    128.001              0            0 FWD ROOT 16384.00030f010f52 128.007
  Ethernet1/0/2    128.002              0             0 BLK ALTR 16384.00030f010f52 128.011

############################## Instance 3 ##############################
Self Bridge Id      : 0.00: 03: 0f: 01: 0e: 30
Region Root Id      : this switch
Int.RootPathCost : 0
Root Port ID        : 0
Current port list in Instance 3:
Ethernet1/0/1 Ethernet1/0/2 (Total 2)

    PortName          ID       IntRPC      State Role        DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
  Ethernet1/0/1    128.001              0 FWD MSTR         0.00030f010e30 128.001
  Ethernet1/0/2    128.002              0 BLK ALTR         0.00030f010e30 128.002

############################## Instance 4 ##############################
Self Bridge Id      : 32768.00: 03: 0f: 01: 0e: 30
Region Root Id      : this switch
Int.RootPathCost : 0
Root Port ID        : 0
Current port list in Instance 4:
Ethernet1/0/1 Ethernet1/0/2 (Total 2)

    PortName          ID       IntRPC      State Role        DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
  Ethernet1/0/1 128.001              0 FWD MSTR 32768.00030f010e30 128.001
  Ethernet1/0/2 128.002              0 BLK ALTR 32768.00030f010e30 128.002
```

Displayed Information	Description
Bridge Information	
Standard	STP version
Bridge MAC	Bridge MAC address

Bridge Times	Max Age, Hello Time and Forward Delay of the bridge
Force Version	Version of STP
Instance Information	
Self Bridge Id	The priority and the MAC address of the current bridge for the current instance
Root Id	The priority and the MAC address of the root bridge for the current instance
Ext.RootPathCost	Total cost from the current bridge to the root of the entire network
Int.RootPathCost	Cost from the current bridge to the region root of the current instance
Root Port ID	Root port of the current instance on the current bridge
MSTP Port List Of The Current Instance	
PortName	Port name
ID	Port priority and port index
ExtRPC	Port cost to the root of the entire network
IntRPC	Cost from the current port to the region root of the current instance
State	Port status of the current instance
Role	Port role of the current instance
DsgBridge	Upward designated bridge of the current port in the current instance
DsgPort	Upward designated port of the current port in the current instance

8.1.2.4 show spanning-tree mst config

Command: show spanning-tree mst config

Function: Display the configuration of the MSTP in the Admin mode.

Command mode: Admin Mode

Usage Guide: In the Admin mode, this command can show the parameters of the MSTP configuration such as MSTP name, revision, VLAN and instance mapping.

Example: Display the configuration of the MSTP on the switch.

Switch#show spanning-tree mst config

Name test
Revision 0
Instance Vlans Mapped
---
00 1-29, 31-39, 41-4094
03 30
04 40

8.1.3 MSTP Spanning-tree Process

8.1.3.1 spanning-tree process

Command: spanning-tree process <process-id>
no spanning-tree **process <process-id>**
Function: Create the new mstp process.
Parameters: process-id: the range is 1-31.
Command Mode: Global Mode.
Default: None.
Usage Guide: Create the new mstp process. Multiple mstp processes can be configured on one device and each process is standalone. The process 0 exists only as default.
Example: Create the new mstp process 1.
Switch(config)#spanning-tree process 1

8.1.3.2 spanning-tree tc-notify process0

Command: spanning-tree tc-notify process0
no spanning-tree tc-notify **process0**
Function: The process N notifies tc to the instance in mstp process 0.
Parameters: None.
Command Mode: mstp process mode.
Default: None.
Usage Guide: When there is a change in mstp process N, the device will receive the tc packet, at the same time, the process N will notify tc to the instance in mstp process 0 on the shared link. It makes the process 0 refresh the table entry for ensuring the traffic not to break off.
Example: Configure to notify TC of process 1 to process 0.
Switch(Config-Mstp-Process-1)#spanning-tree tc-notify process0

8.1.3.3 spanning-tree binding-process

This command is not supported by the switch.

8.1.3.4 spanning-tree binding-process link-share

This command is not supported by the switch.

8.2 VRRP

8.2.1 advertisement-interval

Commands: advertisement-interval <*adver_interval*>

no advertisement-interval

Function: Sets the vrrp timer values; the "**no advertisement-interval**" command restores the default setting.

Parameters: <*adver_interva*> is the interval for sending VRRP packets in seconds, ranging from 1 to 10.

Default: The default **<*adver_interva*>** is 1 second.

Command mode: VRRP protocol configuration mode

Usage Guide: The Master in a VRRP Standby cluster will send VRRP packets to member routers (or L3 Ethernet switch) to announce its properness at a specific interval; this interval is referred to as *adver_interval*. If a Backup does not receive the VRRP packets sent by the Master after a certain period (specified by *master_down_interval*), then it assume the Master is no longer operating properly, therefore turns its status to Master.

The user can use this command to adjust the VRRP packet sending interval of the Master. For members in the same Standby cluster, this property should be set to a same value. To Backup, the value of *master_down_interval* is three times that of adver_interval. Extraordinary large traffic or timer setting differences between routers (or L3 Ethernet switches) may result in *master_down_interval* and invoke instant status changes. Such situations can be avoided through extending *adver_interval* interval and setting longer preemptive delay time.

Example: Configuring vrrp Timer value to 3

Switch(Config-Router-Vrrp)# advertisement-interval 3

8.2.2 circuit-failover

Commands: circuit-failover {IFNAME | Vlan <ID>} <value_reduced>

no circuit-failover

Function: Configures the VRRP monitor interface.

Parameters: < *IFNAME* > is the name for the interface to be monitored.

<*value_reduced*> stands for the amount of priority decreased, the default value is 1~253.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: The interface monitor function is a valuable extension to backup function, which not only enable VRRP to provide failover function on router (or L3 Ethernet switch) fail, but also allow decreasing the priority of a router (or L3 Ethernet switch) to ensure smooth implementation of backup function when status of that network interface is **down**.

When this command is used, if the status of an interface monitored turns from **up** to **down**, then the priority of that very router (or L3 Ethernet switch) in its Standby cluster will decrease, lest Backup cannot changes its status due to lower priority than the Master when the Master fails.

Example: Configuring VRRP monitor interface to vlan 2 and decreasing amount of priority to 10.

Switch(Config-Router-Vrrp)# circuit-failover vlan 2 10

8.2.3 debug vrrp

Commands: debug vrrp [all | event | packet [recv | send]]

no debug vrrp [all | event | packet [recv | send]]

Function: Displays information for VRRP standby cluster status and packet transmission; the "**no debug vrrp**" command disables the debug information.
Default: Debugging information is disabled by default.
Command mode: Admin Mode
Example:
Switch#debug vrrp
2001/01/01 00:50:28 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]
2001/01/01 00:50:30 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]
2001/01/01 00:50:31 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]
2001/01/01 00:50:32 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]
2001/01/01 00:50:33 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]

8.2.4 disable

Commands: disable
Function: Deactivates VRRP
Parameters: N/A.
Default: Not configured by default.
Command mode: VRRP protocol configuration mode
Usage Guide: Deactivates a Virtual Router. VRRP configuration can only be modified when VRRP is deactivated.
Example: Deactivating a Virtual Router numbered as 10.
Switch(config)# router vrrp 10
Switch(Config-Router-Vrrp)#disable

8.2.5 enable

Commands: enable
Function: Activates VRRP.
Parameters: N/A.
Default: Not configured by default.
Command mode: VRRP protocol configuration mode
Usage Guide: Activates the appropriate Virtual Router. Only a router (or L3 Ethernet switch) interface started by this enable command is part of Standby cluster. VRRP virtual IP and interface must be configured first before starting Virtual Router.
Example: Activating the Virtual Router of number 10.
Switch(config)#router vrrp 10
Switch(Config-Router)#enable

8.2.6 interface

Commands: interface {IFNAME | Vlan <*ID*>}

no interface

Function: Configures the VRRP interface.

Parameters: IFNAME: Interface name, for example “VLAN1”.

Vlan <*ID*>: VLAN ID.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: This command adds a layer 3 interface to an existing Standby cluster. The "**no interface**" command removes the L3 interface from the specified Standby cluster.

Example: Configuring the interface as "interface vlan 1".

Switch(config-router)#router vrrp 10

Switch(Config-router)#interface vlan 1

8.2.7 preempt-mode

Commands: preempt-mode {true | false}

Function: Configures the preemptive mode for VRRP.

Parameters: N/A.

Command mode: VRRP protocol configuration mode

Default: Preemptive mode is set by default.

Usage Guide: If a router (or L3 Ethernet switch) requiring high priority needs to preemptively become the active router (or L3 Ethernet switch), the preemptive mode should be enabled.

Example: Setting non-preemptive VRRP mode.

Switch(Config-Router-Vrrp)#preempt-mode false

8.2.8 priority

Commands: priority <*value*>

Function: Configures VRRP priority.

Parameters: < *value*> is the priority value, ranging from 1 to 254.

Default: The priority of all **backup** routers (or L3 Ethernet switch) in a Standby cluster is 100.

Command mode: VRRP protocol configuration mode

Usage Guide: Priority determines the ranking of a router (or L3 Ethernet switch) in a Standby cluster, the higher priority the more likely to become the Master. When a router (or L3 Ethernet switch) is configured as Master dummy IP address, its priority is always 254 and does not allow modification. When 2 or more routers (or L3 Ethernet switch) with the same priority value present in a Standby cluster, the router (or L3 Ethernet switch) with the greatest VLAN interface IP address becomes the Master.

Example: Setting VRRP priority to 150.

Switch(Config-Router-Vrrp)# priority 150

8.2.9 router vrrp

Commands: router vrrp <*vrid*>

no router vrrp <*vrid*>

Function: Creates/Removes the Virtual Router.

Parameters: <*vrid*> is the Virtual Router number ranging from 1 to 255.

Default: Not configured by default.

Command mode: Global Mode

Usage Guide: This command is used to create/remove Virtual Router, which is identified by a unique Virtual Router number. Virtual Router configurations are only available when a Virtual Router is created, 192 Virtual Routers can be configured at best.

Example: Configuring a Virtual Router with number 10.

Switch(config)# router vrrp 10

8.2.10 show vrrp

Commands: show vrrp [<*vrid*>]

Function: Displays status and configuration information for the VRRP standby cluster.

Parameters: < *vrid* > is the Virtual Router number ranging from 1 to 255.

Command mode: Admin and Configuration Mode.

Usage Guide: This command is used to display the Virtual Router configuration and current state. If not specified the Virtual Router number, then display all Virtual Router information.

Example:

Switch# show vrrp

VrId <1>

State is Initialize

Virtual IP is 10.1.20.10 (Not IP owner)

Interface is Vlan1

Priority not configured, Current priority is 254

Advertisement interval is 1 sec

Preempt mode is TRUE

Circuit failover interface Vlan1, Priority Delta 1, Status UP

VrId <10>

State is Initialize

Virtual IP is1.1.1.1 (Not IP owner)

Interface is unset

Priority is unset

Advertisement interval is unset

Preempt mode is TRUE

Switch#

Displayed information	Explanation
State	Status
Virtual IP	Dummy IP address
Interface	Interface Name
Priority	Priority

Advertisement interval	Timer interval
Preempt	Preemptive mode
Circuit failover interface	Interface Monitor information

8.2.11 virtual-ip

Commands: virtual-ip <*A.B.C.D*>

no virtual-ip

Function: Configures the VRRP dummy IP address.

Parameters: <*A.B.C.D*> is the IP address in decimal format.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: This command adds a dummy IP address to an existing Standby cluster. The "**no virtual-ip**" command removes the dummy IP address from the specified Standby cluster. Each Standby cluster can have only one dummy IP. VRRP priority as 255 (not configure), virtual-ip and interface ip should in the same segment.

Special Notice: When updating to the newest version from 5.2.0.0 or an older one, the original VRRP command configuration can't be restored. Please delete the original configuration with "no router vrrp <vrid>", and then reconfigure. Otherwise, problems like suspended tasks may happen.

Example: Setting the backup dummy IP address to 10.1.1.1.

Switch(Config-Router-Vrrp)# virtual-ip 10.1.1.1

8.2.12 vrrp track

Command: vrrp track interface {ethernet IFNAME|IFNAME} priority <priority_value>

no vrrp track interface {ethernet IFNAME|IFNAME}

Function: Configure the status of the VRRP session monitor port.

Parameters: interface {ethernet IFNAME|IFNAME}: port name.

<priority_value>: priority, the range is from 1 to 254.

Command Mode: VRRP Configuration Mode.

Default: Disable.

Usage Guide: This command configures the status of the VRRP session monitor port. When the port status is DOWN, change the local VRRP priority to be the configured value for changing the VRRP session status. For example, when the local VRRP priority is lower than the priority of the opposite, the status of local VRRP should be BACKUP.

Example:

Switch(config)#router vrrp 1

Switch(config-router)#vrrp track interface ethernet 1/0/5 priority 60

8.3 MRPP

8.3.1 control-vlan

Command: control-vlan <*vid*>

no control-vlan

Function: Configure control VLAN ID of MRPP ring; the "**no control-vlan**" command deletes control VLAN ID.

Parameter: ***<vid>*** expresses control VLAN ID, the valid range is from 1 to 4094.

Command Mode: MRPP ring mode

Default: None

Usage Guide: The command specifies Virtual VLAN ID of MRPP ring, currently it can be any value in 1-4094. To avoid confusion, it is recommended that the ID is non-configured VLAN ID, and the same to MRPP ring ID. In configuration of MRPP ring of the same MRPP loop switches, the control VLAN ID must be the same, otherwise the whole MRPP loop may not be able to work normally or form broadcast.

The mrpp enable command must be start before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, the mrpp-ring function is enabled.

Example: Configure control VLAN of mrpp ring 4000 is 4000.

Switch(config)#mrpp ring 4000

Switch(mrpp-ring-4000)#control-vlan 4000

8.3.2 clear mrpp statistics

Command: clear mrpp statistics [<*ring-id*>]

Function: Clear statistic information of MRPP data packet of MRPP ring receiving and transferring.

Parameter: ***<ring-id>*** is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it clears all of MRPP ring statistic information.

Command Mode: Admin Mode.

Default: None.

Usage Guide: None.

Example: Clear statistic information of MRPP ring 4000 of switch.

Switch#clear mrpp statistics 4000

8.3.3 debug mrpp

Command: debug mrpp

no debug mrpp

Function: Open MRPP debug information; "**no description**" command disables MRPP debug information.

Command Mode: Admin Mode
Parameter: None.
Usage Guide: Enable MRPP debug information, and check message process of MRPP protocol and receive data packet process, it is helpful to monitor debug.
Example: Enable debug information of MRPP protocol.
Switch#debug mrpp

8.3.4 enable

Command: enable
no enable
Function: Enable configured MRPP ring, the "**no enable**" command disables this enabled MRPP ring.
Parameter:
Command Mode: MRPP ring mode
Default: Default disable MRPP ring.
Usage Guide: Executing this command, it must enable MRPP protocol, and if other commands have configured, the MRPP ring is enabled.
Example: Configure MRPP ring 4000 of switch to primary node, and enable the MRPP ring.
Switch(config)#mrpp enable
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)# node-mode master
Switch(mrpp-ring-4000)#fail-timer 18
Switch(mrpp-ring-4000)#hello-timer 6
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(config)#in ethernet1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config)#in ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port

8.3.5 errp domain

Command: errp domain <*domain-id*>
no errp domain <*domain-id*>
Function: Create ERRP domain, the no command deletes the configured ERRP domain.
Parameter: <*domain-id*> domain ID of ERRP, the range between 0 and 15.
Command Mode: Global mode
Usage Guide: If domain ID of ERRP needs to be configured, the compatible mode of ERRP should be enabled firstly. When executing this command, it should create a new ERRP domain if there is no ERRP domain. However, the no command is used to delete the corresponding domain ID of ERRP.

Example: Configure domain ID for ERRP globally.
Switch(Config)#errp domain 1

8.3.6 fail-timer

Command: fail-timer *<timer>*
no fail-timer
Function: Configure if the primary node of MRPP ring receive Timer interval of Hello packet or not, the "**no fail-timer**" command restores default timer interval.
Parameter: *<timer>* valid range is from 3 to 300s.
Command Mode: MRPP ring mode
Default: Default configure timer interval 3s.
Usage Guide: If primary node of MRPP ring doesn't receives Hello packet from primary port of primary node on configured fail timer, the whole loop is fail. Transfer node of MRPP doesn't need this timer and configure. To avoid time delay by transfer node forwards Hello packet, the value of fail timer must be more than or equal to 3 times of Hello timer. On time delay loop, it needs to modify the default and increase the value to avoid primary node doesn't receive Hello packet on fail timer due to time delay.
Example: Configure fail timer of MRPP ring 4000 to 10s.
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#fail-timer 10

8.3.7 hello-timer

Command: hello-timer <*timer*>
no hello-timer
Function: Configure timer interval of Hello packet from primary node of MRPP ring, the "**no hello-timer**" command restores timer interval of default.
Parameter: *<timer>* valid range is from 1 to 100s.
Command Mode: MRPP ring mode
Default: Default configuration timer interval is 1s.
Usage Guide: The primary node of MRPP ring continuously sends Hello packet on configured Hello timer interval, if secondary port of primary node can receive this packet in configured period; the whole loop is normal, otherwise fail. Transfer node of MRPP ring doesn't need this timer and configure.
Example: Configure hello-timer of MRPP ring 4000 to 3 seconds.
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#hello-timer 3

8.3.8 mrpp eaps compatible

Command: mrpp eaps compatible

no mrpp eaps compatible

Function: Enable the compatible mode for EAPS, the no command disables the compatible mode.

Parameter: None.

Command Mode: Global mode

Default: Disable the compatible function of EAPS.

Usage Guide: If the compatible function of EAPS needs to be configured, MRPP protocol should be enabled firstly. When executing **no mrpp eaps compatible** command, it should ensure that the switch has enabled MRPP protocol.

Example: Enable the compatible function of EAPS globally.

Switch(Config)#mrpp enable

Switch(Config)#mrpp eaps compatible

8.3.9 mrpp enable

Command: mrpp enable

no mrpp enable

Function: Enable MRPP protocol module, the "**no mrpp enable**" command disables MRPP protocol.

Parameter: None.

Command Mode: Global Mode.

Default: The system doesn't enable MRPP protocol module.

Usage Guide: If it needs to configure MRPP ring, it enables MRPP protocol. Executing "**no mrpp enable**" command, it ensures to disable the switch enabled MRPP ring.

Example: Globally enable MRPP.

Switch(config)#mrpp enable

8.3.10 mrpp errp compatible

Command: mrpp errp compatible

no mrpp errp compatible

Function: Enable the compatible mode for ERRP, the no command disables the compatible mode.

Parameter: None.

Command Mode: Global mode

Default: Disable the compatible function of ERRP.

Usage Guide: If the compatible function of ERRP needs to be configured, MRPP protocol should be enabled firstly. Furthermore, the port with ERRP compatible mode should be configured as hybrid or trunk mode and allow the packets with Control Vlan information.

Example: Enable the compatible function of ERRP globally.

Switch(Config)#mrpp enable

Switch(Config)#mrpp errp compatible

Switch(Config)#mrpp ring 2

Switch(mrpp-ring-2)#control-vlan 4000

Switch(config-if-ethernet1/0/51)#switchport mode hybrid

Switch(config-if-ethernet1/0/51)#switchport hybrid allowed vlan 4000 tag
Switch(config-if-ethernet1/0/52)#switchport mode hybrid
Switch(config-if-ethernet1/0/52)#switchport hybrid allowed vlan 4000 tag

8.3.11 mrpp poll-time

Command: mrpp poll-time <20-2000>
Function: Configure the query interval of MRPP.
Command mode: Global mode.
Usage Guide: Configure the query time to adjust the query interval of MRPP, the default interval is 100ms.
Example: Set the query time as 200ms.
Switch(Config)# mrpp poll-time 200

8.3.12 mrpp ring

Command: mrpp ring <*ring-id*>
no mrpp ring <*ring-id*>
Function: Create MRPP ring, and access MRPP ring mode, the "**no mrpp ring<*ring-id*>**" command deletes configured MRPP ring.
Parameter: <*ring-id*> is MRPP ring ID, the valid range is from 1 to 4096.
Command Mode: Global Mode
Usage Guide: If this MRPP ring doesn't exist it create new MRPP ring when executing the command, and then it enter MRPP ring mode. It needs to ensure disable this MRPP ring when executing the "**no mrpp ring**" command.
Example:
Switch(config)#mrpp ring 100

8.3.13 mrpp ring primary-port

Command: mrpp ring <*ring-id*> primary-port
no mrpp ring <ring-id> primary-port
Function: Specify MRPP ring primary-port.
Parameter: <ring-id> *is* the ID of MRPP ring; range is <1-4096>.
Command Mode: Port mode
Default: None
Usage Guide: The command specifies MRPP ring primary port. Primary node uses primary port to send Hello packet, secondary port is used to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.
The mrpp *enable command* must be enabled before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after

control-vlan, then the mrpp-ring function is enabled.
Example: Configure the primary of MRPP ring 4000 to Ethernet 1/0/1.
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port

8.3.14 mrpp ring secondary-port

Command: mrpp ring < *ring-id* > secondary-port
no mrpp ring < ring-id > secondary-port
Function: Specify secondary *of* MRPP ring.
Parameter: <ring-id> is the ID of MRPP ring; range is <1-4096>.
Command Mode: Port mode
Default: None
Usage **Guide:** The command specifies secondary port of MRPP ring. The primary node uses secondary port to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.
The mrpp *enable command* must be enabled before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, then the mrpp-ring function is enabled.
Example: Configure secondary port of MRPP ring to 1/0/3.
Switch(config)#interface ethernet1/0/3
Switch(Config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port

8.3.15 node-mode

Command: node-mode {maser | transit}
Function: Configure the type of the node to primary node or secondary node.
Parameter: None.
Command Mode: MRPP ring mode.
Default: Default the node mode is secondary node.
Usage Guide: None.
Example: Configure the switch to primary node. MRPP ring 4000.
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#node-mode master

8.3.16 show mrpp

Command: show mrpp [<*ring-id*>]
Function: Display MRPP ring configuration.
Parameter: *<ring-id>* is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it display all of MRPP ring configuration.

Command Mode: Admin and Configuration Mode.
Default: None
Usage Guide: None
Example: Display configuration of MRPP ring 4000 of switch
Switch# show mrpp 4000

8.3.17 show mrpp statistics

Command: show mrpp statistics [<*ring-id*>]
Function: Display statistic information of data packet of MRPP ring receiving and transferring.
Parameter: ***<ring-id>*** is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it displays all of MRPP ring statistic information.
Command Mode: Admin and Configuration Mode.
Default: None
Usage Guide: None
Example: Display statistic information of MRPP ring 4000 of switch.
Switch# show mrpp statistic 4000

8.4 ULPP

8.4.1 clear ulpp flush counter interface

Command: clear ulpp flush counter interface *<name>*
Function: Clear the statistic information of the flush packets.
Parameter: <*name*> is the name of the port.
Default: None.
Command mode: Admin mode.
Usage Guide: None.
Example: Clear the statistic information of the flush packets for the port1/0/1.
Switch#clear ulpp flush counter interface e1/0/1
ULPP flush counter has been reset.

8.4.2 control vlan

Command: control vlan *<integer>*
no control vlan
Function: Configure the control VLAN of ULPP group; the no command restores the default value.
Parameter: ***<integer>*** is the control VLAN ID that sends the flush packets, range from 1 to 4094.

Default: The default is VLAN 1.
Command mode: ULPP group configuration mode.
Usage Guide: Configure the control VLAN of ULPP group. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted. It must belong to the VLAN protected by ULPP group to avoid flush packets loopback.
Example: Configure the sending control VLAN of ULPP group as 10.
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# control vlan 10

8.4.3 debug ulpp error

Command: debug ulpp error
no debug ulpp error
Function: Show the error information of ULPP. The no operation disables showing the error information of ULPP.
Parameter: None.
Default: Do not display.
Command mode: Admin mode.
Usage Guide: None.
Example: Show the error information of ULPP.
Switch# debug ulpp error
Unrecognized Flush packet received.

8.4.4 debug ulpp event

Command: debug ulpp event
no debug ulpp event
Function: Show the event information of ULPP. The no operation disables showing the event information of ULPP.
Parameter: None.
Default: Do not display.
Command mode: Admin mode.
Usage Guide: None.
Example: Show the event information of ULPP.
Switch# debug ulpp event
ULPP group 1 state changes:
Master port ethernet 1/0/1 in ULPP group 1 changed state to Forwading.
Slave port ethernet 1/0/2 in ULPP group 1 changed state to Standby.

8.4.5 debug ulpp flush {send | receive} interface

Command: debug ulpp flush {send | receive} interface *<name>*
no debug ulpp flush {send | receive} interface *<name>*

Function: Show the information of the receiving/sending flush packets, it only shows the receiving packets, but do not show the detailed contents of the packets. The no operation disables the shown information.
Parameter: ***<name>*** is the name of the port.
Default: Do not display.
Command mode: Admin mode.
Usage Guide: None.
Example: Show the information that send the flush packets for the port1/0/1.
Switch# debug ulpp flush send interface e1/0/1
Flush packet send on port Ethernet 1/0/1.

8.4.6 description

Command: description ***<string>***
no description
Function: Configure the description character string of ULPP group. The no command deletes the description.
Parameter: ***<string>*** is the name of ULPP group, the max number of the characters is 128.
Default: Do not configure ULPP name by default.
Command mode: ULPP group configuration mode.
Usage Guide: None.
Example: Configure the description of ULPP group as test.
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# description test

8.4.7 flush disable arp

Command: flush disable arp
Function: Disable sending the flush packets of deleting ARP.
Parameter: None.
Default: By default, enable the sending function of the flush packets which are deleted by ARP.
Command mode: ULPP group configuration mode.
Usage Guide: If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the entries of ARP.
Example: Disable sending the flush packets of deleting ARP.
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush disable arp

8.4.8 flush disable mac

Command: flush disable mac
Function: Disable sending the flush packets of updating MAC address.
Parameter: None.

Default: By default, enable sending the flush packets of updating MAC address.
Command mode: ULPP group configuration mode.
Usage Guide: If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to update the MAC address table.
Example: Disable sending the flush packets of updating MAC address.
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush disable mac

8.4.9 flush disable mac-vlan

Command: flush disable mac-vlan
Function: Disable sending the flush packets of deleting the dynamic unicast mac according to vlan.
Parameter: None.
Default: Disable.
Command mode:ULPP group configuration mode.
Usage Guide: If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the dynamic unicast mac according to vlan.
Example: Disable sending the flush packets deleted by mac-vlan.
Switch(config)#ulpp group 1
Switch(ulpp-group-1)#flush disable mac-vlan

8.4.10 flush enable arp

Command: flush enable arp
Function: Enable sending the flush packets of deleting ARP.
Parameter: None.
Default: By default, enable sending the flush packets of deleting ARP.
Command mode: ULPP group configuration mode.
Usage Guide: If enable this function, when the link is switched, it will actively send the flush packets to notify the upstream device, so as to delete the list entries of ARP.
Example: Enable sending the flush packets of deleting ARP.
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush enable arp

8.4.11 flush enable mac

Command: flush enable mac
Function: Enable sending the flush packets of updating MAC address.
Parameter: None.
Default: By default, enable sending the flush packets of updating MAC address.
Command mode: ULPP group configuration mode.
Usage Guide: If enable this function, when the link is switched, it will actively send the flush

packets to notify the upstream device, so as to update the MAC address table.
Example: Enable sending the flush packets of updating MAC address.
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush enable mac

8.4.12 flush enable mac-vlan

Command: flush enable mac-vlan
Function: Enable sending the flush packets of deleting the dynamic unicast mac according to vlan.
Parameter: None.
Default: Disable.
Command mode:ULPP group configuration mode.
Usage Guide: If configure this command, when the link is switched, it will actively send the flush packets to notify the upstream device to delete the dynamic unicast mac according to vlan.
Example: Enable sending the flush packets deleted by mac-vlan.
Switch(config)#ulpp group 1
Switch(ulpp-group-1)#flush enable mac-vlan

8.4.13 preemption delay

Command: preemption delay *<integer>*
no preemption delay
Function: Configure the preemption delay, the no command configures the preemption delay as the default value.
Parameter: *<integer>*: the preemption delay, range from 1 to 600, in second.
Default: The default preemption delay is 30.
Command mode: ULPP group configuration mode.
Usage Guide: The preemption delay is the delay time before the master port is preempted as the forwarding state, for avoiding the link oscillation in a short time. After the preemption mode is enabled, the preemption delay takes effect.
Example: Configure the preemption delay as 50s for ULPP group.
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# preemption delay 50

8.4.14 preemption mode

Command: preemption mode
no preemption mode
Function: Enable/disable the preemption mode of ULPP group.
Parameter: None.
Default: Do not preempt.
Command mode: ULPP group configuration mode.

Usage Guide: If the preemption mode configured by ULPP group, and the slave port is in forwarding state, and the master port is in the standby state, the master port will turn into the forwarding state and the slave port turn into the standby state after the preemption delay.
Example: Configure the preemption mode of ULPP group.
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# preemption mode

8.4.15 protect vlan-reference-instance

Command: protect vlan-reference-instance *<instance-list>*
no protect vlan-reference-instance *<instance-list>*
Function: Configure the protective VLANs of ULPP group, the no command cancels the protective VLANs.
Parameter: *<instance-list>* is MSTP instance list, such as: i; j-k. The number of the instances is not limited in the list.
Default: Do not protect any VLANs by default that means any instances are not quoted.
Command mode: ULPP group configuration mode.
Usage Guide: Quote the instances of MSTP to protect the VLANs. The VLAN corresponds to this instance is at the forwarding state on one port of this group, and at the blocked state on another port of this group. Each ULPP group can quotes all instances of MSTP. And it can quotes the inexistent MSTP instances that means any VLANs are not protected, the different ULPP groups can't quote the same instance.
Example: Configure the protective VLAN quoted from instance 1 for ULPP group.
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# protect vlan-reference-instance 1

8.4.16 show ulpp flush counter interface

Command: show ulpp flush counter interface {ethernet <IFNAME> | <IFNAME>}
Function: Show the statistic information of the flush packets.
Parameter: <IFNAME> is the name of the ports.
Default: None.
Command mode: Admin mode.
Usage Guide: Show the statistic information of the flush packets, such as: the information of the flush packets number which has been received, the time information that receive the flush packets finally.
Example: Show the statistic information of the flush packets for ULPP group1.
Switch# show ulpp flush counter interface e1/0/1
Received flush packets: 10

8.4.17 show ulpp flush-receive-port

Command: show ulpp flush-receive-port

Function: Show the port which receive flush packet, flush type and control VLAN.
Parameter: None.
Default: None.
Command mode: Admin mode.
Usage Guide: None.
Example: Show the information that the port receives flush packets.

```
Switch# show ulpp flush-receive-port
ULPP flush-receive portlist:
Portname              Type    Control Vlan
------------------------------------------------
Ethernet1/0/1         ARP     1
Ethernet1/0/3         MAC     1;3;5-10
```

8.4.18 show ulpp group

Command: show ulpp group [group-id]
Function: Show the configuration information of the ULPP groups which have been configured.
Parameter: [group-id]: Show the information of the specific ULPP group.
Default: By default, show the information of all ULPP groups which have been configured.
Command mode: Admin mode.
Usage Guide: Show the configuration information of ULPP groups which have been configured, such as: the state of the master port and the slave port, the preemption mode, the preemption delay, etc.
Example: Show the configuration information of ULPP group1.

```
Switch# show ulpp group 1
ULPP group 1 information:
Description: abc
Preemption mode: on
Preemption delay: 30s
Control VLAN:1
Protected VLAN: Reference Instance 1
Member                Role            State
--------------------------------------------------------------
Ethernet1/0/1         MASTER          FORWARDING
Ethernet1/0/2         SLAVE           STANDBY
```

8.4.19 ulpp control vlan

Command: ulpp control vlan *<vlan-list>*
no ulpp control vlan *<vlan-list>*
Function: Configure the receiving control VLANs of the port, the no command restores the default value.

Parameter: ***<vlan-list>*** specify the control VLAN list that receives the flush packets, such as: i; j-k. The number of VLANs in Each character string can not exceed 100. The receiving control VLAN of the port can be added.
Default: The default is VLAN 1.
Command mode: Port mode.
Usage Guide: Configure the receiving control VLAN for the port. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted.
Example: Configure the receiving control VLAN as 10.
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10

8.4.20 ulpp flush disable arp

Command: ulpp flush disable arp
Function: Disable receiving the flush packets of deleting ARP.
Parameter: None.
Default: By default, disable receiving the flush packets of deleting ARP.
Command mode: Port mode.
Usage Guide: If this command is configured, then it will not receive the flush packets of deleting ARP.
Example: Disable receiving the flush packets of deleting ARP.
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush disable arp

8.4.21 ulpp flush disable mac

Command: ulpp flush disable mac
Function: Disable receiving the flush packets of updating MAC address.
Parameter: None.
Default: By default, disable receiving the flush packets of updating MAC address.
Command mode: Port mode.
Usage Guide: If this command is configured, then it will not receive the flush packets of updating MAC address.
Example: Disable receiving the flush packets of updating MAC address.
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush disable mac

8.4.22 ulpp flush disable mac-vlan

Command: ulpp flush disable mac-vlan
Function: Disable receiving the flush packets of mac-vlan type.
Parameter: None.
Default: Disable.

Command mode: Port mode.
Usage Guide: If enabling this function, forward the hardware of the flush packets with mac-vlan type received in port. It will not be analyzed.
Example: Disable receiving the flush packets deleted by mac-vlan of port.
Switch(config)#interface e1/0/2
Switch(config-if-ethernet1/0/2)#ulpp flush disable mac-vlan

8.4.23 ulpp flush enable arp

Command: ulpp flush enable arp
Function: Enable receiving the flush packets of deleting ARP.
Parameter: None.
Default: By default, disable receiving the flush packets of deleting ARP.
Command mode: Port mode.
Usage Guide: Enable this function to receive the flush packets which delete ARP.
Example: Enable receiving of the flush packets of deleting ARP.
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush enable arp

8.4.24 ulpp flush enable mac

Command: ulpp flush enable mac
Function: Enable receiving the flush packets of updating MAC address.
Parameter: None.
Default: By default, disable receiving the flush packets of updating MAC address.
Command mode: Port mode.
Usage Guide: Enable receiving the flush packets of updating MAC address table.
Example: Enable receiving the flush packets of updating the MAC address.
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush enable mac

8.4.25 ulpp flush enable mac-vlan

Command: ulpp flush enable mac-vlan
Function: Enable receiving the flush packets of mac-vlan type.
Parameter: None.
Default: Disable.
Command mode: Port mode.
Usage Guide: If enabling this function, configure the interface to receive the flush packets handled mac-vlan type and delete the dynamic unicast mac according to vlan information in the packets.
Example: Enable receiving the flush packets deleted by mac-vlan of port.
Switch(config)#interface e1/0/2

Switch(config-if-ethernet1/0/2)#ulpp flush enable mac-vlan

8.4.26 ulpp group

Command: ulpp group *<integer>*

no ulpp group *<integer>*

Function: Create a ULPP group. If this group exists, then enter the configuration mode of ULPP group. The no command deletes a ULPP group.

Parameter: *<integer>* is the ID of ULPP group, range from 1 to 48.

Command mode: Global Mode.

Default: Any ULPP groups are not configured.

Usage Guide: None.

Example: Configure ulpp group 20 or enter the mode of ulpp group 20.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)#

8.4.27 ulpp group master

Command: ulpp group *<integer>* master

no ulpp group *<integer>* master

Function: Configure the master port of ULPP group, the no command deletes the master port.

Parameter: *<integer>* is the ID of ULPP group, range from 1 to 48.

Default: There is no master port configured by default.

Command mode: Port mode.

Usage Guide: There is no sequence requirement for the master and slave port configuration in a group, but the protective VLANs must be configured before the member ports. Each group has only one master port, if the master port exists, then the configuration fail.

Example: Configure the master port of ULPP group.

Switch(config)# interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)# ulpp group 20 master

8.4.28 ulpp group slave

Command: ulpp group *<integer>* slave

no ulpp group *<integer>* slave

Function: Configure the slave port of ULPP group, the no command deletes the slave port.

Parameter: *<integer>* is the ID of ULPP group, the range from 1 to 48.

Default: There is no slave port configured by default.

Command mode: Port mode.

Usage Guide: There is no sequence requirement for the master and slave port configuration in a group, but the protective VLANs must be configured before the member ports. Each group has only one slave port, if the slave port exists, then the configuration is fail.

Example: Configure the slave port of ULPP group.

Switch(config)# interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 20 slave

8.5 ULSM

8.5.1 debug ulsm event

Command: debug ulsm event
no debug ulsm event
Function: Show the event information of ULSM. The no operation disables showing ULSM events.
Parameter: None.
Default: None.
Command mode: Admin Mode.
Usage Guide: None.
Example: Show the event information of ULSM.
Switch# debug ulsm event
Downlink synchoronized with ULSM group, change state to Down.

8.5.2 show ulsm group

Command: show ulsm group [group-id]
Function: Show the configuration information of ULSM group.
Parameter: [group-id]: the ID of ULSM group.
Default: By default, show the information of all ULSM groups which have been configured.
Command mode: Admin Mode.
Usage Guide: None.
Example: Show the configuration information of ULSM group1.
Switch# show ulsm group 1
ULSM group 1 information:
ULSM group state: Down

Member	Role	State	Down by ULSM
ethernet1/0/1	UpLINK	Down	
ethernet1/0/2	DownLINK	Down	Yes

8.5.3 ulsm group

Command: ulsm group *<group-id>*
no ulsm group *<group-id>*

Function: Create a ULSM group. The no command deletes the ULSM group.
Parameter: **<*group-id*>** is the ID of ULSM group, range from 1 to 32.
Default: There is no ULSM group configured by default.
Command mode: Global Mode.
Usage Guide: None.
Example: Create ULSM group 10.
Switch(config)# ulsm group 10

8.5.4 ulsm group {uplink | downlink}

Command: ulsm group <*group-id*> {uplink | downlink}
no ulsm group <*group-id*>
Function: Configure the uplink/downlink ports of ULSM group. The no command deletes the uplink/downlink ports.
Parameter: **<*group-id*>:** The ID of ULSM group, the range from 1 to 32.
uplink: Configure the port as the uplink port.
downlink: Configure the port as the downlink port.
Default: The port does not belong to any ULSM group.
Command mode: Port Mode.
Usage Guide: Configure the uplink/downlink ports of ULSM group. Each ULSM group can configure 8 uplink ports and 16 downlink ports at most.
Example: Configure port1/0/3 as the uplink port of ULSM group10.
Switch(config)# interface ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)# ulsm group 10 uplink

8.6 ERPS

8.6.1 ethernet tcn-propagation erps to {erps | stp}

Command: ethernet tcn-propagation erps to {erps | stp}
no ethernet tcn-propagation erps to
Function: Configure the topology changing transmission notification method. Currently, the R-APS event notification among the ERPS rings is supported and it is used for the sub ring topology to send R-APS event packets to the interconnection ring after changing to notify the neighbor ring. The topology changing only takes effect in this ring as default but not be transmitted out of the ring. It does not affect the neighbor topology connected to it. The no command deletes this notification method.
Parameters: erps: topology changing sends the R-APS event packets to notify the connection ring of this device; stp: topology changing sends the stp packets to notify the stp topology connected to this device.
Default: ERPS ring topology changing only takes effect in this ring but does not send the

notification packets.

Command Mode: Global Mode.

Usage Guide: Configure the topology changing transmission notification method supported by this device as the appointed method. The ERPS ring instance detects the changing, it will send the notification packets. If configured erps method, it will send the R-APS event packets to other ERPS rings; if configured stp method, it will send the stp packets outward.

Example:

Configure to send R-APS event notification to the interconnection ring after the topology changing.

Switch(config)#ethernet tcn-propagation erps to erps

Configure to send STP notification to the interconnection ring after the topology changing.

Switch(config)#ethernet tcn-propagation erps to stp

Delete the topology changing transmission notification method.

Switch(config)#no ethernet tcn-propagation erps to

8.6.2 erps-ring <ring-name>

Command: erps-ring < *ring-name* >

no erps-ring < *ring-name* >

Function: Create ERPS ring and enter into the ERPS ring configuration mode. If the ERPS ring has existed, enter into the ERPS ring configuration mode. The no command deletes the ERPS ring.

Parameters: <*ring-name*>: the ERPS ring name created. The maximum character number is 64 and it is made up with letters, numbers and the underlines. The first and last character cannot be the underline.

Command Mode: Global Mode.

Default: Do not configure any ERPS ring.

Usage Guide: If the inputted string of ring name exceeds 64 bytes, there will be the message of "Valid ERPS ring name should be no more than 64 bytes!" If the inputted string format of ring name is not lawful, there will be the message of "Invalid ERPS ring name!" If the total number of ERPS rings configured has reached the maximum value, there will be the message of "Support ERPS ring max number: 32!" If the ERPS ring existed, enter into the ERPS ring configuration mode, otherwise, create it and enter into the ERPS ring configuration mode.

Example:

Create the ERPS ring of ring1

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#

Delete the EPRS ring of ring1

Switch(config)#no erps-ring ring1

8.6.3 version {v1 | v2}

Command: version {v1 | v2}

no version

Function: Configure the supported version of the ERPS ring. Currently it achieves the newest version of v2 and it can be compatible with v1. V1 does not support the management commands of MS, FS, etc. It does not support the multi-instance either. But it supports the Revertive switch only. If the instance is not configured on ERPS ring, the version can be configured multiple times and subject to the last time. If the ERPS ring instance has configured on the ring, the version cannot be modified. The no command recovers to be the default status of v2.

Parameters: {v1 | v2}: parameters selection. V1 means to support v1 which is released in 2008-06 and the amendment (2009-04). v2 means to support v2 which is released in 2010-03 and the amendment (2010-06).

Command Mode: ERPS Ring Configuration Mode.

Default: V2.

Usage Guide:

1. If configured ERPS ring instance on this ERPS ring, there will be the message of “Cann't config version on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!” Otherwise, enter into the next step;
2. Configure the ERPS ring to support the appointed protocol version;
3. If configured ERPS ring to support v1, this ring will not support multi-instance. ERPS ring instance does not support the management commands of MS, FS, etc. and the non-revertive switch is not effective. It only support revertive switch.
4. If configured ERPS ring to support v1, the instance of this ring will deal with the ERPS packets according to the v1 format. Package the R-APS packets and resolve the fields according to v1 format. The fields defined by v2 will not be dealt.

Example:

Configure the ERPS ring of ring1 to support v1

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#version v1
```

Configure the ERPS ring of ring1 to support v2

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#version v2
```

Delete v1 supported by the ERPS ring of ring1

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#no version
```

8.6.4 open-ring

Command: open-ring

no open-ring

Function: Configure the ERPS ring as the sub ring of open type. If configured ERPS ring instance on the ring, the ERPS ring type cannot be modified, the instance must be deleted first. The configuration of all the nodes in the ring must be the same; this type of ERPS can connect to other ERPS rings to be used in the interconnection topology. The no command deletes this configuration and recovers to be the default major ring of close type.

Parameters: None.

Command Mode: ERPS Ring Configuration Mode.
Default: The ERPS ring is major ring of close type as default.
Usage Guide: If the ERPS ring instance has been configured on the ring, there will be the message of “Cann't config open-ring on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!” Otherwise, enter into the next step. Configure this ERPS ring type as sub ring.
Example:
Configure the ERPS ring of ring1 as sub ring of open type.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#open-ring
Delete the configuration of the sub ring of open type.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#no open-ring

8.6.5 raps-virtual-channel {with | without}

Command: raps-virtual-channel {with | without}
Function: Configure if there is the R-APS virtual channel in ERPS ring. Configure it only on all the nodes of the sub ring and the configuration must be the same.
Parameters: {with | without}: parameter selection. If select with, the R-APS virtual channel is existed in this ERPS ring; if select without, the R-APS virtual channel is not existed in this ERPS ring.
Command Mode: ERPS Ring Configuration Mode.
Default: The R-APS virtual channel is not existed in ERPS ring.
Usage Guide:
a) If it is major ring, there will be the message of “Cann't config R-APS virtual channel on ERPS major ring!”
b) Configure if there is the R-APS virtual channel in ERPS ring according to the configuration.
Inputting: Success or error. If there is not R-APS virtual channel on the ERPS ring, the R-APS channel of all the instances of ERPS ring will be unblocked forever and it only blocks the data channel; otherwise, the R-APS channel and the data channel will be blocked at the same time.
Example:
Configure that there is R-APS virtual channel in the ERPS sub ring of ring1.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#raps-virtual-channel with

8.6.6 erps-ring <ring-name> port0 [port1-none]

Command: erps-ring <ring-name> port0 [port1-none]
no erps-ring <ring-name> port0
Function: Configure the port0 of the ERPS ring node. There is only one port0 on each node. If the port0 has existed, the current configuration will not be covered and there will be only the error notice. If configured port1-none, it means there is no port0 on this ring, and it is the interconnection node. The no command deletes the port0.

Parameters: <ring-name>: ERPS ring name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines.

[port1-none]: there is only the port0 on this ERPS ring node, no port1 and it is the interconnection node.

Command Mode: Port Mode.。

Default: Do not configure port0 on ERPS ring.

Usage Guide:

If the inputted string of ring name exceeds 64 bytes, there will be the message of “Valid ERPS ring name should be no more than 64 bytes!”

If the inputted string format of ring name is not lawful, there will be the message of “Invalid ERPS ring name!”

If enabled stp mutual exclusion, there will be the message of “Port %s has enable stp or other mutex module!” %s is the port name;

If this port is the member port of aggregation port, there will be the message of “Port %s is LAG member port!” %s is the port name;

If the ERPS ring did not exist, there will be the message of “The ERPS ring doesn't exist!”

If the port0 has existed in ERPS ring, there will be the message of “Port0 exists on the ERPS ring already!”

If this port is configured as port1 of ERPS ring, there will be the message of “Port %s is already configed as port1 on the ERPS ring!” %s is the port name;

If this ERPS ring is not open-ring type, the port1-none cannot be configured, there will be the message of “Can not config port1-none on ERPS major ring!”

Configure this port as the port0 of the appointed ERPS ring;

Check if the ERPS ring configuration is integral; if it is integral, check if the ERPS instance configuration is integral; if it is integral, activate the instance as active and run the protocol.

Example:

Configure e 1/0/1 as the port0 of ERPS ring1

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#erps-ring ring1 port0

Delete the e 1/0/1 as port0 of ERPS ring1

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port0

8.6.7 erps-ring <ring-name> port1

Command: erps-ring <ring-name> port1

no erps-ring <ring-name> port1

Function: Configure the port1 of the ERPS ring node. There is only one port1 on each node. If the port1 has existed, the current configuration will not be covered and there will be only the error notice. If configured port1-none, it means the configuration of port1 is not successful. The no command deletes the port1.

Parameters: <ring-name>: ERPS ring name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines.

Command Mode: Port Mode.。
Default: Do not configure port1 on ERPS ring.
Usage Guide:
If the inputted string of ring name exceeds 64 bytes, there will be the message of “Valid ERPS ring name should be no more than 64 bytes!”
If the inputted string format of ring name is not lawful, there will be the message of “Invalid ERPS ring name!”
If enabled stp mutual exclusion, there will be the message of “Port %s has enable stp or other mutex module!” %s is the port name;
If this port is the member port of aggregation port, there will be the message of “Port %s is LAG member port!” %s is the port name;
If the ERPS ring did not exist, there will be the message of “The ERPS ring doesn't exist!”
If the port1 has existed in ERPS ring, there will be the message of “Port1 exists on the ERPS ring already!”
If this port is configured as port0 of ERPS ring, there will be the message of “Port %s is already configed as port0 on the ERPS ring!” %s is the port name;
If configured port1-none on this ERPS ring, there will be the message of “Has configed port1-none on the ERPS open ring!”
Configure this port as the port1 of the appointed ERPS ring;
Check if the ERPS ring configuration is integral; if it is integral, check if the ERPS instances configuration is integral; if it is integral, activate the instance as active and run the protocol.
Example:
Configure e 1/0/1 as the port1 of ERPS ring1
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#erps-ring ring1 port1
Delete the e 1/0/1 as the port1 of ERPS ring1
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port1

8.6.8 failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>

Command: {port0 | port1} failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>
no {port0 | port1} failure-detect
Function: Configure the fault detection type of ERPS ring ports. If it is detected as cc type, the maintenance domain, maintenance set that cc belongs to and the monitoring link (it is conditioned with (mep-id, rmep-id)) should be appointed. The premise of this configuration is

that the corresponding ring port has been joined into ERPS ring. The no command deletes the fault detection type of ERPS ring ports.

Parameters: {port0 | port1}: parameter selection. Port0 means the fault detection type of port0. Port1 means the fault detection type ofport1.

{cc | physical-link-or-cc}: parameter selection. cc means that the ERPS ring port detection is cc report fault. physical-link-or-cc means that the ERPS ring port detection is cc report fault and physical link fault.

<domain-name>: the cfm domain name of ERPS ring port detection.

<ma-name>: the service name that cfm belongs to of ERPS ring port detection.

<mep-id>: the local mep id that cfm monitored of ERPS ring port detection.

<rmep-id>: the remote mep id that cfm monitored of ERPS ring port detection.

Command Mode: ERPS Ring Configuration Mode.

Default: ERPS ring port only detects the physical link fault as default.

Usage Guide:

If the inputted string of domain name exceeds 43 bytes, there will be the message of "Valid domain name should be no more than 43 bytes!"

If the inputted string format of domain name is not lawful, there will be the message of "Invalid domain name!"

If the inputted string of service name exceeds 45 bytes, there will be the message of "Valid service name should be no more than 45 bytes!"

If the inputted string format of service name is not lawful, there will be the message of "Invalid service name!"

If local mep and remote mep are the same, there will be the message of "The local mep can not be the same as the remote mep!" otherwise, enter into the next step;

Configure the fault detection type of ERPS ring ports as the appointed type. If the type is cc, save the configured md, ma, mep and rmep information to use for matching after receiving the cfm fault notification.

Example:

Configure the detection type of ERPS ring1 port0as cc.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#port0 failure-defect cc domain domain1 service serivice1 mep 1 rmep 2

Delete this configuration.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no port0 failure-defect

8.6.9 erps-instance <instance-id>

Command: erps-instance <instance-id>

no erps-instance <instance-id>

Function: Create the ERPS ring instance and enter into the ERPS ring instance configuration mode. If this ERPS ring instance has existed, enter into the ERPS instance configuration mode. If ERPS ring supports v2, multiple ERPS ring instances can be configured. The no command deletes the ERPS ring instance.

Parameters: <instance-id>: id of ERPS ring, the range is 1 to 48.

Command Mode: ERPS Ring Configuration Mode.

Default: Do not configure any ERPS ring instance.

Usage Guide: If the ERPS ring supports v1, there will be the message of "Doesn't support multiple ERPS instance capability on the ring running version 1!" when configured more than one ERPS instance.

If the configured instance exceeds the maximum ERPS instance number supported, there will be the message of "Support ERPS instance max number: 32 per ERPS ring!"

If the ERPS ring instance has existed on the ERPS ring, enter into the ERPS ring instance configuration mode;

Otherwise, create the corresponding ERPS ring instance and enter into the ERPS ring instance configuration mode.

Example:

Configure the ERPS ring instance 1 on ERPS ring1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#

Delete the ERPS ring instance 1 on ERPS ring1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no erps-instance 1

Switch(config-erps-ring-inst-1)#

8.6.10 description

Command: description <instance-name>

no description <instance-name>

Function: Configure the description string of ERPS instance.

Parameters: <instance-name>: ERPS instance name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines. The no command deletes the ERPS instance name.

Command Mode: ERPS Instance Configuration Mode.

Default: Do not configure the ERPS instance name as default.

Usage Guide: Judge the length of the string, if exceed 64, there will be the message of "Valid ERPS instance name should be no more than 64 bytes!" if the string format is not lawful, there will be the message of "Invalid ERPS instance name!" otherwise, configure the ERPS instance name as the appointed string.

Example:

Configure the ERPS instance1 name on ring1 as instance1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# description instance1

Delete this name of instance1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)# no description

8.6.11 ring-id <ring-id>

Command: ring-id <ring-id>
no ring-id <ring-id>
Function: Configure the last byte of R-APS packets destination MAC address sent by ERPS ring node to carry ring-id. If ERPS ring supports v1, ring-id only can be configured as 1. The no command configures it not to carry the ring-id, it means that the MAC is 01-19-A7-00-00-01.
Parameters: <ring-id>: ERPS ring id and the range is 1 to 64.
Command Mode: ERPS Instance Configuration Mode.
Default: The MAC address is 01-19-A7-00-00-01 as default.
Usage Guide: If ERPS ring supports v1, ring-id only can be configured as 1. Because v1 only supports the destination MAC address of 01-19-A7-00-00-01, otherwise, there will be the message of “Cann't config ringid other than 1 on the ERPS ring running version 1!”
If ERPS ring supports v2, configure the last byte of R-APS packets destination MAC address sent by ERPS ring node to carry the appointed ring-id.
Example:
Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 to carry the ring-id 2.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 2
Switch(config-erps-ring-inst-2)#ring-id 2
Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 not to carry the ring-id, it means the destination MAC is 01-19-A7-00-00-01.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 2
Switch(config-erps-ring-inst-2)#no ring-id

8.6.12 rpl {port0 | port1} {owner | neighbour}

Command: rpl {port0 | port1} {owner | neighbour}
no rpl {port0 | port1}
Function: Configure the member port of ERPS ring instance as RPL owner or RPL neighbour, the RPL node roles of different instances on the same ERPS ring cannot be configured on the same member port. The no command configures the member port of ERPS ring instance as the ordinary transmission port member.
Parameters: {port0 | port1}: parameter selection. Port0 means the RPL role of port0 in ERPS ring instance; port1 means the RPL role of port1 in ERPS ring instance.
{owner | neighbour }: parameter selection. Owner means to configure the appointed member port as rpl owner; neighbour means to configure the appointed member port as rpl neighbour.
Command Mode: ERPS Instance Configuration Mode.

Default: None, it is the ordinary transmission node type.

Usage Guide: If configured port1-none, the node role of port1 cannot be configured, there will be the message of “Has configed port1-none on the ERPS open ring!”

If this instance node is already rpl owner or rpl neighbour, cannot run this command to any member port, there will be the message of “Has configed port rpl role: %s on the ERPS instance!” %s is the configured rpl role;

If other instance has configured the appointed rpl role on the ERPS ring, there will be the message of “Has configed port rpl role: %s in this or other ERPS instance on the ERPS ring!” configure the appointed member port on the ERPS ring of that instance as the appointed node role.

Example:

Configure the port0 of ERPS ring1 instance1 as RPL owner node.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# rpl port0 owner

Configure the port0 of ERPS ring1 instance1 as the ordinary transmission port role.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# no rpl port0

8.6.13 non-revertive

Command: non-revertive

no non-revertive

Function: Configure the ERPS ring instance as non-revertive. If this ERPS ring supports v1, this command is null and cannot be configured. The no command configures the ERPS ring instance as revertive. If this ERPS ring supports v1, this command is null. This command can be configured only on the RPL owner node of the sub ring.

Parameters: None.

Command Mode: ERPS Instance Configuration Mode.

Default: ERPS ring instance supports the revertive as default.

Usage Guide: If ERPS ring supports v1, there will be the message of “Cann't config non-revertive on the ERPS ring running version 1!”

If the ERPS ring supports v2, configure this ERPS ring instance to support the non-revertive.

Example:

Configure the ERPS ring1 instance1 to support the non-revertive.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#non-revertive

Delete this configuration.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no non-revertive

8.6.14 guard-timer <guard-times>

Command: guard-timer <guard-times>

no guard-timer

Function: Configure the Guard timer. The guard timer is used for the Ethernet node to avoid the error handling and the close loop according to the outdated R-APS packets. In the starting time of the timer, any R-APS packets received (the R-APS packets that the Request/State=”1110” are except) will be dropped. The no command configures the guard timer as the default value.

Parameters: <guard-times>: the interval is 10ms and the range is 10ms to 2s.

Command Mode: ERPS Instance Configuration Mode.

Default: 500ms.

Usage Guide: If the timer is not enabled, configure the guard timer of ERPS ring instance as the appointed time; if it is enabled, configure the guard timer as the configuration value immediately. The timer will not be cleared, it will run still according to the last configuration time and this configuration will be effective next time.

Example:

Configure the guard timer of ERPS ring1 instance1 as 1s.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)guard-timer 100

Configure the guard timer of ERPS ring1 instance1 as the default value.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1) no guard-timer

8.6.15 holdoff-timer < holdoff-times>

Command: holdoff –timer <holdoff-times>

no holdoff -timer

Function: Configure the Holdoff timer. The Holdoff timer is used for the Ethernet node to block the default report time. When the new default happened or the default was more serious, this default will not be reported to the protection switching for handling immediately if the useful Holdoff timer is not 0, but enable the Holdoff timer. When the timer is time out, check if the link default in the timer starting still existed. If there is still the default, report it to handle it with protection switching, this default is not necessarily the one in the timer starting. The no command configures the Holdoff timer as the default value.

Parameters: <holdoff-times>: the interval is 1s and the range is 0 to 10s.

Command Mode: ERPS Instance Configuration Mode.

Default: 0s.

Usage Guide: If the timer is not enabled, configure the holdoff timer of ERPS ring instance as the appointed time; if it is enabled, configure the holdoff timer as the configuration value immediately. The timer will not be cleared, it will run still according to the last configuration time and this configuration will be effective next time.

Example:

Configure the Holdoff timer of ERPS ring1 instance1 as 5s.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#holdoff –timer 5

Configure the Holdoff timer of ERPS ring1 instance1 as the default value.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no holdoff –timer

8.6.16 wtr-timer <wtr-times>

Command: wtr-timer <wtr-times>

no wtr-timer

Function: Configure the WTR timer. WTR timer is used to avoid the frequent protection switching of RPL owner node because of the periodic (intermittent) default. When RPL owner port received the default recovery packets, after some time, and then check if the default still existed on the other nodes and prevent blocking RPL owner port immediately to cause the chokepoint shocking. The no command configures the WTR timer as the default.

Parameters: <wtr-times>: the interval is 1min and the range is from 1 to 12min.

Command Mode: ERPS Instance Configuration Mode.

Default: 5min.

Usage Guide: If the timer is not enabled, configure the WTR timer of ERPS ring instance as the appointed time; if it is enabled, configure the WTR timer as the configuration value immediately. The timer will not be cleared, it will run still according to the last configuration time and this configuration will be effective next time.

Example:

Configure the WTR timer of ERPS ring1 instance1 as 10min.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#wtr-timer 10

Configure the WTR timer of ERPS ring1 instance1 as the default value.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no wtr-timer

8.6.17 protected-instance

Command: protected-instance <instance-list>

no protected-instance <instance-list>

Function: Configure the protection instance of ERPS ring instance. ERPS ring instance can protect all the MSTP instances. The same instance cannot be quoted by multiple ERPS ring instances under the same topology. Under the same ERPS ring instance, run this command more than once

to protect instance, the result will be accumulated. The no command deletes the protection instance of ERPS ring instance.

Parameters: <instance-list>: the MSTP instance list protected by ERPS ring instance, such as i, j-k. The number of the instances in the list is not limited.

Command Mode: ERPS Instance Configuration Mode.

Default: ERPS ring instance does not protect any MSTP instance.

Usage Guide: If the inputting instance has been protected by other ERPS instance, there will be the message of "Instance: %d is protected by erps instance: %d on ring: %s!" the first %d is mstp instance id and the second is erps instance id; %s is ERPS ring name;

Configure the protection instance of ERPS ring instance as the appointed MSTP instance;

Check if the ERPS instance configuration is complete, if it is complete, activate the instance as active, and run the protocol.

Example:

Configure the protection instance of ERPS ring1 instance1 as instance 2.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#protected-instance 2

Delete this configuration.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no protected-instance 2

8.6.18 raps-mel <level-value>

Command: raps-mel <level-value>

no raps-mel

Function: Configure the level of R-APS channel.

Parameters: <level-value>: the level value of APS packets, range is from 0 to 7.

Command Mode: ERPS Instance Configuration Mode.

Default: Level is 7.

Usage Guide: Configure the level of R-APS channel of ERPS ring instance as the appointed level. If configured successfully, the mel field of the R-APS packet sent by this ERPS ring instance will be added as the appointed level and only the R-APS packets with the level that is larger than or same as the appointed level can be allowed passing by, or notify the error. The no command configures the level as the default of 7. The MEL field in the protocol packets is used to detect if the current packet can pass by. If the MEL value configured in ERPS ring is letter than the value in the fault detection protocol, it means that the packet level is low and cannot pass by. The level configuration of all the nodes in the instance must be identical.

Example:

Configure the level of R-APS channel of ERPS ring1 instance1 as 5.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)raps-mel 5

Configure the level of R-APS channel of ERPS ring1 instance1 as 7.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)no raps-mel

8.6.19 control-vlan <vlan-id>

Command: control-vlan <vlan-id>
no control-vlan

Function: Configure the control vlan of R-APS packets of R-APS channel. In the ERPS ring instance, this vlan is only used to transmit ERPS protocol packets but not to forward the user business packets. It improves the ERPS protocol security. User makes sure the configuration uniqueness. This vlan is as the vlan tag when sending R-APS packets. The protection VLAN configuration of all the nodes in the instance must be identical. The no command deletes the control vlan.
Parameters: <vlan-id>: vlan id of R-APS packets, range is from 2 to 4094.
Command Mode: ERPS Instance Configuration Mode.
Default: Do not configure any control vlan.
Usage Guide: User configuration should meet the following situations:
The protection VLAN configuration of all the nodes in the instance must be identical;
The control vlan has uniqueness;
If the ring type with the instance is major ring, the control vlan and the protection vlan are in the same instance;
If the ring type with the instance is sub open-ring and it is the virtual channel method without R-APS, the control vlan belongs to one instance all alone;
The member port belongs to the control vlan and protection vlan.
The control vlan handling is as below:

a) If the inputting VLAN does not existed, there will be the message of “Error, VLAN %d does not exist!” %d is the inputting value;
b) If this ERPS ring instance has configured the control VLAN, there will be the message of “Control vlan has existed already!”
c) Configure the control VLAN of the ERPS ring instance as the appointed VLAN;
d) Check if the ERPS instance is integral, if it is integral, activate the instance as active and run the protocol.

Notice: The ordinary data vlan and the control vlan of the different erps instances cannot associated with the same MSTI.
Example:
Configure the control vlan of ERPS ring1 instance1 as vlan10.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)control-vlan 10
Delete this configuration.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)no control-vlan

8.6.20 forced-switch {port0 | port1}

Command: forced-switch {port0 | port1}

Function: Run the forced switch on the port of ERPS ring node. Two or more forced switch are allowed existing at the same time in one ERPS ring instance. But only one forced switch command can be existed on one ring node. User should avoid using multiple forced switch in ERPS ring instance to cause the ERPS ring instance splitting.

Parameters: {port0 | port1}: parameter selection, port0 means to run the forced switch configuration on port0 of the ring node; port1 means to run the forced switch configuration on port1 of the ring node.

Command Mode: ERPS Instance Configuration Mode.

Default: No forced switch in ERPS ring instance.

Usage Guide: If this ring supports version1, there will be the message of “Doesn't support the command on the ring running version 1!” otherwise, enter into the next step;

If this instance configuration is not integral, it is on the status of unactive, there will be the message of “The request is rejected because the ERP instance in unactive state!” otherwise, enter into the next step;

If the local forced switch has existed on the node of this ring instance (on same time, only one of port0 and port1 can be in the status of local FS), there will be the message of “The FS request is rejected because an local FS request is present!” otherwise, enter into the next step;

If the forced switch is on the current highest priority, block the data channel and R-APS channel of this ERPS ring instance on the appointed member port (port0 or port1), and unblock the other member port of this ring node;

When the forced switch command is the highest priority command, send the P-APS (FS) packets with FS message on the two ring ports (port0 and port1) stably and steadily;

For the node which received the R-APS (FS) packets, if there is no higher priority request in local, unblock all the blocked ring ports;

The node which received the R-APS (FS) packets should run the flush FDB configuration according the corresponding demand.

Example:

Run the forced switch configuration on the port0 of ERPS ring1 instance1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#force-switch port0

8.6.21 manual-switch {port0 | port1}

Command: manual-switch {port0 | port1}

Function: Run the manual switch on the port of ERPS ring node. Only one manual switch is allowed existing in one ERPS ring instance, and the premise is that there is no SF fault or FS command in ERPS ring instance.

Parameters: {port0 | port1}: parameter selection, port0 means to run the manual switch configuration on port0 of the ring node; port1 means to run the manual switch configuration on port1 of the ring node.

Command Mode: ERPS Instance Configuration Mode.

Default: No manual switch in ERPS ring instance.

Usage Guide: If this ring supports version1, there will be the message of “Doesn't support the command on the ring running version 1!” otherwise, enter into the next step;

If this instance configuration is not integral, it is on the status of unactive, there will be the message of “The request is rejected because the ERP instance in unactive state!” otherwise, enter into the next step;

If the MS status has existed in ERPS ring node, there will be the message of “The MS request is rejected because an existing MS request is present!”

If the manual switch has existed on the node of this ring instance, there will be the message of “The MS request is rejected because an existing FS request is present!” otherwise, enter into the next step;

If there has been the fault in ERPS ring instance, there will be the message of “The MS request is rejected because an existing SF is present!” otherwise, enter into the next step;

If the manual switch is on the current highest priority, block the data channel and R-APS channel of this ERPS ring instance on the appointed member port (port0 or port1), and unblock the other member port of this ring node;

When the manual switch command is the highest priority command, send the P-APS (MS) packets with MS message on the two ring ports (port0 and port1) stably and steadily;

For the node which received the R-APS (MS) packets, if there is no higher priority request in local, unblock all the blocked ring ports;

The node which received the R-APS (MS) packets should run the flush FDB configuration according the corresponding demand.

Example:

Run the manual switch configuration on the port0 of ERPS ring1 instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#manual-switch port0
```

8.6.22 clear command

Command: clear command

Function: Run the clear command to the member port of ERPS ring node, it can clear the management command of the local activity: forced switch command and manual switch command; it can be also used to trigger the link switch under the revertive mode before WTR or WTB is time out; and trigger the link to switch from the standby link RPL back to the intrinsic link under the non-revertive mode after the fault recovery. For the last two situations, run this command on the rpl owner node universally.

Parameters: None.

Command Mode: ERPS Instance Configuration Mode.

Default: No clear command in ERPS ring instance.

Usage Guide: If this ring supports version1, there will be the message of “Doesn't support the command on the ring running version 1!” otherwise, enter into the next step;

If this instance configuration is not integral, it is on the status of unactive, there will be the message of “The request is rejected because the ERP instance in unactive state!” otherwise, enter into the next step;

If the forced or manual switch command has existed on the node of this ring instance, clear the switch command and keep the block status of the data channel and R-APS channel of the blocked member ports. And send the P-APS (NR) packets on the two member ports stably and steadily until received R-APS (NR, RB) packets and known the RPL is blocked. Or the higher level request happens on the ring (such as SF);

If the local forced or manual switch has existed on the node of this ring instance, clear the command and then receive the R-APS (NR) packets whose node ID is larger than the local node ID. Unblock all the ring ports without SF fault and stop sending the R-APS (NR) packets on the two member ports.

If the ERPS ring instance that RPL owner node is in is the revertive mode and the WTR or WTB timer is enabled, delete the timer, block the RPL port and send the R-APS (NR, RB) packets on the two ring ports; and run flush FDB configuration, trigger the link switch in advance. Otherwise, enter into the next step;

If the ERPS ring instance that RPL owner node is in is the non-revertive mode, block the RPL port and send the R-APS (NR, RB) packets on the two ring ports; and run flush FDB configuration, trigger the link to switch from the standby link RPL back to the intrinsic link.

Example:

Run clear configuration on ERPS ring1 instance1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#clear command

8.6.23 show erps ring {<ring-name> | brief}

Command: show erps ring {<ring-name> | brief}

Function: Read the ERPS ring information.

Parameters: <*ring-name*>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, show all the ERPS rings of this device.

brief: Show the ERPS ring main information.

Command Mode: Admin Mode.

Default: None.

Example: show all the ERPS rings information.

Switch#show erps ring brief

```
Ring-Name          Ring-topo     Port0    Port1    Version   Inst-Count
-----------------------------------------------------------------------------------------
ring1              maijor-ring   1/0/1    1/0/2    V2        1
```

ring2 open-ring 1/0/5 1/0/6 V2 1

Fields	Explanation
Ring-Name	ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines.
Ring-topo	ERPS ring topology mode: major-ring, open-bring
Port0	Port0 information of ERPS ring
Port1	Port1 information of ERPS ring
Version	Version that ERPS ring supports: V1, V2
Inst-Count	Instances number range of ERPS ring: 1 to 64

Show the ERPS ring1 information:

```
Switch#show erps ring ring1
R: RPL Owner
N: RPL Neighbour
C: Common Node
-------------------------------------------------------------------------------------------------
R-APS ring topology: open-ring
R-APS Virtual-Channel: with
Port0: Ethernet1/0/1                    Failure-detect type: physical-link-or-cc
Port1: Ethernet1/0/2                    Failure-detect type: physical-link
Instance  Contral  Protected  WTR_Timer  Guard_Timer  Holdoff_Timer  Port0 Port1
ID        Vlan     Instance   (min)      (csec)       (second)
-------------------------------------------------------------------------------------------------
1         10       3          6          100          0              R     C
2         20       4          5          500          0              C     C
```

Fields	Explanation
Instance ID	Id number of ERPS ring instance, range is from 1 to 64.
Contral Vlan	R-APS channel vlan, package R-APS packet of tag
Protected Instance	MSTP instance protected by ERPS ring instance
WTR_Timer	Wait to Restore timer, range is from 1 to 12min.
Guard_Timer	Guard timer, range is from 10ms to 2s
Holdoff_Timer	Holdoff timer, range is from 0 to 10s
Port0	Port0 information of ERPS ring
Port1	Port1 information of ERPS ring
R-APS ring topology	ERPS ring topology mode: major-ring, open-bring
R-APS Virtual-Channel	If it is ERPS sub ring, whether there is the R-APS virtual channel: with, without

8.6.24 show erps instance [ring <ring-name> [instance <instance-id>]]

Command: show erps instance [ring <ring-name> [instance <instance-id>]]

Function: Show the ERPS ring instance information.

Parameters: <*ring-name*>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, show all the ERPS ring instances of this device.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show all the ERPS ring instances information.

Command Mode: Admin Mode.

Default: None.

Example:

Show all the ERPS ring instances information.

```
Switch#show erps instance
ERPS Ring ring1
  Instance 1
  Description: instance1
  Protected Instance: 1
  Revertive mode: non-revertive
  R-APS MEL: 7
  R-APS Virtual-Channel: with
  Control Vlan: 10
  Ring ID:
  Guard Timer (csec): 100
  Holdoff Timer (seconds): 0
  WTR Timer (min): 6
  ----------------------------------------------------------------
  Port          Role              Port-Status
  ----------------------------------------------------------------
  port0         RPL Owner         Blocked
  port1         Common            Forwarding
```

Fields	Explanation
Description	ERPS ring instance name
Protected Instance	MSTP instance protected by ERPS ring instance
Revertive mode	ERPS ring link mode: revertive, non-revertive
R-APS MEL	Level of R-APS channel, package R-APS packets
R-APS Virtual-Channel	If the ERPS ring is the sub ring, the R-APS virtual channel of the inherited ring: with, without
Ring ID	The ring-id number carried by the packets sent by ERPS ring instance, range is from 1 to 64.

Contral Vlan	R-APS channel vlan, package R-APS packet of tag
WTR_Timer	Wait to Restore timer, range is from 1 to 12min
Guard_Timer	Guard timer, range is from 10ms to 2s
Holdoff_Timer	Holdoff timer, range is from 0 to 10s
Port	ERPS ring port information: port0, port1
Role	ERPS ring node roles: RPL Owner, RPL neighbor, Common
Port Status	Blocked: port is in block status forwarding: port is in forwarding status

8.6.25 show erps status [ring <ring-name> [instance <instance-id>]]

Command: show erps status [ring <ring-name> [instance <instance-id>]]

Function: Show the status information of ERPS ring instance.

Parameters: <*ring-name*>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, show all the ERPS rings of this device.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show all the ERPS ring instances status information.

Command Mode: Admin Mode.

Default: None.

Example:

Show all the ERPS ring instances status information.

```
Switch#show erps status
ERPS ring ring1 instance 1 status：
Active：1
Node State：Idle
Time last topology change : Jan 01 00:17:25 2012
---------------------------------------------------------------------------------------------
Port      Interface     Port-Status       Signal-Status     R-RAPS-NodeId       BPR
---------------------------------------------------------------------------------------------
Port0     1/0/1         blocked           Non-failed        00-00-00-00-00-00   0
Port1     1/0/2         forwarding        Non-failed        00-00-00-00-00-00   0
```

Active	Current active status of ERPS ring instance: 1, 0
Node State	Current status of ERPS ring instance: Idle, Protection, Forced-switch, Manual-switch, Pending
Port Status	Blocked: the port is in block status Forwarding: the port is in forwarding status
Signal Status	ERPS ring port fault status: Non-failed: no fault

	Failed: fault happened
Remote R-APS NodeId	NodeId information carried by the receiving last R-APS saved by ERPS ring port, it is mac information.
BPR	The block link information carried by the receiving last R-APS saved by ERPS ring port, it is port0 or port1 which was blocked.
Time last topology change	Topology switching last time

8.6.26 show erps statistics [ring <ring-name> [instance <instance-id>]]

Command: show erps statistics [ring <ring-name> [instance <instance-id>]]

Function: Show the statistic information of ERPS ring instance.

Parameters: <ring-name>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, show the statistic information of all the ERPS rings of this device.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show the statistic information of all the ERPS ring instances of this device.

Command Mode: Admin Mode.

Default: None.

Example:

Show the statistic information of ERPS ring instance.

```
Switch#show erps statistics ring 1 instance 1
Statistics for ERPS ring ring1 instance 1：
R-APS          Port0(Tx/Rx)          Port1(Tx/Rx)
------------------------------------------------------------------------
NR                  3/0                  3/0
NR,RB               0/0                  0/0
SF              19129/0              19129/0
MS                  0/0                  0/0
FS                  0/0                  0/0
EVENT               0/0                  0/0
------------------------------------------------------------------------
TOTOL          19132/0              19132/0
```

8.6.27 clear erps statistics [ring <ring-name> [instance <instance-id>]]

Command: clear erps statistics [ring <ring-name> [instance <instance-id>]]

Function: Clear the statistic information of ERPS.

Parameters: <ring-name>: ERPS ring name, the maximum characters number is 64 and it is made

up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, clear the statistic information of all the ERPS rings of this device.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, clear the statistic information of all the ERPS ring instances of this device.

Command Mode: Admin Mode.

Default: None.

Example: Clear the statistic information of ERPS ring1 instance1.

Switch#clear erps statistics ring 1 instance 1

8.6.28 debug erps

Command: debug erps packet [detail] {send | receive] {[ring <ring-name> [instance <instance-id>]] | [port]}

debug erps fsm [ring <ring-name> [instance <instance-id>]]

debug erps timer [ring <ring-name> [instance <instance-id>]]

no debug eprs

Function: Enable the debug information of ERPS. The no command disables this information.

Parameters: packet: Enable the packets debug information.

detail: Enable the detail debug information of packets.

send: Enable the sending packets debug information.

received: Enable the receiving packets debug information.

fsm: Enable the status device debug information.

timer: Enable the timer debug information.

<ring-name>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48.

Command Mode: Admin Mode.

Default: Do not show.

8.6.29 debug erps error

Command: debug erps error

no debug erps error

Function: Show the default information of ERPS. The no command disables this information.

Parameters: None.

Command Mode: Admin Mode.

Default: Do not show.

8.6.30 debug erps event

Command: debug erps event

no debug erps event

Function: Show the event information of ERPS. The no command disables this information.

Parameters: None.
Command Mode: Admin Mode.
Default: Do not show.

8.6.31 no debug all

Command: no debug all
Function: Disable all the debug information of this device.
Parameters: None.
Command Mode: Admin Mode.
Default: None.
Usage Guide: When using no debug all command to disable all the debug information of the switch, this command is effective to the debug information of ERPS, the debug information of ERPS will be disabled too.

8.6.32 show debugging

Command: show debugging
Function: Enable all the debug information of this module.
Parameters: None.
Command Mode: Admin Mode.
Default: None.
Usage Guide: When using **show debugging erps** command to show the debug information, this module supports this command.

Chapter 9 Commands for Debugging and Diagnosis

9.1 Monitor and Debug

9.1.1 clear history all-users

Command: clear history all-users
Function: Clear the command history of all users saved by the switch.
Command Mode: Admin mode
Usage Guide: Using this command can clear the command history of all users.
Example:
Switch#clear history all-users

9.1.2 history all-users max-length

Command: history all-users max-length <count>
Function: Set the max command history of all users saved by the switch.
Parameter: <count>: the command history number can be saved, ranging from 100 to 1000
Command Mode: Global mode
Usage Guide: The system can save 100 recent command history of all users at best by default, using this command can set the max command history number.
Example:
Switch(config)#history all-users max-length 500

9.1.3 ping

Command: ping [[src *<source-address>*] { *<destination-address>* | host *<hostname>* }]
Function: Issue ICMP request to remote devices, check whether the remote device can be reached by the switch.
Parameters: *<source-address>* is the source IP address where the ping command is issued, with IP address in dotted decimal format. ***<destination-address>*** is the target IP address of the ping command, with IP address in dotted decimal format. ***<hostname>*** is the target host name of the ping command, which should not exceed 64 characters.
Default: 5 ICMP echo requests will be sent. The default packet size and time out is 56 bytes and 2 seconds.
Command Mode: Admin mode
Usage Guide: When the ping command is entered without any parameters, interactive configuration mode will be invoked. And ping parameters can be entered interactively.

Example:

Example 1: To ping with default parameters.

Switch#ping 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds.

...!!

Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms

In the example above, the switch is made to ping the device at 10.1.128.160. The command did not receive ICMP reply packets for the first three ICMP echo requests within default 2 seconds timeout. The ping failed for the first three tries. However, the last two ping succeeded. So the success rate is 40%. It is denoted on the switch "." for ping failure which means unreachable link, while "!" for ping success, which means reachable link.

Example 2: Use ping command with source address configuration, and leave other fields to default.

Switch#ping src 10.1.128.161 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, using source address 10.1.128.161, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

In the example above, 10.1.128.161 is configured as the source address of the ICMP echo requests, while the destination device is configured to be at 10.1.128.160. The command receives all the ICMP reply packets for all of the five ICMP echo requests. The success rate is 100%. It is denoted on the switch "." for ping failure which means unreachable link, while "!" for ping success, which means reachable link.

Example 3: Ping with parameters entered interactively.

Switch#ping

VRF name：

Target IP address：10.1.128.160

Use source address option[n]: y

Source IP address: 10.1.128.161

Repeat count [5]: 100

Datagram size in byte [56]：1000

Timeout in milli-seconds [2000]: 500

Extended commands [n]: n

Display Information	Explanation
VRF name	VRM name. If MPLS is not enabled, this field will be left empty.
Target IP address：	The IP address of the target device.
Use source address option[n]	Whether or not to use ping with source address.
Source IP address	To specify the source IP address for ping.

Repeat count [5]	Number of ping requests to be sent. The default value is 5.
Datagram size in byte [56]	The size of the ICMP echo requests, with default as 56 bytes.
Timeout in milli-seconds [2000]:	Timeout in milli-seconds, with default as 2 seconds.
Extended commands [n]:	Whether or to use other extended options.

9.1.4 ping6

Command: ping6 [<dst-ipv6-address> | host *<hostname>* / src *<src-ipv6-address>* {*<dst-ipv6-address >* / host *<hostname>*}]

Function: To check whether the destination network can be reached.

Parameters: ***<dst-ipv6-address>*** is the target IPv6 address of the ping command. ***<src-ipv6-address>*** is the source IPv6 address where the ping command is issued. ***<hostname>*** is the target host name of the ping command, which should not exceed 64 characters.

Default: Five ICMP6 echo request will be sent by default, with default size as 56 bytes, and default timeout to be 2 seconds.

Command Mode: Normal user mode

Usage Guide: When the ping6 command is issued with only one IPv6 address, other parameters will be default. And when the ipv6 address is a local data link address, the name of VLAN interface should be specified. When the source IPv6 address is specified, the command will fill the icmp6 echo requests with the specified source address for ping.

Example:

(1) To issue ping6 command with default parameters.

Switch>ping6 2001:1:2::4

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 2001:1:2::4, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms

(2) To issue the ping6 command with source IPv6 address specified.

switch>ping6 src 2001:1:2::3 2001:1:2::4

Type *^c* to abort.

Sending 5 56-byte ICMP Echos to 2001:1:2::4, using src address 2001:1:2::3, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

(3) To issue the ping6 command with parameters input interactively.

switch>ping6

Target IPv6 address:fe80::2d0:59ff:feb8:3b27

Output Interface: vlan1

Use source address option[n]:y

Source IPv6 address: fe80::203:fff:fe0b:16e3

Repeat count [5]:

Datagram size in byte [56]:
Timeout in milli-seconds [2000]:
Extended commands [n]:
Type ^c to abort.
Sending 5 56-byte ICMP Echos to fe80::2d0:59ff:feb8:3b27, using src address fe80::203:fff:fe0b:16e3, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

Display Information	Explanation
ping6	The ping6 command
Target IPv6 address	The target IPv6 address of the command.
Output Interface	The name of he VLAN interface, which should be specified when the target address is a local data link address.
Use source IPv6 address [n]:	Whether or not use source IPv6 address. Disabled by default.
Source IPv6 address	Source IPv6 address.
Repeat count[5]	Number of the ping packets.
Datagram size in byte[56]	Packet size of the ping command. 56 byte by default.
Timeout in milli-seconds[2000]	Timeout for ping command. 2 seconds by default.
Extended commands[n]	Extended configuration. Disabled by default.
!	The network is reachable.
.	The network is unreachable.
Success rate is 100 percent(8/8), round-trip min/avg/max = 1/1/1ms	Statistic information, success rate is 100 percent of ping packet.

9.1.5 show boot-files

Command: show boot-files
Function: Display the first and second IMG files and the CFG file enabled by switch.
Command Mode: Admin and Configuration Mode.
Usage Guide: After implementing this command, the booting sequence of IMG files in the corresponding storage device, which IMG file is currently used in booting, the configuration information of the CFG file in the storage device and the CFG file currently booted.
Example: Display the first and second IMG files and the CFG file enabled by switch.
Switch(config)#show boot-files
The primary img file at the next boot time: mmc:/nos.img
The backup img file at the next boot time: mmc:/nos.img
Current booted img file: mmc:/nos.img

Repair primary img by backup img: yes

The startup-config file at the next boot time: flash:/initial.cfg
Current booted startup-config file: flash:/vsf_startup.cfg

9.1.6 show debugging

Command: show debugging {bgp | dvmrp | igmp | ipv6 | mld | nsm **| ospf | other | pim | rip | spanning-tree | vrrp}**
Function: Display the debug switch status.
Usage Guide: If the user needs to check what debug switches have been enabled, **show debugging** command can be executed.
Command mode: Admin Mode
Example: Check for currently enabled debug switch.
Switch#show debugging ospf
OSPF debugging status:
OSPF all IFSM debugging is on
OSPF packet Hello detail debugging is on
OSPF packet Database Description detail debugging is on
OSPF packet Link State Request detail debugging is on
OSPF packet Link State Update detail debugging is on
OSPF packet Link State Acknowledgment detail debugging is on
OSPF all LSA debugging is on
OSPF all NSM debugging is on
OSPF all events debugging is on
OSPF all route calculation debugging is on
Switch#
Relative command: debug

9.1.7 show fan

Command: show fan
Function: Show fan information of switch.
Parameter: None.
Command Mode: Any modes.
Usage Guide: Check fan information of switch.
Example: Show the current fan information of switch.
Switch#show fan
Fan board information:

Fan No	Inserted	Status	Speed
1	NO	Abnormal	None

2	YES	Normal	Medium
3	YES	Normal	Medium
4	YES	Normal	Medium

9.1.8 show flash

Command: show flash

Function: Show the size of the files which are reserved in the system flash memory.

Command Mode: Admin Mode and Configuration Mode.

Example: To list the files and their size in the flash.

Switch#show flash

boot.rom	329,828 1900-01-01 00:00:00 --SH
boot.conf	94 1900-01-01 00:00:00 --SH
nos.img	2,449,496 1980-01-01 00:01:06 ----
startup-config	2,064 1980-01-01 00:30:12 ----

9.1.9 show history

Command: show history

Function: Display the recent user command history.

Command mode: Admin Mode

Usage Guide: The system holds up to 20 commands the user entered, the user can use the UP/DOWN key or their equivalent (ctrl+p and ctrl+n) to access the command history.

Example:

Switch#show history

enable

config

interface ethernet 1/0/3

enable

dir

show ftp

9.1.10 show history all-users

Command: show history all-users [detail]

Function: Show the recent command history of all users.

Parameter: [detail] shows user name of the executing command. IP address of the user will be shown when logging in the executing command through Telnet or SSH.

Command Mode: Admin and configuration mode

Usage Guide: This command is used to show the recent command history of all users, including time, logging type, executing command, etc.

Notice: The user can only check the command history of other users whose purview should not be higher than oneself.

Example:

Switch(config)#show history all-users detail

Time	Type	User	Command
0w 0d 0h 2m	Telnet/SSH	admin	show history all-users detail 192.168.1.2:1419
0w 0d 0h 1m	Telnet/SSH	admin	show history all-users 192.168.1.2:1419
0w 0d 0h 1m	Console	Null	show history all-users
0w 0d 0h 1m	Console	Null	end
0w 0d 0h 1m	Console	Null	ip address 192.168.1.1 255.255.255.0
0w 0d 0h 0m	Console	Null	in v 1
0w 0d 0h 0m	Console	Null	telnet-server enable

9.1.11 show memory usage

Command: show memory [usage]

Function: Display the contents in the memory.

Parameter: usage means memory use information.

Command mode: Admin Mode

Usage Guide: This command is used for switch debug purposes. The command will interactively prompt the user to enter start address of the desired information in the memory and output word number. The displayed information consists of three parts: address, Hex view of the information and character view.

Example:

Switch#show memory
start address : 0x2100
number of words[64]:

```
002100:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002110:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002120:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002130:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002140:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002150:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002160:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002170:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
```

9.1.12 show running-config

Command: show running-config
Function: Display the current active configuration parameters for the switch.
Default: If the active configuration parameters are the same as the default operating parameters, nothing will be displayed.
Command mode: Admin Mode
Usage Guide: When the user finishes a set of configuration and needs to verify the configuration, show running-config command can be used to display the current active parameters.
Example:
Switch#show running-config

9.1.13 show running-config current-mode

Command: show running-config current-mode
Function: Show the configuration under the current mode.
Command mode: All configuration modes.
Default: None.
Usage Guide: Enter into any configuration mode and input this command under this mode, it can show all the configurations under the current mode.
Example:

```
 Switch(config-if-ethernet1/0/1)#show run c
!
Interface Ethernet1/0/1
switchport access vlan 2
!
```

9.1.14 show startup-config

Command: show startup-config
Function: Display the switch parameter configurations written into the Flash memory at the current operation; those are usually also the configuration files used for the next power-up.
Default: If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.
Command mode: Admin Mode
Usage Guide: The **show running-config** command differs from **show startup-config** in that when the user finishes a set of configurations, **show running-config** displays the added-on configurations whilst **show startup-config** won't display any configurations. However, if **write** command is executed to save the active configuration to the Flash memory, the displays of **show running-config** and **show startup-config** will be the same.

9.1.15 show switchport interface

Command: show switchport interface [ethernet *<IFNAME>*]

Function: Show the VLAN port mode, VLAN number and Trunk port messages of the VLAN port mode on the switch.

Parameter: ***<IFNAME>*** is the port number.

Command mode: Admin mode

Example: Show VLAN messages of port ethernet 1/0/1.

Switch#show switchport interface ethernet 1/0/1

Ethernet1/0/1

Type :Universal

Mac addr num : No limit

Mode :Trunk

Port VID :1

Trunk allowed Vlan :ALL

Displayed Information	Description
Ethernet1/0/1	Corresponding interface number of the Ethernet.
Type	Current interface type.
Mac addr num	Numbers of interfaces with MAC address learning ability.
Mode: Trunk	Current interface VLAN mode.
Port VID :1	Current VLAN number the interface belongs.
Trunk allowed Vlan :ALL	VLAN permitted by Trunk.

9.1.16 show tcp

Command: show tcp

Function: Display the current TCP connection status established to the switch.

Command mode: Admin Mode

Example:

Switch#show tcp

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	23	0.0.0.0	0	LISTEN
0.0.0.0	80	0.0.0.0	0	LISTEN

Displayed information	Description
LocalAddress	Local address of the TCP connection.
LocalPort	Local pot number of the TCP connection.
ForeignAddress	Remote address of the TCP connection.
ForeignPort	Remote port number of the TCP connection.
State	Current status of the TCP connection.

9.1.17 show tcp ipv6

Command: show tcp ipv6

Function: Show the current TCP connection.

Command mode: Admin and configuration mode.

Example:

Switch#show tcp ipv6

LocalAddress LocalPort RemoteAddress RemotePort State IF VRF

:: *80* :: 0 LISTEN 0 0

:: 23 :: 0 LISTEN 0 0

Displayed Information	Explanation
LocalAddress	Local IPv6 address of TCP connection
LocalPort	Local port of TCP connection
RemoteAddress	Remote IPv6 address of TCP connection
RemotePort	Remote Port of TCP connection
State	The current state of TCP connection
IF	Local port index of TCP connection
VRF	Virtual route forward instance

9.1.18 show telnet login

Command: show telnet login

Function: List information of currently available telnet clients which are connected to the switch.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: This command used to list the information of currently available telnet clients which are connected to the switch.

Example:

Switch#show telnet login

Authenticate login by local.

Login user:

aa

9.1.19 show temperature

命令：show temperature

功能： 显示交换机 CPU 当前温度。

参数： 无。

命令模式： 各种配置模式

使用指南： 该命令用于监测交换机 CPU 的温度。

举例： 显示交换机 CPU 当前温度。

Switch(Config)#show temperature

Temperature: 47.0625 ℃

9.1.20 show tech-support

Command: show tech-support

Function: Display various information about the switch and the running tasks. This command is used to diagnose the switch by the technical support specialist.

Command Mode: Admin mode and configuration mode

Usage Guide: When failure occurred on the switch, this command can be used to get related information, in order to diagnose the problems.

Example:

Switch#show tech-support

9.1.21 show udp

Command: show udp

Function: Display the current UDP connection status established to the switch.

Command mode: Admin Mode

Example:

Switch#show udp

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	161	0.0.0.0	0	CLOSED
0.0.0.0	123	0.0.0.0	0	CLOSED
0.0.0.0	1985	0.0.0.0	0	CLOSED

Displayed information	Description
LocalAddress	Local address of the UDP connection.
LocalPort	Local pot number of the UDP connection.
ForeignAddress	Remote address of the UDP connection.
ForeignPort	Remote port number of the UDP connection.
State	Current status of the UDP connection.

9.1.22 show udp ipv6

Command: show udp ipv6

Function*:* Show the current UDP connection.

Command mode: Admin and configuration mode.

Example:

LocalAddress	LocalPort	RemoteAddress	RemotePort	State
::	69	::	0	CLOSED
::	1208	::	0	CLOSED

Displayed Information	Explanation
LocalAddress	Local IPv6 address of UDP connection
LocalPort	Local port of UDP connection
RemoteAddress	Remote IPv6 address of UDP connection
RemotePort	Remote Port of UDP connection
State	The current state of UDP connection

9.1.23 show version

Command: show version

Function: Display the switch version.

Command mode: Admin Mode

Usage Guide: Use this command to view the version information for the switch, including hardware version and software version.

Example:

Switch#show version

9.1.24 traceroute

Command: traceroute [source <*ipv4-addr*>] vrf <vrfname> { <*ip-addr*> | host <*hostname*> |[ethernet target-mac <mac-address>| target-mep <1-4094> domain WORD server (WORD) (number <0-65535>) |(pvlan <1-4094 >) fdb-only|source|ttl] } [hops <*hops*>] [timeout <*timeout*>]

Function: This command is tests the gateway passed in the route of a packet from the source device to the target device. This can be used to test connectivity and locate a failed sector.

Parameter: *<ipv4-addr>* is the assigned source host IPv4 address in dot decimal format. ***<ip-addr>*** is the target host IP address in dot decimal format. ***<hostname>*** is the hostname for the remote host. ***<hops>*** is the maximum gateway number allowed by Traceroute command. ***<timeout>*** Is the timeout value for test packets in milliseconds, between 100 -10000,<vrfname> is vrf instance name.

Default: The default maximum gateway number is 30, timeout in 2000 ms.

Command mode: Admin Mode

Usage Guide: Traceroute is usually used to locate the problem for unreachable network nodes.

9.1.25 traceroute6

Command: traceroute6 *[*source <addr>*]* {<ipv6-addr> | host <hostname>} *[hops* <hops>] *[timeout* <timeout>]

Function: This command is for testing the gateways passed by the data packets from the source device to the destination device, so to check the accessibility of the network and further locating the network failure.

Parameter*: <addr>* is the assigned source host IPv6 address in colonned hex notation. ***<ipv6-addr>*** is the IPv6 address of the destination host, shown in colonned hex notation; ***<hostname>*** is the name of the remote host; ***<hops>*** is the max number of the gateways the traceroute6 passed through, ranging between 1-255; ***<timeout>*** is the timeout period of the data packets, shown in millisecond and ranging between 100~10000.

Default: Default number of the gateways passes by the data packets is 30, and timeout period is defaulted at 2000ms.

Command Mode: Admin Mode

Usage Guide: Traceroute6 is normally used to locate destination network inaccessible failures.

Example:

Switch# traceroute6 2004:1:2:3::4

Relevant Command: ipv6 host

9.2 Logging

9.2.1 logging executed-commands

Command: logging executed-commands {enable | disable}

Function: Enable or disable the logging executed-commands.

Parameter: None.

Command Mode: Global mode.

Default: Disable state.

Usage Guide: After enable this command, the commands executed by user at the console, telnet or ssh terminal will record the log.

Example: Enable the command executed by user.

Switch(Config)#logging executed-commands enable

9.2.2 show logging executed-commands state

Command: show logging executed-commands state

Function: Show the state of logging executed-commands.

Parameter: None.

Command Mode: Admin mode.

Default: None.

Usage Guide: Use this command to display the state (enable or disable).

Example:

Switch#show logging executed-commands state

Logging executed command state is enable

9.2.3 clear logging

This command is not supported by the switch.

9.2.4 logging

no

9.2.5 logging loghost sequence-number

This command is not supported by the switch.

9.2.6 logging source-ip

This command is not supported by the switch.

9.2.7 show logging buffered

This command is not supported by the switch.

9.2.8 show logging executed-commands state

This command is not supported by the switch.

9.2.9 show logging source

This command is not supported by the switch.

9.3 Reload Switch after Specified Time

9.3.1 reload after

Command: reload after {[<*HH:MM:SS*>] [days <*days*>]}
Function: Reload the switch after a specified period of time.
Parameters: ***<HH:MM:SS>*** the specified time, HH (hours) ranges from 0 to 23, MM (minutes) and SS (seconds) range from 0 to 59.

<days> the specified days, unit is day, range from 1 to 30.

time and day may be configured at the same time or configured solely.

Command Mode: Admin mode

Usage Guide: With this command, users can reboot the switch without shutdown its power after a specified period of time, usually when updating the switch version. The switch can be rebooted after a period of time instead of immediately after its version being updated successfully. This command will not be reserved, which means that it only has one-time effect. After this command is configured, it will prompt the reboot information when user logging in the switch by telnet.

Example: Set the switch to automatically reload after 2 days, 10 hours and 1 second.

Switch#reload after 10:00:01 days 2

Process with reboot after? [Y/N] y

Related Commands: reload, reload cancel, show reload

9.3.2 reload cancel

Command: reload cancel

Function: Cancel the specified time period to reload the switch.

Parameters: None

Command Mode: Admin mode.

Usage Guide: With this command, users can cancel the specified time period to reload the switch, that is, to cancel the configuration of command “reload after”. This command will not be reserved.

Example: Prevent the switch to automatically reboot after the specified time.

Switch#reload cancel

Reload cancel successful.

Related Commands: reload, reload after, show reload

9.3.3 show reload

Command: show reload

Function: Display the user’s configuration of command “reload after”.

Parameters: None.

Command Mode: Admin and configuration mode

Usage Guide: With this command, users can view the configuration of command “reload after” and check how long a time is left before rebooting the switch.

Example: View the configuration of command “reload after”. In the following case, the user set the switch to be rebooted in 10 hours and 1 second, and there are still 9 hours 59 minutes and 48 seconds left before rebooting it.

Switch#show reload

The original reload after configuration is 10:00:01.

System will be rebooted after 09:59:48 from now.

Related Commands: reload, reload after, reload cancel

9.4 Debugging and Diagnosis for Packets Received and Sent by CPU

9.4.1 clear cpu-rx-stat protocol

Command: clear cpu-rx-stat protocol[<protocol-type>]

Function: Clear the statistics of the CPU received packets of the protocol type.

Parameter: ***<protocol-type>*** is the type of the protocol of the packet**,** including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh, bgp, bgp4plus, rip, ripng, ospf, ospfv3, pim, pimv6, unknownnnnn-mcast, unknownnnn-mcast6, mld

Command Mode: Global Mode

Usage Guide: This command clear the statistics of the CPU received packets of the protocol type, it is supposed to be used with the help of the technical support.

Example: Clear the statistics of the CPU receives ARP packets.

Switch#clear cpu-rx-stat protocol arp

9.4.2 cpu-rx-limitnotify enable interval

Command: cpu-rx-limitnotify enable interval<180-86400>

no cpu-rx-limitnotify **enable**

Function: Enable cpu-rxlimitnotify function and specified the time interval of trigger. The no command disables cpu-rxlimitnotify function.

Parameters: ***interval*** interval time, the default time is 86400s.

Command Mode: Configuration mode.

Usage Guide: This command used for diagnosing protocol information that switch received. Please using under the guidance of manufacturer technical staff

Example:

Switch(config)#cpu-rx-limitnotify enable interval 180

9.4.3 cpu-rx-limitnotify protocol (all|WORD)(enable|disable)

Command: cpu-rx-limitnotify protocol (all|WORD)(enable|disable**)**

Function: Open or close all protocols or specified protocols. After open, cpu-rx-limitnotify detected cpu-rx happened deny in interval period, sending the deny amount in the time to users

by snmp trap.

Command Mode: Configuration mode.

Example:

Close all protocols

Switch(config)# cpu-rx-limitnotify protocol all disable

Open all protocols

Switch(config)# cpu-rx-limitnotify protocol all enable

Open specified protocols

Switch(config)# cpu-rx-limitnotify protocol snmp enable

Close specified protocols

Switch(config)# cpu-rx-limitnotify protocol snmp disable

9.4.4 cpu-rx-ratelimit channel

This command is not supported by the switch.

9.4.5 cpu-rx-ratelimit enhanced

Command： cpu-rx-ratelimit enhanced

no cpu-rx-ratelimit enhanced

Function：Enable CPU speed limit enhancement feature. The 'no' command disables the enhanced speed limit for CPU packet reception

Parameter： none

Command Mode： Config mode.

Usage Guide：This command is used to restrict the protocol information received by the switch. Please use under the guidance of the manufacturer's technical personnel.

Example： Configure CPU packet reception **received limit** enhancement

Switch(config)#cpu-rx-ratelimit enhanced

9.4.6 cpu-rx-ratelimit protocol

Command: cpu-rx-ratelimit protocol <*protocol-type*> <*packets*>

no cpu-rx-ratelimit protocol <*protocol-type*>

Function: Set the max rate of the CPU receiving packets of the protocol type, the no command set the max rate to default.

Parameter: <protocol-type> is the type of the protocol, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh; <packets> is the max rate of CPU receiving packets of the protocol type, ***its range*** is 1-2000 pps.

Command Mode: Global Mode

Default: A different default rate is set for the different type of protocol.

Usage Guide: The rate limit set by this command have an effect on CPU receiving packets, so it is

supposed to be used with the help of the technical support.
Example: Set the rate of the ARP packets to 500pps.
Switch(config)#cpu-rx-ratelimit protocol arp 500

9.4.7 cpu-rx-ratelimit queue-length

This command is not supported by the switch.

9.4.8 cpu-rx-ratelimit total

Command: cpu-rx-ratelimit total <*packets*>
no cpu-rx-ratelimit total
Function: Set the total rate of the CPU receiving packets, the no command sets the total rate of the CPU receiving packets to default.
Parameter: <packets> is the max number of CPU receiving packets per second.
Command Mode: Global Mode
Default: 1200pps.
Usage Guide: The total rate set by the command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.
Example: Set the total rate of the CPU receive packets to 1500pps.
Switch(config)#cpu-rx-ratelimit total 1500

9.4.9 debug driver

Command: debug driver {receive | send} [interface {<*interface-name*> | all}] [protocol {<*protocol-type*> | discard | all}] [detail]
no debug driver {receive | send}
Function: Turn on the on-off of showing the information of the CPU receiving or sending packets, the "**no debug driver {receive | send}**" command turns off the on-off.
Parameter: receive | send show the information of receiving or sending packets;
interface {<*interface-list*>| all}: interface-list is the Ethernet port number, **all** indicate all the Ethernet ports.
protocol {<*protocol-type*> | discard | all}: protocol-type is the type of the protocol of the packet, including snmp, telnet, http, dhcp, igmp, hsrp, arp, bgp, rip, ospf, pim, ssh, vrrp, ripng, ospfv3, pimv6, icmpv6, bgp4plus, unknownnnnn-mcast, unknownnnnn-mcast6, ttl0-2cpu, isis, dot1x, gvrp, stp, lacp, cluster, mld, vrrpv3, ra, uldp, lldp, eapou **all** means all of the protocol types, **discard** means all the discarded packets. **Detail** show detail information.
Command Mode: Admin Mode
Usage Guide: This command is used to debug, it is supposed to be used with the help of the technical support.
Example: Turn on the on-off for showing the receiving packets.
Switch#debug driver receive

9.4.10 protocol filter

Command: protocol filter {protocol-type}
no Protocol filter **{protocol-type}**
Function: Turn on/off the corresponding treatment of the named protocol packets.
Parameter: ***<protocol-type>*** stands for protocol type, it can be configured:
{arp|bgp|dhcp|dhcpv6|hsrp|http|igmp|ip|ldp|mpls|ospf|pim|rip|snmp|telnet|vrrp}
Command Mode: Admin Mode
Usage Guide: This command turns on/off the corresponding treatment of the named protocol packets, and it is used to debug and diagnose the switch. Please use it with direction of the manufacturers technical personnel.
Example: Turn on the treatment of the arp protocol packets.
Switch#protocol filter arp

9.4.11 show cpu-rx protocol

Command: show cpu-rx protocol [*<protocol-type>*]
Function: Show the statistics of the CPU received packets of the specified protocol type.
Parameter: ***<protocol- type>*** is the protocol type of the packets, if do not input parameters, show all statistic packets.
Command Mode: Admin and configuration mode
Default: None.
Usage Guide: This command is used to debug, it is supposed to be used with the help of the technical support.
Example: Show the statistics of CPU receiving ARP packets.
Switch#show cpu-rx protocol arp

Type	Rate-limit	TotPkts	CurState
arp	500	3	allowed

9.5 CPU-Protect

9.5.1 cpu-protect enable

Command: cpu-protect enable
no cpu-protect enable
Function: This command will enable cpu-protect function on the switch, the no operation of this command will disable that function.
Parameters: None.
Default: Disable.
Command Mode: Global Configuration Mode.
Usage Guide: cpu-protect enable is used to enable the cpu-protect function, the no operation

of this command is used to disable that function.
Example: Enable the cpu-protect function.
Switch(Config)# cpu-protect enable

9.5.2 cpu-protect log enable

Command: cpu-protect log enable
no cpu-protect log enable
Function: This command will enable cpu-protect logging function on the switch, the no operation of this command will disable that function.
Parameters: None.
Default: Disable.
Command Mode: Global Configuration Mode.
Usage Guide: cpu-protect log enable is used to enable the cpu-protect logging function, the no operation of this command is used to disable that function.
Example: Enable the cpu-protect logging function.
Switch(Config)#cpu-protect log enable

9.5.3 cpu-protect trap enable

Command: cpu-protect trap enable
no cpu-protect trap enable
Function: This command will enable cpu-protect trap alarm function on the switch, the no operation of this command will disable that function.
Parameters: None.
Default: Disable.
Command Mode: Global Configuration Mode.
Usage Guide: cpu-protect trap enable is used to enable the cpu-protect trap alarm function, the no operation of this command is used to disable that function.
Example: Enable the cpu-protect trap alarm function.
Switch(Config)# cpu-protect trap enable

9.5.4 cpu-protect interval

Command: cpu-protect interval <time>
no cpu-protect interval
Function: Configure the cpu-protect sampling period.
Parameters: time is sampling interval, range is 1-10s.
Default: 3.
Command Mode: Global Configuration Mode.
Usage Guide: cpu-protect interval is used to configure the cpu-protect sampling period, the no operation of this command is used to restore the sampling period to the default value.
Example: Set the cpu-protect sampling period to 5s

Switch(Config)# cpu-protect interval 5

9.5.5 cpu-protect recovery-time

Command: cpu-protect recovery-time <time>

no cpu-protect recovery-time

Function: Configure the cpu-protect policy recovery period.

Parameters: time is recovery period, range is 1-3000s.

Default: 60.

Command Mode: Global Configuration Mode.

Usage Guide: cpu-protect recovery-time is used to configure the cpu-protect policy recovery period, the no operation of this command is used to restore the recovery period to the default value.

Example: Set the cpu-protect policy recovery period to 100s

Switch(config)#cpu-protect recovery-time 100

9.5.6 cpu-protect threshold

Command: cpu-protect (protocol <WORD>|per-ip|per-mac) threshold <pps> action (none|speed-limit)

no cpu-protect (protocol <WORD>|per-ip|per-mac) threshold

Function: Configure the upper limit of the rate of sending CPU for a stream (protocol type, IP address or MAC address).

Parameters: WORD is the protocol type. At present, the supported protocol types are ARP / IP / ICMP / IGMP / DHCP.

pps is the upper limit of the rate of sending CPU. The range is shown in the range column of the following table, and the unit is packet / s.

none means no rate-limiting action after overrun, only log, send trap alarm and record attack source list; speed-limit means to perform rate-limiting action, log, send trap alarm and record attack source list after overrun.

Default: The default threshold is shown in the default column of the following table and the unit is packet / s.The default action is speed-limit after overrun.

Protocal	Default	Range
ARP	300	10/20～800
IP	300	10/20～800
ICMP	80	10/20～800
IGMP	150	10/20～800
DHCP	150	10/20～800
specific host（IP）	400	10/20～800
specific host（MAC）	400	10/20～800

Command Mode: Global Configuration Mode.

Usage Guide: cpu-protect threshold is used to configure the upper limit of the rate of sending CPU for a stream, the no operation of this command is used to restore the threshold to the

default value.

Example: Set the upper limit of the rate of sending CPU for ARP packet to 500 and set the action to none after overrun.

Switch(Config)# cpu-protect protocal arp threshold 500 action none

9.5.7 cpu-protect limit-speed

Command: cpu-protect (protocol <WORD>|per-ip|per-mac) limit-speed <pps>

no cpu-protect (protocol <WORD>|per-ip|per-mac) limit-speed

Function: Configure the rate-limiting value of sending CPU for a stream (protocol type, IP address or MAC address) after overrun.

Parameters: WORD is the protocol type. At present, the supported protocol types are ARP / IP / ICMP / IGMP / DHCP.

pps is the rate-limiting value of sending CPU after overrun. The range is shown in the range column of the following table, and the unit is packet / s.

Default: The default threshold is shown in the default column of the following table and the unit is packet / s.

Protocal	Default	Range
ARP	150/200	10/20～250
IP	150/200	10/20～250
ICMP	50/50	10/20～250
IGMP	80/100	10/20～250
DHCP	80/100	10/20～250
specific host（IP）	200/250	10/20～300
specific host（MAC）	200/250	10/20～300

Command Mode: Global Configuration Mode.

Usage Guide: cpu-protect limit-speed is used to configure the rate-limiting value of sending CPU for a stream after overrun, the no operation of this command is used to restore the rate-limiting value to the default value.

Example: Set the rate-limiting value of sending CPU for ARP packet to 100 after overrun.

Switch(config)#cpu-protect protocal arp limit-speed 100

9.5.8 show cpu-protect attack-list

Command: show cpu-protect attack-list (detail|top)

Function: Show the attack source information detected by cpu-protect module.

Parameters: detail means to show all attack source table items, and top means only the TOP10 items of attack source table are displayed.

Default: None.

Command Mode: Admin and configuration mode.

Usage Guide: Show the attack source information detected by cpu-protect module.

Example: Display the TOP10 items of attack source table.

Switch# show cpu-protect attack-list top

Attack Num Total: 1

Type	Item-Info	AttackTimes	Port	VLAN-LIST	Speed	State
Protocal	ARP	5	Ethernet1/0/1	1	64	Speed-Limit

9.5.9 show cpu-protect running-config

Command: show cpu-protect running-config
Function: Show the configuration and operation information of cpu-protect module.
Parameters: None.
Default: None.
Command Mode: Admin and configuration mode.
Usage Guide: Show the configuration and operation information of cpu-protect module.
Example: Show the configuration and operation information of cpu-protect module.
Switch# show cpu-protect running-config
Cpu-Protect Globle: enable
Cpu-Protect trap : enable
Cpu-Protect Log: enable
Cpu-Protect Interval: 3
Cpu-Protect Recovery-Time: 60

Cap-Num	Ip-Num	Mac-Num	Protocal-Num
0	0	0	0

Stream	Threshould	Limit-Speed	Action
IP	300	150	Speed-Limit
DHCP	150	80	Speed-Limit
IGMP	150	80	Speed-Limit
ARP	300	150	Speed-Limit
ICMP	80	50	Speed-Limit
PER-IP	400	200	Speed-Limit
PER-MAC	400	200	Speed-Limit

9.6 Info-Center

9.6.1 info-center enable

Command：

info-center enable

no info-center enable

Functions: Information center output enable

Parameters:

Command mode: Global configuration mode

Default: Enable

Usage Guide:

This command is responsible for enabling information center output.The information center can still be configured with or without output enabled.That is, the command is a switch that controls the information output of the information center.Disabling can turn off the information output and the original configuration will still be in effect after enabling again.

Examples:

Switch(config)#info-center enable

Switch(config)#no info-center enable

9.6.2 info-center prefix

Command：

info-center (console | logbuffer | monitor | trapbuffer) prefix (on|off)

info-center (logfile <1-4> | loghost <1-8>) prefix (on|off) (member <1-16> |)

Functions: Configure whether to carry the log record prefix

Parameters:

Parameter	Description
console | logbuffer | monitor | logfile <1-4> | loghost <1-8> | trapbuffer	**Represents the output direction to be configured**
on|off	**Switch of carrying the log record prefix**
member <1-16>	**Member ID**

Command mode: Global configuration mode

Default: Enable

Usage Guide:

The command turns on or off the log prefix for each direction. By default, the prefix is on for all directions.

Examples:

Switch(config)# info-center console prefix on

9.6.3 info-center match

Command：info-center (console | logbuffer | monitor | trapbuffer) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact |) (keyword WORD |)
info-center (logfile <1-4> | loghost <1-8>) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact) (keyword WORD |) (member <1-16> |)
no info-center (console | logbuffer | monitor | trapbuffer) match
no info-center (logfile <1-4> | loghost <1-8>) match (member <1-16>)
Functions: Configure the output direction log matching condition
Parameters:

Parameter	Description
console | logbuffer | monitor | logfile <1-4> | loghost <1-8> | trapbuffer	Represents the output direction to be configured
emergencies | alerts | critical | errors | warnings | notifications | informational | debugging	Configure the matching information level
exact	Strict level matching
keyword WORD	Use regular expressions as brush selection criteria
member <1-16>	Member ID

Command mode: Global configuration mode
Default: Enable
Usage Guide:

This command sets the matching condition of logs in each direction. Behind match, you can directly configure which level of logs are allowed to enter, and you can also configure exact level matching.So-called strictly match, what grade is set, only match what level, if without exact, the order of matching levels in turn is emergencies, alerts, critical, errors, warnings, notifications, informational, debugging, also can use the keyword followed a regular expression.

The no command cancels the matching condition for the corresponding output direction.

Examples:
Sysname(config)#info-center console match level warnings exact
Sysname(config)#info-center logfile 1 match level errors

9.6.4 info-center output-enable

Command：**info-center (console | logbuffer | monitor | trapbuffer) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact |) (keyword WORD |)**

info-center (logfile <1-4> | loghost <1-8>) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact) (keyword WORD |) (member <1-16> |)

no info-center (console | logbuffer | monitor | trapbuffer) match

no info-center (logfile <1-4> | loghost <1-8>) match (member <1-16>)

Functions: Configure the output direction enable

Parameters:

Parameter	Description
console | logbuffer | monitor | logfile <1-4> | loghost <1-8> | trapbuffer	**Represents the output direction to be configured**
member <1-16>	**Member ID**

Command mode: Global configuration mode

Default: Enable

Usage Guide:

This command configures enabling in one of the output directions. Note that this command is only enabling/disabling and does not affect the matching condition or other configuration. When the direction is enabled again, the previously configuration is still valid.

Note that console, monitor, logbuffer, trapbuffer and logfile 4 are enabled by default, and the others are disabled by default.Here logfile 4 is used as the output direction of the default logfile, so it is enabled by default.

Examples:

Sysname(config)#info-center monitor output-enable

Sysname(config)#info-center logfile 1 output-enable

9.6.5 info-center record-cmd

Command: info-center (logbuffer | logfile <1-4> | loghost <1-8>) record-cmd

no info-center (logbuffer | logfile <1-4> | loghost <1-8>) record-cmd

Functions: Configure log user execution commands

Parameters:

Parameter	Description
logbuffer | logfile <1-4> | loghost <1-8>	**Represents the output direction to be configured**

Command mode: Global configuration mode

Default: Disable

Usage Guide:

This command records user execution commands in a certain direction.Note that the command line recording operation is not bound by the matching condition in that direction and can be recorded as long as the output direction is enabled.User execution commands are not logged by default.

Examples:

Sysname(config)#info-center logbuffer record-cmd

9.6.6 info-center loghost

Command: info-center loghost <1-8> config (vrf <vrfname>|A.B.C.D | X:X::X:X) facility (local0|local1|local2|local3|local4|local5|local6|local7) (member <1-16> |)

no info-center loghost <1-8> config (member <1-16> |)

Functions: Configure the IP and facility of the log host

Parameters:

Parameter	Description
loghost <1-8>	**Represents the configuration of loghost output direction**
A.B.C.D | X:X::X:X	**IP address of Log host**
local0|local1|local2|local3|local4|local5|local6|local7	**Optional facility local0~7**
member <1-16>	**Member ID**
<vrfname>	**Vrf instance name**

Command mode: Global configuration mode

Default: Disable

Usage Guide:

This command configures the IP address and facility of loghost.

The no command is used to cancel the IP address and facility configuration for the corresponding loghost.if use in vsf mode,you need to add member at the end of the line.

Examples:

Sysname(config)#info-center loghost 1 config 192.168.1.1 facility local0

9.6.7 info-center logfile

Command: info-center logfile <1-4> config count <1-40960> (flash|usb|mmc) WORD (member <1-16> |)

no info-center logfile <1-4> config (member <1-16> |)

Functions: Configure the number of log files and access paths

Parameters:

Parameter	Description
logfile <1-4>	Represents the configuration of logfile output direction
count <1-40960>	The number of log files
flash|usb|mmc	Optional access path
WORD	Log file name
member <1-16>	Member ID

Command mode: Global configuration mode

Default: Disable

Usage Guide:

This command configures the number of log files and the access path.For the default logfile, the system uses logfile 4 as the default output direction. If there is a mmc device, the default storage path is mmc. Otherwise, the default storage path is flash.In this way, under the default configuration, the log information of the single board before power failure can still be viewed from the mainboard by using the “show info-center logfile” command after the single board is restarted. if use in vsf mode,you need to add member at the end of the line.

The no command is used to cancel the number and access path configuration of the logfile.

Examples:

Sysname(config)#info-center logfile 1 config count 40960 flash logfile.log

9.6.8 info-center clear

Command: info-center clear trapbuffer

info-center clear logbuffer (member <1-16> |)

Functions: Delete all logs logged by logbuffer or trapbuffer in the information center

Parameters:

Parameter	Description
logbuffer|trapbuffer	Optional output direction for clearing log
member <1-16>	Member ID

Command mode: Global configuration mode

Default: Disable

Usage Guide:

This command deletes all logs logged by logbuffer or trapbuffer in the information center.

Examples:

Sysname(config)#info-center clear logbuffer

Sysname(config)#info-center clear trapbuffer

9.6.9 show info-center config

Command：show info-center config

Functions：Display the current configuration of the information center

Parameters:

Command mode: All mode

Default: Disable

Usage Guide:

This command displays all the current configurations of the information center.

Examples:

SW1(config)#show info-center config
info-center enable
info-center sync enable
info-center console output-enable
info-center monitor output-enable
info-center trapbuffer output-enable
info-center logbuffer output-enable
info-center logfile 4 config count 40960 mmc logfile.log
info-center logfile 4 output-enable
info-center console match level warnings
info-center console prefix on
info-center monitor match level debugging
info-center monitor prefix on
info-center trapbuffer prefix on
info-center logbuffer match level warnings
info-center logbuffer prefix on
info-center loghost 1 prefix on
info-center loghost 2 prefix on
info-center loghost 3 prefix on
info-center loghost 4 prefix on
info-center loghost 5 prefix on
info-center loghost 6 prefix on
info-center loghost 7 prefix on
info-center loghost 8 prefix on
info-center logfile 1 prefix on
info-center logfile 2 prefix on
info-center logfile 3 prefix on
info-center logfile 4 match level warnings
info-center logfile 4 prefix on

9.6.10 show info-center logbuffer

Command: show info-center logbuffer ((keyword WORD)|) (member <1-16> |)

Functions: Display the contents of the logbuffer output direction

Parameters:

Parameter	Description
keyword WORD	Use regular expressions as brush selection criteria
member <1-16>	Member ID

Command mode: All mode

Default: Disable

Usage Guide:

This command displays the contents of the logbuffer output direction, and can be filtered by using regular expressions.

Note that there is no single command for displaying user operation commands, and all the operation commands have been added CMD: characters to the string, which can be used as a keyword for filtering. if use in vsf mode,you need to add member at the end of the line.

Examples:

```
Sysname(config)#show info-center logbuffer
severity: 1-emergencies 2-alerts 3-critical 4-errors 5-warnings 6-notifications
7-informational 8-debugging
Allowed max messages:2000,Current messages:51
51 Jan 25 11:43:21:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state
to UP
50 Jan 25 11:43:20:000 2019 SNR-S2995G-12FX
MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1,
changed state to UP
49 Jan 25 11:43:07:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state
to DOWN
48 Jan 25 11:43:06:000 2019 SNR-S2995G-12FX
MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1,
changed state to DOWN
47 Jan 25 11:38:22:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state
to UP
46 Jan 25 11:38:21:000 2019 SNR-S2995G-12FX
MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1,
changed state to UP
45 Jan 25 11:38:08:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state
to DOWN
44 Jan 25 11:38:07:000 2019 SNR-S2995G-12FX
MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1,
changed state to DOWN
43 Jan 25 11:29:33:000 2019 SNR-S2995G-12FX DEFAULT/2/:System cold restart...
42 Jan 25 11:28:36:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state
to UP
...
----finish show log buffer----
```

9.6.11 show info-center trapbuffer

Command:

Functions: Display the contents of the output direction of the trapbuffer

Parameters:

Parameter	Description
keyword WORD	Use regular expressions as brush selection criteria

Command mode: All mode

Default: Disable

Usage Guide:

This command displays the contents of the trapbuffer output direction, and can be filtered by using regular expressions.

Examples:

Sysname(config)#show info-center trapbuffer
severity: 1-emergencies 2-alerts 3-critical 4-errors 5-warnings 6-notifications
7-informational 8-debugging
Allowed max messages:2000,Current messages:44
44 Jan 25 11:43:21:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP
43 Jan 25 11:43:20:000 2019 SNR-S2995G-12FX
MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1, changed state to UP
42 Jan 25 11:43:07:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to DOWN
41 Jan 25 11:43:06:000 2019 SNR-S2995G-12FX
MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1, changed state to DOWN
40 Jan 25 11:38:22:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP
39 Jan 25 11:38:21:000 2019 SNR-S2995G-12FX
MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1, changed state to UP
38 Jan 25 11:38:08:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to DOWN
37 Jan 25 11:38:07:000 2019 SNR-S2995G-12FX
MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1, changed state to DOWN
36 Jan 25 11:29:33:000 2019 SNR-S2995G-12FX DEFAULT/2/:System cold restart...

35 Jan 25 11:28:36:000 2019 SNR-S2995G-12FX
DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP
.....
----finish show trap buffer----

9.6.12 show info-center logfile

Command:

Functions: Display the contents of the logfile output direction

Parameters:

Parameter	Description
logfile <1-4>	Optional logfile output direction
keyword WORD	Use regular expressions as brush selection criteria
member <1-16>	Member ID

Command mode: All mode

Default: Disable

Usage Guide:

This command displays the contents of the logfile output direction, and can be filtered by using regular expressions.

Note that there is no single command for displaying user operation commands, and all the operation commands have been added CMD: characters to the string, which can be used as a keyword for filtering. if use in vsf mode,you need to add member at the end of the line.

Examples:

Sysname(config)#show info-center logfile 1
severity: 1-emergencies 2-alerts 3-critical 4-errors 5-warnings 6-notifications 7-informational 8-debugging
55 Dec 18 14:47:22:000 2018 ECS8830F/ECS8854F MODULE_UTILS_FILESYSTEM/2/:fs_write_file 2167: FS_DEV_UNLOCK Slot: 1 dev_name:flash: file_name:flash:/board_web_language
54 Dec 18 14:47:22:000 2018 ECS8830F/ECS8854F MODULE_UTILS_FILESYSTEM/2/:fs_write_file 2149: FS_DEV_LOCK_NO_WAIT Slot: 1 dev_name:flash: file_name:flash:/board_web_language
53 Dec 18 14:47:16:000 2018 ECS8830F/ECS8854F MODULE_MANAGEINTF/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to DOWN
52 Dec 18 14:47:16:000 2018 ECS8830F/ECS8854F MODULE_MANAGEINTF/5/:%LINK-5-CHANGED: Interface Ethernet0, changed state to UP
51 Dec 18 14:47:16:000 2018 ECS8830F/ECS8854F DEFAULT/3/:Clock between master and slave has been synchronized!
50 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:topo success! vsf

done 1 state ALIVE master 00-03-0f-aa-aa-ab seq 0 local seq 0
49 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:disc success! cpu num 1 vsf done 0 state TOPO master 00-03-0f-aa-aa-ab seq 0 pri 0x4000207f local seq 0 pri 0x4000207f
48 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:Master 00-03-0f-aa-aa-ab mid 1 pri 0x4000207f seq 0
47 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:vsf_proto_handle_start 2448: vsf done 0 local seq 0 pri 0x207f
.....
----finish show log file----

9.6.13 info-center list all disk

Command: info-center list all disk
Functions: View the disks that support storing files in the information center
Parameters:
Command mode: Global configuration mode
Default: Disable
Usage Guide:

This command is used to view the disks that support storing files in the information center. Supported areas can be flash, usb, and mmc.

Examples:

```
Sysname(config)# info-center list all disk
flash:
usb:
mmc:
```

9.6.14 info-center save all

Command:info-center save all ((flash|usb|mmc) WORD)
Functions: Onekey collecting function of information center
Parameters:

Parameter	Description
flash|usb|mmc	Optional file storage area
WORD	File name

Command mode: Global configuration mode
Default: Disable
Usage Guide:

This command is used for onekey collection in the information center.The collected content is the configuration of the information center, as well as the log information recorded by logbuffer and trapbuffer.When the file path and name are not configured, the collected

information is stored in the default area with the default file name.If there is a mmc device, the default storage path is mmc, otherwise the default storage path is flash, and the default file name is icsaveall.txt.

Examples:

```
Sysname(config)# info-center save all flash saveall.log
*****Now saving Master card(member 1)*****
Now saving infocenter all configuration, please wait..
Now saving infocenter logbuffer content, please wait..
Now saving infocenter trapbuffer content, please wait..
*****Master card(member 1) saving finished!*****
```

9.7 Mirror

9.7.1 monitor session source interface

Command: monitor session *<session>* source {interface *<interface-list>*} *{*rx| tx| both}

no monitor **session *<session>* source {interface *<interface-list>*}**

Function: Specify the *source interface* for the mirror*. The no* form command will disable this configuration.

Parameters: <session> is the session number for the mirror. Currently 1 to 7 is supported. ***<interface-list>*** is the list of source interfaces of the mirror which can be separated by '-' and ';'. **rx** means to filter the datagram received by the interface, while **tx** for the datagram sent out, and **both** means both of income and outcome datagram.

Command mode: Global mode

Usage Guide: This command is used to configure the source interfaces **for *the*** mirror. It is not restricted the source interface of the mirror on the switch. The source can be **one** interface, or can be multiple interfaces. Both of the income and outcome datagram can be mirrored, or they can be mirrored selectively. **If** no [rx | tx | both] is specified, both **are** made to be the default. When **multiple** interfaces are mirrored, the direction of the mirror can be different, but they should be configured separately.

Example: Configure to mirror the datagram sent out by interface 1/0/1-4 and to mirror the datagram received by interface1/0/5

Switch(config)#monitor session 1 source interface ethernet 1/0/1-4 tx

Switch(config)#monitor session 1 source interface ethernet1/0/5 rx

9.7.2 monitor session source interface access-list

Command: monitor session *<session>* source {interface *<interface-list>*} access-list *<num>*

{rx|tx|both}

no monitor **session <*session*> source {interface <*interface-list*>} access-list <*num*>**

Function: Specify the access control for the source of the mirror. The no form command will disable this configuration.

Parameters: <session> is the session number for the mirror. Currently 1 to 7 is supported. <interface-list> is the list of source interfaces of the mirror which can be separated by '-' and ';'. **<*num*>** is the number of the access list. **rx** means to filter the datagram received by the interface. **tx** for the datagram sent out, and **both** means both of income and outcome datagram.

Command Mode: ***Global*** Mode.

Usage Guide: This command is used to configure the source interfaces **for *the*** mirror. It is not restricted the source interface of the mirror on the switch. The source can be ***one*** **interface**, or can be multiple interfaces. For **flow** mirror, only datagram received can be mirrored. The parameters **can** be rx, tx, both. The related access list should be prepared before this command is issued. For how to configure the access list, please refer to ACL configuration. The mirror can only be created after the destination interface of the corresponding session has been configured.

Example: Configure the mirror interface 1/0/6 to filter with access list 120 in session 2.

Switch(config)#monitor session 2 source interface 1/0/6 access-list 120 rx

9.7.3 monitor session destination interface

Command: monitor session <*session*> destination interface <*interface-number*>

no monitor session <*session*> destination interface <*interface-number*>

Function: Specify the destination interface of the mirror. The no form command will disable this configuration.

Parameters: <*session*> is the session number of the mirror, which is currently limited to 1-7. **<*interface-number*>** is the destination interface of the mirror.

Default: None.

Command Mode: Global mode

Usage Guide: 7 destination mirror interface is supported on the switch. To be mentioned. The interface which is configured as the destination of the mirror should not be configured as the member of the interface trunk. And the maximum throughput of the interface is recommended to be larger than the total throughput of the interfaces to be mirrored. If the destination of a session is removed, the mirror path configured in the session will be removed at the same time. And if the destination interface is reconfigured, the interface path will be recovered. To be mentioned, the flow mirror can only be recovered after the destination of the interface is re-configured.

Example: Configure interface 1/0/7 as the destination of the mirror.

Switch(config)#monitor session 1 destination interface ethernet 1/0/7

9.7.4 show monitor

Command: show monitor

Function: To display information about the source and destination ports of all the mirror sessions.

Command Mode: Admin Mode

Usage Guide: This command is used to display the source and destination ports for the configured mirror sessions. For port mirroring and flow mirroring, the mirror mode of the source can be displayed. For MAC mirroring, MAC mirror configuration will be displayed for the supported switch cards.

Example:

Switch#show monitor

9.7.5 mirror sample rate

This command is not *supported* by the switch.

9.8 RSPAN

9.8.1 remote-span

Command: remote-span

no remote-span

Function: To configure VLAN to RSPAN VLAN. The no form of this command will delete the RSPAN VLAN.

Parameter: None.

Command Mode: VLAN Configuration Mode.

Default: Not configured.

Usage Guide: This command is used to configure the existing VLAN as RSPAN VLAN. Dedicated RSPAN VLAN should be configured before RSPAN can function. When configuring RSPAN VLAN, it should be made sure that specialized VLAN, such as the default VLAN, dynamic VLAN, private VLAN, multicast VLAN, and layer 3 interface enabled VLAN, should not be configured as RSPAN VLAN. If any existing sessions are still working when RSPAN is disabled, these sessions will be still working regardless the configuration change. However, if any layer 3 interface is configure in the VLAN after RSPAN is disable, the existing RSPAN session will be stopped.

Example:

Switch(Config-Vlan5)#remote-span

9.8.2 monitor session remote vlan

Command: monitor session <*session*> remote vlan <*vid*>

no monitor session <*session*> remote vlan

Function: To configure local mirror session to RSPAN. The no form of this command will restore the RSPAN to local mirror.

Parameter: <*session*>: session ID, range between 1~7. **<*vid*>:** The id of RSPAN VLAN.

Command Mode: Global Mode.

Default: Not configured.

Usage Guide: To configure local mirror session to RSPAN. The VLAN id is the RSPAN VLAN. The mirrored data grams will be attached with RSPAN tags.

Example:

Switch(config)#monitor session 1 remote vlan 5

9.8.3 monitor session reflector-port

Command: monitor session <*session*> reflector-port <*interface-number*>

no monitor session <*session*> reflector-port <*interface-number*>

Function: To configure reflector port, the no form of this command will delete the reflector port.

Parameter: <*session*>: Session ID, range between 1~7, **<*interface-number*>:** Interface number.

Command Mode: Global Mode.

Default: Not configured.

Usage Guide: This command configures the reflector port for the destination of mirror data grams, and disables the MAC learning function of the specified port. The configuration of reflector port is to change the mode of the local port from the destination port mode to be the reflector mode. Hence, the configuration of reflector port and the destination port are exclusive. The no command is used to restore the reflector port to normal port. The source port, in access or trunk mode, should not be added to RSPAN VLAN. When the reflector port is configured as springboard of CPU TX direction mirroring, it must be configured as TRUNK port and allows the RSPAN VLAN data passing, the Native VLAN should not be configured as RSPAN VLAN. After configured RSPAN, the vlan tag will be added on the packet of the egress mirror. It will cause the abort error frame on the reflection port, so the default MTU value of the switch should be modified.

Example:

Switch(config)#monitor session 1 reflector-port inter ethernet 1/0/3

9.9 ERSPAN

9.9.1 monitor session destination tunnel

Command: monitor session <*session*> destination tunnel <*tunnel-number*> reflector-port <interface-number>

no monitor session <*session*> destination tunnel <*tunnel-number*> reflector-port <interface-number>

Function: Specify the destination port of the mirror as the tunnel. The no command deletes this configuration.

Parameters: <*session*> is the session number of the mirror, which is currently limited from 1 to 4; **<*tunnel-number*>** is the tunnel number, <interface-number> is the **reflector-port number of the mirror destination**.

Default: No configuration

Command Mode: Global mode

Usage Guide: 4 destination tunnels are supported on the switch. To be mentioned, the destination tunnel which is configured as the physical ports or tunnel, it should not be configured as the member of the port aggregation group, also the reflector-port number of the mirror destination needs to be specified. And the maximum throughput of the port is recommended to be larger than the total throughput of the source ports to be mirrored. If the destination tunnel of a session is removed, the mirror path configured in the session will be removed at the same time. And if the destination tunnel is reconfigured, the port mirror path will be recovered. To be mentioned, the flow mirror can only be recovered after the destination port is reconfigured. If the destination tunnel is configured as the tunnel which must completed the configuration, and it must be configured as GRE tunnel.

Example:

Switch(config)#monitor session 4 destination tunnel 1 reflector-port ethernet1/0/3

9.10 sFlow

9.10.1 sflow agent-address

Command: sflow agent-address <*agent-address*>

no sflow agent-address

Function: Configure the sFlow sample proxy address. The “no” form of this command deletes the proxy address.

Parameter: *<agent-address >* is the sample proxy IP address which is shown in dotted decimal notation.

Command Mode: Global Mode.

Default: None default value.

Usage Guide: The proxy address is used to mark the sample proxy which is similar to OSPF or the Router ID in the BGP. However it is not necessary to make the sFlow sample proxy work properly.
Example: Sample the proxy address at global mode.
switch (config)#sflow agent-address 192.168.1.200

9.10.2 sflow analyzer

Command: sflow analyzer sflowtrend
no sflow analyzer sflowtrend
Function: Configure the analyzer used by sFlow, the no command deletes the analyzer.
Parameter: sflowtrend is the analyzer of Inmon.
Command Mode: Global Mode
Default: Do not configure
Usage Guide: Configure this command when using sFlowTrend.
Example:
Switch(config)#sflow analyzer sflowtrend

9.10.3 sflow counter-interval

Command: sflow counter-interval *<interval-value>*
no sflow counter-interval
Function: Configure the max interval of the sFlow statistic sampling; the "no" form of this command deletes the statistic sampling interval value.
Parameter:*<interval-value>* is the value of the interval with a valid range of 20~120 and shown in second.
Command Mode: Port Mode
Default: No default value
Usage Guide: If no statistic sampling interval is configured, there will not be any statistic sampling on the interface.
Example: Set the statistic sampling interval on the interface e1/1/1 to 20 seconds.
Switch(Config-If-Ethernet1/1/1)#sflow counter-interval 20

9.10.4 sflow data-len

Command: sflow data-len *<length-value>*
no sflow data-len
Function: Configure the max length of the sFlow packet data; the "**no sflow data-len**" command restores the default value.
Parameter: *<length-value>* is the value of the length with a value range of 500-1470.
Command Mode: Port Mode.
Default: The value is 1400 by default.
Usage Guide: When combining several samples to a sFlow group to be sent, the length of the group excluding the MAC head and IP head parts should not exceed the configured value.

Example: Configure the max length of the sFlow packet data to 1000.
switch (Config-If-Ethernet1/1/2)#sflow data-len 1000

9.10.5 sflow destination

Command: sflow destination <*collector-address*> [<*collector-port*>]
no sflow destination
Function: Configure the IP address and port number of the host on which the sFlow analysis software is installed. If the port has been configured with IP address, the port configuration will be applied, or else the global configuration will be applied. The "no" form of this command restores the port to default and deletes the IP address.
Parameter: ***<collector-address>*** is the IP address of the analyzer, shown in dotted decimal notation. ***<collector-port>*** is the destination port of the sent sFlow packets.
Command Mode: Global Mode and Port Mode.
Default: The destination port of the sFlow packet is defaulted at 6343, and the analyzer has no default address.
Usage Guide: If the analyzer address is configured at Port Mode, this IP address and port configured at Port Mode will be applied when sending the sample packet. Or else the address and port configured at global mode will be applied. The analyzer address should be configured to let the sFlow sample proxy work properly.
Example: Configure the analyzer address and port at global mode.
switch (config)#sflow destination 192.168.1.200 1025

9.10.6 sflow header-len

Command: sflow header-len *<length-value>*
no sflow header-len
Function: Configure the length of the head data packet copied in the sFlow data sampling. The "no" form of this command restores the default value.
Parameter: ***<length-value>*** is the value of the length with a valid range of 32-256.
Command Mode: Port Mode.
Default: 128 by default.
Usage Guide: If the packet sample can not be identified whether it is IPv4 or IPv6 when sent to the CPU, certain length of the head of the group has to be copied to the sFlow packet and sent out. The length of the copied content is configured by this command.
Example: Configure the length of the packet data head copied in the sFlow data sampling to 50.
Switch(Config-If-Ethernet1/1/2)#sflow header-len 50

9.10.7 sflow priority

Command: sflow priority <*priority-value*>

no sflow priority

Function: Configure the priority when sFlow receives packet from the hardware. The "no" form of the command restores the default.

Parameter: ***<priority-value>*** is the priority value with a valid range of 0-3.

Command Mode: Global Mode.

Default: The default value is 0.

Usage Guide: When sample packet is sent to the CPU, it is recommended not to assign high priority for the packet so that regular receiving and sending of other protocol packet will not be interfered. The higher the priority value is set, the higher its priority will be.

Example: Configure the priority when sFlow receives packet from the hardware at global mode.

switch (config)#sflow priority 1

9.10.8 sflow rate

Command: sflow rate { input *<input-rate>* | output *<output-rate >*}

no sflow rate [input | output]

Function: Configure the sample rate of the sFlow hardware sampling. The "no" form of this command deletes the sampling rate value.

Parameter: ***<input-rate>*** is the rate of ingress group sampling, the valid range is 1000~16383500.

<output-rate> is the rate of egress group sampling, the valid range is 1000~16383500.

Command Mode: Port Mode.

Default: No default value.

Usage Guide: The traffic sampling will not be performed if the sampling rate is not configured on the port. And if the ingress group sampling rate is set to 10000, this indicates there will be one group be sampled every 10000 ingress groups.

Example: Configure the ingress sample rate on port e1/1/1 to 10000 and the egress sample rate to 20000.

Switch(Config-If-Ethernet1/1/1)#sflow rate input 10000

Switch(Config-If-Ethernet1/1/1)#sflow rate output 20000

9.10.9 sflow version

Command: sflow version<version>

no sflow version

Function: Configure the global sflow version. The no command recovers to be the default value.

Parameters: <*version*>: it is the sflow version, version4 and 5 are supported currently.

Default: 4.

Command Mode: Global Configuration Mode.

Usage Guide: This command is used to configure the global sflow version. Version4 and 5 are supported currently.

Example: Configure the sflow version as 5.

Switch (config)#sflow version 5

9.10.10 show sflow

Command: show sflow

Function: Display the sFlow configuration state.

Parameter: None.

Command Mode: All Modes.

Usage Guide: This command is used to acknowledge the operation state of sFlow.

Switch#show sflow

Sflow version 1.2

Agent address is 172.16.1.100

Collector address have not configured

Collector port is 6343

Sampler priority is 2

Sflow DataSource: type 2, index 194(Ethernet1/1/2)

Collector address is 192.168.1.200

Collector port is 6343

Counter interval is 0

Sample rate is input 0, output 0

Sample packet max len is 1400

Sample header max len is 50

Sample version is 4

Displayed Information	Explanation
Sflow version 1.2	Indicates the sFlow version is 1.2
Agent address is 172.16.1.100	Address of the sFlow sample proxy is 172.16.1.100
Collector address have not configured	the sFlow global analyzer address is not configured
Collector port is 6343	the sFlow global destination port is the defaulted 6343
Sampler priority is 2	The priority of sFlow when receiving packets from the hardware is 2.
Sflow DataSource: type 2, index 194(Ethernet1/1/1)	One sample proxy data source of the sFlow is the interface e1/1/1 and its type is 2 (Ethernet), the interface index is 194.
Collector address is 192.168.1.200	The analyzer address of the sampling address of the E1/1/1 interface is 192.168.1.200
Collector port is 6343	Default value of the port on E1/1/1 interface sampling proxy is 6343.
Counter interval is 20	The statistic sampling interval on e1/1/1 interface is 20 seconds
Sample rate is input 10000, output 0	The ingress traffic rate of e1/1/1 interface sampling proxy is 10000 and no egress traffic sampling will be performed
Sample packet max len is 1400	The length of the sFlow group data sent by the e1/1/1 interface should not exceed 1400 bytes.

Sample header max len is 50	The length of the packet data head copied in the data sampling of the e1/1/1 interface sampling proxy is 50
Sample version is 4	The datagram version of the sFlow group sent by the E1/1/1 interface sampling proxy is 4.

9.11 NQA

9.11.1 nqa agent

Command: nqa agent

no nqa agent

Function: Enable the nqa client function. The no operation of this command is to turn off the nqa client function.

Parameter: NONE.

Default: Default does not enable NQA client.

Command Mode: Global Mode.

Usage Guide: When using nqa client functionality, configure this command.

Example: Enable nqa client functionality

Switch#config terminal

Switch(config)#nqa agent

9.11.2 nqa entry type icmp-echo

Command: nqa entry <1-64> type icmp-echo dest-ip *A.B.C.D* (src-ip *A.B.C.D* |)

(nexthop-ip *A.B.C.D* |) (vrf *WORD* |)

no nqa entry <1-64>

Function: Configure the nqa entry probe type to icmp-echo. The no operation of this command is to delete the nqa entry.

Parameter: <1-64>: nqa entry id,

dest-ip *A.B.C.D*: dest addr,

src-ip *A.B.C.D*: source addr,

nexthop-ip *A.B.C.D*: nexthop addr,

vrf *WORD*: vrf name.

Default: None.

Command Mode: Global Mode.

Usage Guide: If you need to probe icmp-echo, you can configure this command line.

Example: Configure the nqa entry probe type to icmp-echo

Switch#config terminal
Switch(config)#nqa entry 1 type icmp-echo dest-ip 1.1.1.1 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

9.11.3 nqa entry type icmp-jitter

Command: nqa entry <1-64> type icmp-jitter dest-ip *A.B.C.D* (src-ip *A.B.C.D* |)
(nexthop-ip *A.B.C.D* |) (vrf *WORD* |)
no nqa entry <1-64>

Function: Configure the nqa entry probe type to icmp-jitter. The no operation of this command is to delete the nqa entry.

Parameter: <1-64>: nqa entry id,
dest-ip *A.B.C.D*: dest addr,
src-ip *A.B.C.D*: source addr,
nexthop-ip *A.B.C.D*: nexthop addr,
vrf *WORD*: vrf name.

Default: None.

Command Mode: Global Mode.

Usage Guide: If you need to probe icmp-jitter, you can configure this command line.

Example: Configure the nqa entry probe type to icmp-jitter
Switch#config terminal
Switch(config)#nqa entry 1 type icmp-jitter dest-ip 1.1.1.1 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

9.11.4 nqa entry type udp-echo

Command: nqa entry <1-64> type udp-echo dest-ip *A.B.C.D* dest-port <1-65535>
(src-ip *A.B.C.D* |) (nexthop-ip *A.B.C.D* |) (vrf *WORD* |)
no nqa entry <1-64>

Function: Configure the nqa entry probe type to udp-echo. The no operation of this command is to delete the nqa entry.

Parameter: <1-64>: nqa entry id,
dest-ip *A.B.C.D*: dest addr,
dest-port <1-65535>: dest port,
src-ip *A.B.C.D*: source addr,
nexthop-ip *A.B.C.D*: nexthop addr,
vrf *WORD*: vrf name.

Default: None.

Command Mode: Global Mode.

Usage Guide: If you need to probe udp-echo, you can configure this command line.

Example: Configure the nqa entry probe type to udp-echo
Switch#config terminal
Switch(config)#nqa entry 1 type udp-echo dest-ip 1.1.1.1 dest-port 1500 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

9.11.5 nqa entry type udp-jitter

Command: nqa entry <1-64> type udp-jitter dest-ip *A.B.C.D* dest-port <1-65535>
(src-ip *A.B.C.D* |) (nexthop-ip *A.B.C.D* |) (vrf *WORD* |)
no nqa entry <1-64>

Function: Configure the nqa entry probe type to udp-jitter. The no operation of this command is to delete the nqa entry.

Parameter: <1-64>: nqa entry id,
dest-ip *A.B.C.D*: dest addr,
dest-port <1-65535>: dest port,
src-ip *A.B.C.D*: source addr,
nexthop-ip *A.B.C.D*: nexthop addr,
vrf *WORD*: vrf name.

Default: None.

Command Mode: Global Mode.

Usage Guide: If you need to probe udp-jitter, you can configure this command line.

Example: Configure the nqa entry probe type to udp-jitter

Switch#config terminal
Switch(config)#nqa entry 1 type udp-jitter dest-ip 1.1.1.1 dest-port 1500 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

9.11.6 nqa entry type tcp

Command: nqa entry <1-64> type tcp dest-ip *A.B.C.D* dest-port <1-65535>
(src-ip *A.B.C.D* |) (nexthop-ip *A.B.C.D* |) (vrf *WORD* |)
no nqa entry <1-64>

Function: Configure the nqa entry probe type to tcp. The no operation of this command is to delete the nqa entry.

Parameter: <1-64>: nqa entry id,
dest-ip *A.B.C.D*: dest addr,
dest-port <1-65535>: dest port,
src-ip *A.B.C.D*: source addr,
nexthop-ip *A.B.C.D*: nexthop addr,
vrf *WORD*: vrf name.

Default: None.

Command Mode: Global Mode.

Usage Guide: If you need to probe tcp, you can configure this command line.

Example: Configure the nqa entry probe type to tcp

Switch#config terminal
Switch(config)#nqa entry 1 type tcp dest-ip 1.1.1.1 dest-port 1500 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

9.11.7 nqa entry type dhcp

Command: nqa entry <1-64> type dhcp interface vlan <1-4094>

no nqa entry <1-64>

Function: Configure the nqa entry probe type to dhcp. The no operation of this command is to delete the nqa entry.

Parameter: <1-64>: nqa entry id,

vlan <1-4094>: vlan id.

Default: None.

Command Mode: Global Mode.

Usage Guide: If you need to probe dhcp, you can configure this command line.

Example： Configure the nqa entry probe type to dhcp

Switch#config terminal

Switch(config)#nqa entry 1 type dhcp interface vlan 1

9.11.8 nqa entry description

Command: nqa entry <1-64> description *TEXT*

no nqa entry <1-64> description

Function: Configure nqa entry descriptors**.** The no operation of this command is to delete the nqa entry description.

Parameter: <1-64>: nqa entry id,

description *TEXT*: description.

Default: None.

Command Mode: Global Mode.

Usage Guide: If you need to configure the nqa entry description, you can configure this command line.

Example: Configure nqa entry description is icmp-test

Switch#config terminal

Switch(config)#nqa entry 1 description icmp-test

9.11.9 nqa entry frequency

Command: nqa entry <1-64> frequency <3-60>

no nqa entry <1-64> frequency

Function: Configure the nqa entry frequency. The no operation of this command is to restore the frequency to the default value.

Parameter: <1-64>: nqa entry id,

frequency <3-60>: The interval for frequency, value limited between 3 and 60 seconds.

Default: icmp-jitter,udp-jitter probe default to 40 seconds; other probe default to 3 seconds .

Command Mode: Global Mode.

Usage Guide: If you need to modify the nqa frequency interval time, you can configure this

command line.

Example: Configure the nqa entry with a frequency interval of 10 seconds

Switch#config terminal

Switch(config)#nqa entry 1 frequency 10

9.11.10 nqa entry probe-count

Command: nqa entry <1-64> probe-count <1-5>

no nqa entry <1-64> probe-count

Function: Configure probe-count within the nqa entry frequency. The no operation of this command restores the default probe-count.

Parameter: <1-64>: nqa entry id,

probe-count <1-5>: The interval for probe-count, value limited between 1 and 5 times.

Default: icmp-jitter,udp-jitter probe default to 20 times; other probe default to 1 times.

Command Mode: Global Mode.

Usage Guide: If you need to modify probe-count within the nqa entry frequency, you can configure this command line.

Example: Configure probe-count 3 times within the nqa entry frequency

Switch#config terminal

Switch(config)#nqa entry 1 probe-count 3

9.11.11 nqa entry probe-timeout

Command: nqa entry <1-64> probe-timeout <1-5>

no nqa entry <1-64> probe-timeout

Function: Configure the nqa entry probe-timeout. The no operation of this command is to restore probe-timeout to the default value.

Parameter: <1-64>: nqa entry id,

probe-timeout <1-5>: The interval for probe-timeout, value limited between 1 and 5 seconds.

Default: 2 seconds by default.

Command Mode: Global Mode.

Usage Guide: If you need to modify nqa entry probe-timeout, you can configure this command line.

Example: Configure nqa entry probe-timeout to 3 seconds

Switch#config terminal

Switch(config)#nqa entry 1 probe-timeout 3

9.11.12 nqa entry datasize

Command: nqa entry <1-64> datasize <1-8100>

no nqa entry <1-64> datasize

Function: Configure the nqa entry packet datasize. The no operation of this command is to restore datasize to the default value.

Parameter: <1-64>: nqa entry id,

datasize <1-8100>: The interval for packet datasize, value limited between 1 and 8100 bytes.

Default: 56 bytes by default.

Command Mode: Global Mode.

Usage Guide: If you need to modify nqa entry packet datasize, you can configure this command line.

Example: Configure nqa entry packet datasize to 1500 bytes

Switch#config terminal

Switch(config)#nqa entry 1 datasize 1500

9.11.13 nqa entry ttl

Command: nqa entry <1-64> ttl <1-255>

no nqa entry <1-64> ttl

Function: Configure the nqa entry packet ttl. The no operation of this command is to restore ttl to the default value.

Parameter: <1-64>: nqa entry id,

ttl <1-255>: The interval for packet ttl， value limited between 1 and 255.

Default: ttl is 30 by default.

Command Mode: Global Mode.

Usage Guide: If you need to modify nqa entry packet ttl, you can configure this command line.

Example: Configure nqa entry packet ttl to 100

Switch#config terminal

Switch(config)#nqa entry 1 ttl 100

9.11.14 nqa entry tos

Command: nqa entry <1-64> tos <0-255>

no nqa entry <1-64> tos

Function: Configure the nqa entry packet tos. The no operation of this command is to restore tos to the default value.

Parameter: <1-64>: nqa entry id,

tos <0-255>: The interval for packet tos， value limited between 0 and 255.

Default: ttl is 0 by default.

Command Mode: Global Mode.

Usage Guide: If you need to modify nqa entry packet tos, you can configure this command line.

Example: Configure nqa entry packet tos to 100

Switch#config terminal

Switch(config)#nqa entry 1 tos 100

9.11.15 nqa entry fail-percent

Command: nqa entry <1-64> fail-percent <1-100>

no nqa entry <1-64> fail-percent

Function: Configure the nqa entry fail-percent. The no operation of this command is to restore fail-percent to the default value.

Parameter: <1-64>:nqa entry id,

fail-percent <1-100>: The interval for fail-percent, value limited between 1 and 100.

Default: fail-percent is 100 by default.

Command Mode: Global Mode.

Usage Guide: If you need to modify nqa entry fail-percent, you can configure this command line.

Example: Configure nqa entry fail-percent to 10%

Switch#config terminal

Switch(config)#nqa entry 1 fail-percent 10

9.11.16 nqa entry records-result

Command: nqa entry <1-64> records-result <1-10>

no nqa entry <1-64> records-result

Function: Configure the nqa entry max records-result. The no operation of this command is to restore max records-result to the default value.

Parameter: <1-64>: nqa entry id,

records-result <1-10>: The interval for max records-result, value limited between 1 and 10.

Default: max records-result is 5 by default.

Command Mode: Global Mode.

Usage Guide: If you need to modify nqa entry max records-result, you can configure this command line.

Example: Configure nqa entry max records-result is 10

Switch#config terminal

Switch(config)#nqa entry 1 records-result 10

9.11.17 nqa entry probe-threshold

Command: nqa entry <1-64> probe-threshold <50-5000>

no nqa entry <1-64> probe-threshold

Function: Configure the nqa entry probe-threshold. The no operation of this command is to restore probe-threshold to the default value.

Parameter: <1-64>: nqa entry id,

probe-threshold <50-5000>： The interval for probe-threshold, value limited between 50ms and 5000ms.

Default: probe-threshold is 2000ms by default.

Command Mode: Global Mode.

Usage Guide: If you need to modify nqa entry probe-threshold, you can configure this command line.

Example: Configure nqa entry probe-threshold to 3000ms

Switch#config terminal

Switch(config)#nqa entry 1 probe-threshold 3000

9.11.18 nqa entry start

Command: nqa entry <1-64> start (|forever|time-range *WORD*)

no nqa entry <1-64> start

Function: Configure the nqa entry start. The no operation of this command is to restore start to the default value.

Parameter: <1-64>: nqa entry id,

Forever: keep probe,

time-range *WORD*: probe running time.

Default: the nqa entry stop probe by default.

Command Mode: Global Mode.

Usage Guide: If the probe time is not configured, it will end after one cycle of detection by default.

Example: Configure the nqa entry to start and continue probe

Switch#config terminal

Switch(config)#nqa entry 1 start forever

9.11.19 nqa alarm enable

Command: nqa alarm enable

no nqa alarm enable

Function: Enable nqa global alarm functionality. The no operation of this command is to turn off the nqa global alarm function.

Parameter: None.

Default: nqa turns off global alarm functionality by default.

Command Mode: Global Mode.

Usage Guide: If nqa global alarm functionality is enabled, configure this command line.

Example: Enable nqa global alarm functionality.

Switch#config terminal

Switch(config)#nqa alarm enable

9.11.20 nqa traps enable

Command: nqa traps enable

no nqa traps enable

Function: Enable nqa global traps functionality. The no operation of this command is to turn off the nqa global traps function.

Parameter: None.
Default: nqa turns off global traps functionality by default.
Command Mode: Global Mode.
Usage Guide: If nqa global traps functionality is enabled, configure this command line.
Example: Enable nqa global traps functionality.
Switch#config terminal
Switch(config)#nqa traps enable

9.11.21 nqa entry alarm enable

Command: nqa entry <1-64> alarm enable
no nqa entry <1-64> alarm enable
Function: Enable the nqa entry alarm functionality. The no operation of this command is to disable the nqa entry alarm function.
Parameter: <1-64>: nqa entry id.
Default: the nqa entry turns off alarm function by default.
Command Mode: Global Mode.
Usage Guide: If you need to use the nqa entry alarm function, configure this command line.
Example: Configure the nqa entry to enable alarm function.
Switch#config terminal
Switch(config)#nqa entry 1 alarm enable

9.11.22 nqa entry traps enable

Command: nqa entry <1-64> traps enable
no nqa entry <1-64> traps enable
Function: Enable the nqa entry traps functionality. The no operation of this command is to disable the nqa entry traps function.
Parameter: <1-64>: nqa entry id.
Default: the nqa entry turns off traps function by default.
Command Mode: Global Mode.
Usage Guide: If you need to use the nqa entry traps function, configure this command line.
Example: Configure the nqa entry to enable traps function.
Switch#config terminal
Switch(config)#nqa entry 1 traps enable

9.11.23 nqa server

Command: nqa server
no nqa server
Function: Enable nqa server functionality. The no operation of this command is to turn off the nqa server function.
Parameter: None.

Default: nqa turns off server functionality by default.
Command Mode: Global Mode.
Usage Guide: If nqa server functionality is enabled, configure this command line.
Example: Enable nqa server functionality
Switch#config terminal
Switch(config)#nqa server

9.11.24 nqa server tcp-port

Command: nqa server tcp-port <1-65535> (vrf *WORD* |)
no nqa server tcp-port (vrf *WORD* |)
Function: Configure the nqa server TCP listening port number. The no operation of this command is to turn off the nqa server TCP listening function.
Parameter: tcp-port <1-65535>: TCP listening port number,
vrf *WORD*: vrf name.
Default: TCP listening port number is 2000 by default.
Command Mode: Global Mode.
Usage Guide: If you need the nqa server to listen to the TCP port, configure this command line.
Example: Configure the nqa server to listen to TCP port number 3000 with vrf set to a
Switch#config terminal
Switch(config)#nqa server tcp-port 3000 vrf a

9.11.25 nqa server udp-port

Command: nqa server udp-port <1-65535> (vrf *WORD* |)
no nqa server udp-port (vrf *WORD* |)
Function: Configure the nqa server UDP listening port number. The no operation of this command is to turn off the nqa server UDP listening function.
Parameter: udp-port <1-65535>: UDP listening port number,
vrf *WORD*: vrf name.
Default: UDP listening port number is 2000 by default.
Command Mode: Global Mode.
Usage Guide: If you need the nqa server to listen to the UDP port, configure this command line.
Example: Configure the nqa server to listen to UDP port number 3000 with vrf set to a
Switch#config terminal
Switch(config)#nqa server udp-port 3000 vrf a

9.11.26 track nqa

Command: track <1-32> nqa <1-64>
no track <1-32> (nqa <1-64>|)
Function: Configure track association with nqa entry. The no operation of this command is to

unlink the nqa entry.

Parameter: track <1-32>: track id,

nqa <1-64>: nqa entry id.

Default: None.

Command Mode: Global Mode.

Usage Guide: If you need to associate nqa entry with tracks, you need to configure this command line.

Example: Configure nqa entry association with track

Switch#config terminal

Switch(config)#track 1 nqa 1

9.11.27 track list boolean

Command: track <1-32> list boolean (and|or)

no track <1-32> list boolean

Function： Configure the Boolean relationship of track association with multiple nqa entry. The no operation of this command is to unlink the Boolean relationship of multiple nqa entry.

Parameter: track <1-32>: track id,

boolean (and|or): Multiple nqa entry have a Boolean relationship of AND or OR.

Default: None.

Command Mode: Global Mode.

Usage Guide: If multiple nqa entry need to be associated with tracks, the command line needs to be configured; 'add' If there is a probe failure, it is considered a failure, 'or' if there is a probe success, it is considered a success.

Example: Configure track to associate multiple nqa entry with a Boolean relationship of and

Switch#config terminal

Switch(config)#track 1 list boolean and

9.11.28 ip route track

Command: ip route (*A.B.C.D A.B.C.D* | *A.B.C.D/M*) *A.B.C.D* track <1-32>

no ip route (*A.B.C.D A.B.C.D* | *A.B.C.D/M*) (*A.B.C.D*|) (track <1-32>|)

Function: Configure track associated static routing. The no operation of this command is to delete static routing.

Parameter: *A.B.C.D*: ip address,

***A.B.C.D*:** ip address mask,

***A.B.C.D/M*:** ip address prefix,

***A.B.C.D*:** nexthop ip address,

<1-32>: track id.

Default: None.

Command Mode: Global Mode.

Usage Guide: If you need to associate track with static route, you need to configure this command line.

Example: Configure track associated static routing
Switch#config terminal
Switch(config)#ip route 1.1.1.1/32 2.2.2.2 track 1

9.11.29 rip track

Command: rip track <1-32>
no rip track <1-32>
Function: Configure track associated rip. The no operation of this command is to cancel track associated rip.
Parameter: <1-32>: track id.
Default: None.
Command Mode: Interface Configuration Mode.
Usage Guide: If you need to associate track with rip, you need to configure this command line.
Example: Configure track associated rip
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#rip track 1

9.11.30 ospf track

Command: ip ospf track <1-32>
no ip ospf track <1-32>
Function: Configure track associated ospf. The no operation of this command is to cancel track associated ospf.
Parameter: <1-32>: track id.
Default: None.
Command Mode: Interface Configuration Mode.
Usage Guide: If you need to associate track with ospf, you need to configure this command line.
Example: Configure track associated ospf
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf track 1

9.11.31 bgp track

Command: neighbor {*<ip-address>*|*<TAG>*} track <1-32>
no neighbor {*<ip-address>*|*<TAG>*} track <1-32>
Function: Configure track associated bgp. The no operation of this command is to cancel track associated bgp.
Parameter: *<ip-address>*: IP address of the neighbor,
<TAG>: Name of peer group,
<1-32>: track id.

Default: None.

Command Mode: BGP route mode.

Usage Guide: If you need to associate track with bgp, you need to configure this command line.

Example: Configure track associated bgp neighbor 1.1.1.1

Switch#config terminal

Switch(config)#router bgp 1

Switch(config-router)#neighbor 1.1.1.1 track 1

9.11.32 show nqa results

Command: show nqa (entry <1-64>|) results

Function: Show nqa entry probe results.

Parameter: <1-64>: nqa entry id.

Default: None.

Command Mode: Any mode.

Usage Guide: After the nqa entry completes the probe, the probe result is show through this command line; If there is no nqa entry ID, all nqa entry probe results will be displayed.

Example: switch#show nqa entry 1 results

NQA entry(test probe-type, icmp-echo)

1, Test 17 result The test is finished.

Send operation times: 1 Receive response times: 1

Min/Max/Avg/Sum RTT: 0/0/0/0

RTT Square Sum: 0

Start probe Time: 2023-11-10 11:26:55

Lost packet ratio: 0%

Displayed information	Explaination
probe-type	Probe type
Send operation times	Probe send times
Receive response times	Receive response times
Min/Max/Avg/Sum RTT	Min/Max/Avg/Sum Round-Trip Time
RTT Square Sum	Round-Trip Time Square Sum
Start probe Time	Probe start time
Lost packet ratio	Packet loss rate

9.11.33 show track status

Command: show track (all|<1-32>) status

Function: show track status.

Parameter: all: show all track status,

<1-64>: track id.

Default: None.

Command Mode: Any mode.

Usage Guide: After the track is created, the track status can be viewed through this command line**.**

Example: switch#show track 1 status

Track ID: 1

Notification delay: Positive 0, Negative 0 (in milliseconds)

Logical mode: Default

Remote-ip: * probe-status: positive

protocal: NQA 1 status: success

Chapter 10 Commands for Network Time Management

10.1 NTP

10.1.1 clock timezone

Command: clock timezone WORD {add | subtract} <0-23> [<0-59>]

no clock timezone WORD

Function: This command configures timezone in global mode, the no command deletes the configured timezone.

Parameters: WORD: timezone name, the length should not exceed 16

add | subtract: the action of timezone

<0-23>: the hour value

<0-59>: the minute value

Command Mode: Global mode

Default: None.

Usage Guide: The timezone name is invalid with the blank, the hour and minute value must be in the specific range.

Example: Configure the action as add for the eighth timezone globally.

Switch(config)#clock timezone aaa add 8

10.1.2 debug ntp adjust

Command: debug ntp adjust

no debug ntp adjust

Function: To enable/disable the debug switch of displaying local time adjust information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable the debug switch of displaying local time adjust information.

Switch# debug ntp adjust

10.1.3 debug ntp authentication

Command: debug ntp authentication

no debug ntp authentication

Function: To display NTP authentication information, the no form command disabled the switch

of displaying NTP authentication information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: To display NTP authentication information, if the switch is enabled, and if the packets schlepped authentication information when the packet in sending or receiving process, then the key identifier will be printed out.

Example: To enable the switch of displaying NTP authentication information.

Switch# debug ntp authentication

10.1.4 debug ntp events

Command: debug ntp events

no debug ntp events

Function: To enable/disable debug switch of displaying NTP event.

Parameter: None.

Default: Disable the debug switch of displaying NTP event.

Command Mode: Admin Mode.

Usage Guide: To enable debug switch of displaying NTP event, after that, if some server changed from available to unavailable or from unavailable to available, the received illegal packet events will be printed.

Example: To enable debug switch of displaying NTP event information.

Switch# debug ntp events

10.1.5 debug ntp packet

Command: debug ntp packet [send | receive]

no debug ntp packet [send | receive]

Function: To enable/disable the debug switch of displaying NTP packet information.

Parameter: send: The debug switch of sending NTP packet.

receive: The debug switch of receiving NTP packet.

If there is no parameter, that means should enable the sending and receiving switch of NTP packet in the same time.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable the debug switch of displaying NTP packet information.

Switch# debug ntp packet

10.1.6 debug ntp sync

Command: debug ntp sync

no debug ntp sync

Function: To enable/disable debug switch of displaying local time synchronization information.
Parameter: None.
Default: Disabled.
Command Mode: Admin Mode.
Usage Guide: None.
Example: To enable debug switch of displaying local time synchronization information.
Switch# debug ntp sync

10.1.7 ntp access-group

Command: ntp access-group server <*acl*>
no ntp access-group server <*acl*>
Function: To configure/cancel the access control list of NTP Server.
Parameter: <*acl*>: ACL number, range is from 1 to 99.
Default: Not configure the access control of NTP Server.
Command Mode: Global Mode.
Usage Guide: None.
Example: To configure access control list 2 on the switch.
Switch(config)#ntp access-group server 2

10.1.8 ntp authenticate

Command: ntp authenticate
no ntp authenticate
Function: To enable/cancel NTP authentication function.
Parameter: None.
Default: Disabled.
Command Mode: Global Mode.
Usage Guide: None.
Example: To enable NTP authentication function.
Switch(config)#ntp authenticate

10.1.9 ntp authentication-key

Command: ntp authentication-key <*key-id*> md5 <*value*>
no ntp authentication-key <*key-id*>
Function: To enable/cancel NTP authentication function, and defined NTP authentication key.
Parameter: key-id: The id of key, range is from 1 to 4294967295.
value: The value of key, range between 1 to 16 of ascii code.
Default: The authentication key of NTP authentication is not configured by default.
Command Mode: Global Mode.
Usage Guide: None.
Example: To define the authentication key of NTP authentication, the key-id is 20, the md5 is abc.

Switch(config)# ntp authentication-key 20 md5 abc

10.1.10 ntp broadcast client

Command: ntp broadcast client

no ntp broadcast client

Function: To configure/cancel the specified port to receive NTP broadcast packets.

Parameter: None.

Default: Disabled.

Command Mode: vlan Configuration Mode.

Usage Guide: None.

Example: Enable the function of VLAN1 interface to receive NTP broadcast packets.

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp broadcast client

10.1.11 ntp broadcast server count

Command: ntp broadcast server count *<number>*

no ntp broadcast server count

Function: Set the max number of broadcast or multicast servers supported by the NTP client. The no operation will cancel the configuration and restore the default value.

Parameters: number： 1-100, the max number of broadcast servers.

Default: The default max number of broadcast servers is 50.

Command Mode: Global Mode.

Examples: Configure the max number of broadcast servers is 70 on the switch.

Switch(config)#ntp broadcast server count 70

10.1.12 ntp disable

Command: ntp disable

no ntp disable

Function: To disable/enable the NTP function on port.

Parameter: None.

Default: To enable NTP function on all ports.

Command Mode: vlan Configuration Mode.

Usage Guide: None.

Example: To disable the NTP function on vlan1 interface.

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp disable

10.1.13 ntp enable

Command: ntp enable

ntp disable

Function: To enable/disable NTP function globally.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To enable NTP function.

Switch(config)#ntp enable

10.1.14 ntp ipv6 multicast client

Command: ntp ipv6 multicast client

no ntp ipv6 multicast client

Function: Configure the specified interface to receive IPv6 NTP multicast packets, the no command will cancels the specified interface to receive IPv6 NTP multicast packets.

Parameter: None.

Command mode: vlan mode

Default: Interface does not receive IPv6 NTP multicast packets.

Usage guide: None.

Example: Enable the function for receiving IPv6 NTP multicast packets on vlan1 interface.

Switch(Config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp ipv6 multicast client

10.1.15 ntp multicast client

Command: ntp multicast client

no ntp multicast client

Function: Configure the specified interface to receive NTP multicast packets, the no command will cancels the specified interface to receive NTP multicast packets.

Parameter: None.

Command mode: vlan mode

Default: Interface does not receive NTP multicast packets.

Usage guide: None.

Example: Enable the function for receiving NTP multicast packets on vlan1 interface.

Switch(Config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp multicast client

10.1.16 ntp server

Command: ntp server {vrf <vrfname>|host <hostname>|<*ip-address*> / <*ipv6-address*>} [version <*version_no*>] [key <*key-id*>]

no ntp server {vrf <vrfname>|host <hostname>|<*ip-address*>/<*ipv6-address*>}

Function: To enable specified time server of time source, the no form of this command cancels

the specified time server of time source.

Parameter: ip-address: IPv4 address of time server.

ipv6-address: IPv6 address of time server.

version: The version information configured for server.

version_no: The version number of server, range is from 1 to 4, default is 4.

key: To configure key for server.

key-id: The key id.

<vrfname>:vrf instance name

<hostname>:hostname of server

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure time server address as 1.1.1.1 on switch.

Switch(config)#ntp server 1.1.1.1

10.1.17 ntp syn-interval

Command: ntp syn-interval <1-3600>

no ntp syn-interval

Function: Configure the request packet sending interval of ntp client as 1s-3600s. The no command recovers to be the default value of 64s.

Default: 64s.

Command Mode: Global Mode.

Usage Guide: For responding the risk of ntp adjusting the system time under the high latency network, ntp client will select the time information with the smallest latency for the system time synchronization after sent 8 ntp time requisitions. So at the default configuration, ntp client sends the requisition packet once every 64s, after 8 times, it will adjust the time. It means to adjust the system time every 8 minutes. If user wants to configure the interval, such as one hour, user should adjust the packet sending interval as 450(3600/8) s.

Example: Configure to adjust the system time once an hour, and the packet sending time is 450s.

Switch(config)#ntp syn-interval 450

10.1.18 ntp trusted-key

Command: ntp trusted-key <*key-id*>

no ntp trusted-key <*key-id*>

Function: To configure the trusted key. The no command cancels the trusted key.

Parameter: key-id: The id of key, range is from 1 to 4294967295.

Default: Trusted key is not configured by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure the specified key 20 to trusted key.

Switch(config)# ntp trusted-key 20

10.1.19 show ntp status

Command: show ntp status

Function: To display time synchronization status, include synchronized or not, layers, address of time source and so on.

Parameter: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: None.

Example:

Switch# show ntp status
Clock status: synchronized
Clock stratum: 3
Reference clock server: 1.1.1.2
Clock offset: 0.010 s
Root delay: 0.012 ms
Root dispersion: 0.000 ms
Reference time: TUE JAN 03 01:27:24 2006

10.1.20 show ntp session

Command: show ntp session [<*ip-address*> | <*ipv6-address*>]

Function: To display the information of all NTP session or one specific session, include server ID, server layer, and the local offset according to server. (The symbol * means this server is the selected local time source)

Parameter: ip-address: The IPv4 address of some specifics configured time server.

ipv6-address: The IPv6 address of some specifics configured time server.

If no parameter, the session relative information of all servers will be displayed (Include broadcast and multicast servers)

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: None.

Example:

(Switch)# show ntp session

	server	stream	type	rootdelay	rootdispersion	trustlevel
*	1.1.1.2	2	unicast	0.010s	0.002s	10
	2.2.2.2	3	unicast	0.005s	0.000s	10

10.2 SNTP

10.2.1 clock timezone

Command: clock timezone WORD {add | subtract} <0-23> [<0-59>]

no clock timezone WORD

Function: This command configures timezone in global mode, the no command deletes the configured timezone.

Parameters: WORD: timezone name, the length should not exceed 16

add | subtract: the action of timezone

<0-23>: the hour value

<0-59>: the minute value

Command Mode: Global mode

Default: None.

Usage Guide: The timezone name is invalid with the blank, the hour and minute value must be in the specific range.

Example: Configure the action as add for the eighth timezone globally.

Switch(config)#clock timezone aaa add 8

10.2.2 debug sntp

Command: debug sntp {adjust | packet | select|config }

no debug sntp {adjust | packet | select|config}

Function: Displays or disables SNTP debug information.

Parameters: adjust stands for SNTP clock adjustment information; **packet** for SNTP packets, **select** for SNTP clock selection,config for SNTP config infomation.

Command mode: Admin Mode

Example: Displaying debugging information for SNTP packet.

Switch#debug sntp packet

10.2.3 sntp polltime

Command: sntp polltime *<interval>*

no sntp polltime

Function: Sets the interval for SNTP clients to send requests to NTP/SNTP; the "**no sntp polltime**" command cancels the polltime sets and restores the default setting.

Parameters: *<interval>* is the interval value from 16 to 16284.

Default: The default polltime is 64 seconds.

Command Mode: Global Mode

Example: Setting the client to send request to the server every 128 seconds.

Switch#config

Switch(config)#sntp polltime128

10.2.4 sntp server

Command: sntp server {vrf <vrfname>|host <hostname> |<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]

no sntp server {vrf <vrfname>|host <hostname>|<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]

Function: Enable the specified time server as clock source, the no command deletes the specified time server.

Parameters: ip-address: IPv4 address of time server
ipv6-address: IPv6 address of time server
source: Specify the interface of the source address
vlan: Configure the virtual LAN
vlan no: Virtual LAN number, ranging from 1 to 4094
loopback: Configure loopback interface
loopback no: Loopback identifier, ranging from 1 to 1024
version: Configure the version for the server
version_no: Version number, ranging from 1 to 4, the default is 4
<vrfname>:vrf instance name
<hostname>:hostname of server

Default: Do not configure the time server.

Command Mode: Global mode

Usage Guide: None.

Example:

Configure the time server address as 1.1.1.1, specify the interface of the source address as vlan1:

Switch(config)#sntp server 1.1.1.1 source vlan 1

Delete the time server that the address is 1.1.1.1, the interface of the specified source address is vlan1:

Switch(config)#no sntp server 1.1.1.1 source vlan 1

10.2.5 show sntp

Command: show sntp

Function: Displays current SNTP client configuration and server status.

Parameters: N/A.

Command Mode: Admin and Configuration Mode.

Example: Displaying current SNTP configuration.

Switch#show sntp

SNTP server	Version	Last Receive
2.1.0.2	1	6

10.3 DNSv4/v6

10.3.1 clear dynamic-host

Command: clear dynamic-host {*<ip-address>* | *<ipv6-address>* | all}
Function: To delete the domain entry of specified address or all address in dynamic cache.
Parameter: ***<ip-address>*** is the IP address, in dotted decimal notation; ***<ipv6-address>*** is the IPv6 address; **all** is to delete the domain entry of all address in dynamic cache.
Command Mode: Admin Mode.
Default: Disabled.
Usage Guide: This command is used to manually delete the domain name and address entry in dynamic cache, this command is much useful when domain name have lived long time in cache.
Example: To delete the address of 202.108.22.5 of domain entry.
Switch# clear dynamic-host 202.108.22.5

10.3.2 debug dns

Command: debug dns {all | packet [send | recv] | events | relay}
no debug dns {all | packet [send | recv] | events | relay}
Function: To display the application debug information of DNS domain name resolution, the no form of this command disables the debug display.
Parameter: None.
Command Mode: Admin Mode.
Example:
Switch# debug dns all
Switch# ping host www.google.com

%Jan 01 00:03:13 2006 domain name www.google.com is to be parsed!
%Jan 01 00:03:13 2006 Dns query type is A!
%Jan 01 00:03:13 2006 Connect dns server 10.1.120.241 .....
ping www.google.com [104.244.42.197]
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 104.244.42.197, timeout is 2 seconds.
%Jan 01 00:03:15 2006 Host:www.google.com Address: 104.244.42.197
.....
Success rate is 0 percent (0/5), round-trip min/avg/max = 0/0/0 ms

10.3.3 dns-server

Command: dns-server {*<ip-address>*|*<ipv6-address>*} [priority *<value>*]
no dns-server {*<ip-address>*|*<ipv6-address>*}
Function: To configure/delete DNS server.

Parameter: ***<ip-address>*** is the IP address, in dotted decimal notation, ***<ipv6-address>*** is the IPv6 address, ***<value>*** is the priority of DNS server, range between 0~255, 0 by default.
Command Mode: Global Mode.
Default: Not configuration.
Usage Guide: This command is used for configure or delete DNS server, when need to enable dynamic domain name mapping, the switch will sending a domain name search request packet to configured DNS server, the DNS server can be configured no more than 6. The priority is the optional parameter, if priority is configured, the DNS server must be organized according to the order of priority, from high to low. That is the switch sending domain name search request to the server which have the biggest priority, so some DNS server with quick search speed and used frequently can be configured to highest priority. If priority is not configured, to search DNS server must according to the configuration order. When the switch serves as a DNS SERVER, the queries to the DNS SERVER won't follow the above privilege rule; instead, the requests will be sent to all configured servers at the same time
Example: To configure the priority of DNS server as 200, the server's address is 10.1.120.241.
Switch(config)# dns-server 10.1.120.241 priority 200

10.3.4 dns lookup

Command: dns lookup {ipv4 | ipv6} ***<hostname>***
Function: To enable DNS dynamic domain name resolution.
Parameter: {ipv4 | ipv6} means the IPv4 or IPv6 address look up, ***<hostname>*** is the resolute dynamic host name, less than 63 characters.
Command Mode: Global Mode.
Default: Disabled.
Usage Guide: This command is used to look up correspond address based on entered client name, it can look up both IPv4 and IPv6 address. This command only used for domain name mapping, it have no other application function. When command is running, interrupt is forbidding. If configured many servers and domain name suffix, longer time will be required for domain name mapping.
Example: To look up the IPv4 address of www.google.com.
Switch(config)# dns lookup ipv4 www.google.com

10.3.5 show dns name-server

Command: show dns name-server
Function: To display the information of configured DNS server.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Example:
Switch# show dns name-server
DNS NAME SERVER:
Address Priority

10.1.120.231	100
10.1.180.85	80
2001::1	20

10.3.6 show dns domain-list

Command: show dns domain-list
Function: To display the suffix information of configured DNS domain name.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Example:
Switch# show dns domain-list
DNS DOMAIN LIST:
com

10.3.7 show dns hosts

Command: show dns hosts
Function: To display the dynamic domain name information of resolute by switch.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Example:
Switch# show dns hosts
Total number of dynamic host is 2
DNS HOST LIST：

Hostname	Address	Time to live	Type
www.google.com	104.244.42.197	168000	dynamic
www.ipv6.org	2001:6b0:1:	168060	dynamic

10.3.8 show dns config

Command: show dns config
Function: Display the configured global DNS information on the switch.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Example:
Switch(config)#show dns config
ip dns server enable
ip domain-lookup enable
the maximum of dns client in cache is 3000, timeout is 5
dns client number in cache is 0

dns dynamic host in cache is 0
dns name server number is 1
dns domain-list number is 0

10.3.9 show dns client

Command: show dns client
Function: Display the DNS Client information maintained by the switch.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Example:
Switch(config)#show dns client
DNS REQUEST LIST:
Total number of dns request is 2

Address	Request Id
192.168.11.141	1
192.168.11.138	2

10.3.10 ip domain-lookup

Command: ip domain-lookup
no ip domain-lookup
Function: To enable/disable DNS function, whether the switch will send dynamic DNS domain queries to the real DNS server or not.
Parameter: None.
Command Mode: Global Mode.
Default: Disabled.
Usage Guide: This command is used to enable or disable the switch DNS dynamic query function. If DNS dynamic query function is enabled, the DNS server will resolve the host name and domain name to the IPv4 or IPv6 address for requests from the clients. If DNS is disabled, client applications will not be able to send any DNS requests to the DNS server. In this situation, only the static address resolution is available. For the address mapping in the resolve cache, which is learnt through DNS before, will be invalid after aging.
Example: To enable DNS function, can resolve the domain name dynamic.
Switch(config)# ip domain-lookup

10.3.11 ip domain-list

Command: ip domain-list *<WORD>*
no ip domain-list *<WORD>*
Function: To configure/delete domain name suffix.
Parameter: *<WORD>* is the character string of domain name suffix, less than 63 characters.
Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to configure or delete suffix of domain name, when the entered domain name is not integrity (such as google), the switch can add suffix automatically, after that, address mapping can run, the domain name suffix can be configured no more than 6. The first configured domain name suffix will be added first.

Example: To configure domain name suffix of com.

Switch(config)# ip domain-list com

10.3.12 ip dns server

Command: ip dns server

no ip dns server

Function: Enable/disable DNS SERVER function.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled by default.

Usage Guide: After the DNS SERVER function is enabled, the switch will be able to receive and handle DNS Requests from the clients by looking up locally or forward the request to the real DNS server.

Example: Configure to enable the dns server function of the switch.

Switch(config)#ip dns server

10.3.13 ip dns server queue maximum

Command: ip dns server queue maximum <1-5000>

no ip dns server queue maximum

Function: Configure the max number of client information in the switch queue.

Parameter: <1-5000> the value can be 1—5000.

Command Mode: Global Mode.

Default: The default client number is 3000.

Usage Guide: When receiving a DNS Request from a client, the switch will cache the client's information. But the number of client information in the queue should not exceed the configured maximum number; otherwise the client's request won't be handled.

Example: Set the max number of client information in the switch queue as 2000.

Switch(config)#ip dns server queue maximum 2000

10.3.14 ip dns server queue timeout

Command: ip dns server queue timeout <1-100>

no ip dns server queue timeout

Function: Configure the timeout value of caching the client information on the switch.

Parameters: <1-100> the value can be1—100s.

Command Mode: Global Mode.

Default: The default timeout value is 5s.

Usage Guide: When receiving a DNS Request from a client, the switch will cache the client's information. But the time of maintaining the client information should not exceed the configured maximum timeout value; otherwise the client's information will be cleared out.

Example: Configure the maximum timeout value of caching the client information on the switch as 10s.

Switch(config)#ip dns server queue timeout 10

10.4 Summer Time

10.4.1 clock summer-time absolute

Command: clock summer-time <*word*> absolute <*HH:MM*> <*YYYY.MM.DD*> <*HH:MM*> <*YYYY.MM.DD*> [<*offset*>]

no clock summer-time

Function: Configure summer time range, the time in this range is summer time. The no command deletes the configuration.

Parameter: ***<word>*** is the time zone name of summer time; ***<HH:MM>*** is the start time, the format is hour (from 0 to 23):minute (from 0 to 59); ***<YYYY.MM.DD>*** is the start date, the format is year (from 2001 to 2037).month (from 1 to 12).date (from 1 to 31); ***<HH:MM>*** is the end time, the format is hour (from 0 to 23):minute (from 0 to 59); ***<YYYY.MM.DD>*** is the end date, the format is year (from 2001 to 2037).month (from 1 to 12).date (from 1 to 31); ***<offset>*** is the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes.

Default: There is no summer time range.

Command Mode: Global Mode

Usage Guide: This command sets the absolute start and end time for summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. Note: the end time should be bigger than the start time for configuring summer time.

Example: Configure the time range of summer time at 12:10 from april 6th to augest 6th in 2010, offset value as 70 minutes, summer time is named as aaa.

Switch(config)#clock summer-time aaa absolute 12:10 2010.4.6 12:10 2010.8.6 70

10.4.2 clock summer-time recurring

Command: clock summer-time <*word*> recurring <*HH:MM*> <*MM.DD*> <*HH:MM*> <*MM.DD*> [<*offset*>]

no clock summer-time

Function: Configure the recurrent summer time range, the time in this range is summer time.

Parameter: ***<word>*** is the time zone name of summer time; ***<HH:MM>*** is the start time, the format is hour (from 0 to 23):minute (from 0 to 59); ***<MM.DD>*** is the start date, the format is month(from 1 to 12).date(from 1 to 31); ***<HH:MM>*** is the end time, the format is hour(from 0 to 23):minute(from 0 to 59); ***<MM.DD>*** is the end date, the format is month(from 1 to 12).date(from 1 to 31); ***<offset>*** is the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes.

Default: There is no summer time range.

Command Mode: Global Mode

Usage Guide: This command sets the start and the end time for the recurrent summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. There is no relation between the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports the summer time of southern hemisphere.

Example: Configure the time range of summer time at 12:10 from april 6th to augest 6th year after year, offset value as 70 minutes, summer time is named as aaa.

Switch(config)# clock summer-time aaa recurring 12:10 4.6 12:10 8.6 70

10.4.3 clock summer-time recurring

Command: clock summer-time <*word*> recurring <*HH:MM*> <*week*> <*day*> <*month*> < *HH:MM* > <*week*> <*day*> <*month*> [<*offset*>]

no clock summer-time

Function: Configure the recurrent summer time range, the time in this range is summer time.

Parameter: ***<word>*** is the time zone name of summer time; ***<HH:MM>*** is the start time, the format is hour(from 0 to 23):minute(from 0 to 59); ***<week>*** is the week from 1 to 4, first or last; ***<day>*** is the week value, the value as “Sun”, “Mon”, “Tue”, “Wed”, “Thu”, “Fri”, “Sat”; ***<month>*** is the month, the value as ”Jan”, “Feb”, “Mar”, “Apr”, “May”, ”Jun”, “Jul”, “Aug”, “Sep”, “Oct”, “Nov”, “Dec”; ***<HH:MM>*** is the end time, the format is hour(from 0 to 23):minute(from 0 to 59); ***<week>*** is the week from 1 to 4, first or last; ***<day>*** is the week value, the value as “Sun”, “Mon”, “Tue”, “Wed”, “Thu”, “Fri”, “Sat”; ***<month>*** is the month, the value as ”Jan”, “Feb”, “Mar”, “Apr”, “May”, ”Jun”, “Jul”, “Aug”, “Sep”, “Oct”, “Nov”, “Dec” ***<offset>*** is the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes.

Default: There is no summer time range.

Command Mode: Global Mode

Usage Guide: This command sets the start and end time for the recurrent summer time flexibly. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system

time, the system finishes summer time. There is no relation between the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports summer time of southern hemisphere.

Example: Configure summer time at 12:10 from the first Monday of april to the last Saturday of augest year after year, offset value as 70 minutes, summer time is named as aaa.

Switch(config)#clock summer-time aaa recurring 12:10 1 mon apr 12:10 last sat aug 70

Chapter 11 Commands for Virtualization

11.1 VSF

11.1.1 Basic VSF

11.1.1.1 switch convert mode

Command: switch convert mode (stand-alone | vsf)

Function: Make the device transform from independent operation mode to VSF mode or transform from VSF mode to independent operation mode.

Parameters: <*stand-alone*>: Independent operation mode. **<*vsf*>:** VSF mode.

Default: Judge the mode that the device should enter in according to the VSF configuration file of vsf.cfg.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: The device supports two kinds of modes: independent operation mode and VSF mode. The device under the independent operation mode can just operate in stand-alone. The device under the VSF mode can form VSF with other devices. The two modes can be switched through this command.

Example: Configure the device to enter in the VSF mode when it is under the independent operation mode.

Switch#config

Switch(config)#switch convert mode vsf

11.1.1.2 write

Command: write

Function: When the device is under the independent operation mode, **write** command can save the current running-config and it can also write the current relevant VSF configuration into vsf.cfg. if the device is under the VSF mode, **write** command will save the current running-config into vsf_startup.cfg and save the current relevant VSF configuration into vsf.cfg.

Parameters: None.

Default: running-config and the relevant vsf configuration are not saved.

Command Mode: Admin Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: The device with VSF function will write the current configuration information into startup.cfg and vsf.cfg respectively when save the configuration.

Example: Save the configuration.

Switch#write

11.1.1.3 vsf port-group

Command: vsf port-group <*port-number*>

no vsf port-group <*port-number*>

Function: Configure the logic VSF port. The no command deletes the VSF port.

Parameters: <*port-number*>: the number of logic VSF port, value is 1 to 2.

Default: Do not configure.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: Configure the logic VSF port. Only two vsf port-group can be configured on the same device, they are vsf port-group1 and vsf port-group2.

Example: Configure the logic VSF port.

Switch(config)#vsf port-group 1

11.1.1.4 vsf port-group interface ethernet

Command: vsf port-group interface Ethernet <*interface-list*>

no vsf port-group interface Ethernet <*interface-list*>

Function: After created the logic VSF port, bind the actual physical port under the VSF port mode. The no command cancels the binding.

Parameters: < *interface-list* >: physical port number.

Default: The physical port is not bond as default.

Command Mode: VSF Port Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: One vsf port-group can bind 8 physical ports at most, the mode of port in vsf port-group is on. When there are more than 8 ports binding to it, it will prompt the user cannot bind. It supports spread binding of the physical port. Currently, it only supports 10G port and logic VSF port to bind.

Example: Create the logic VSF port and enter in the VSF port configuration mode. Bind the physical port 1/0/1 to the logic VSF port.

Switch(config)# vsf port-group 1

Switch(config)# vsf port-group interface ethernet 1/0/1

11.1.1.5 vsf domain

Command: vsf domain <*domain-id*>

no vsf domain

Function: Configure the logic domain that VSF is in. The no command recovers to be default of 1. When the device is in independent operation mode, the vsf domain configuration becomes effective immediately; when the device is in VSF mode, after configured vsf domain, the newest configuration will be shown in running-config, but this configuration will become effective after it is saved and restarted.

Parameters: <*domain-id*>: domain number, range is 1 to 32.

Default: The device is in domain 1.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: Domain is a kind of logic concept. The devices are connected together through VSF link; they will make up the VSF. The set of these member devices is a VSF domain. For adapting all kinds of network applications, multiple VSF can be deployed in the same network; the domain number is used to distinguish the VSF. The devices in the same domain can form the VSF; the devices or VSF groups in different domains cannot form the VSF. Before forming the VSF, it will conduct the judgement of domain numbers conflict. The default domain number is 1.

This command is not supported by the switch.

11.1.1.6 vsf member

Command: vsf member <*member-id*>

no vsf member <*member-id*>

Function: Configure the number of VSF members. The no command deletes the number.

Parameters: <*member-id*>: member number. The range is 1 to 16.

Default: There is no member number of the device.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode.

Usage Guide: The member number marks every device. In VSF group, each device has the unique member number. After configured the number, enter in the VSF mode. If configured the

command with multiple times, it will become effective the last once. There is no member number in the initialization status. After the device enter in the VSF mode, the port format will be modified according to the member number. If there is member number conflict, the VSF cannot be formed.

This command is not supported by the switch.

11.1.1.7 vsf non-wait port-inactive

Command: vsf non-wait port-inactive

no vsf non-wait port-inactive

Function: Detect the VSF link status' change quickly for discovering the vsf splitting. The no command recovers to be the default method.

Parameters: None.

Default: The quick detection of vsf link status is not configured.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

Usage Guide: After configured this command, if the vsf link status has changed, the system will receive and confirm the vsf link status immediately, and detect the vsf topology's change. This command will be effective immediately after configured. We suggest using this command when the physical vsf link is stable.

Example: Configure to detect the VSF link status' change quickly.

Switch(config)# vsf non-wait port-inactive

11.1.1.8 vsf priority

Command: vsf priority <*priority*>

no vsf priority

Function: Configure the priority of the VSF members in the VSF group. The no command recovers to be default of 1. When the device is under the independent operation mode, the priority configuration of vsf member will become effective immediately; when the device is under the VSF mode, after configured the priority of vsf member, the newest configuration will be shown in running-config, but the configuration will become effective after it is saved and restarted.

Parameters: < *priority* >: the priority value of VSF member, range is 1 to 32.

Default: 1.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode.VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: Under the independent operation mode, configure the member priority. The member priority is used for roles election, the larger the member priority value is, and the higher the priority is. The possibility of the device with higher priority becomes the Master is bigger when it is electing. Through configuring the different priorities for different devices, appoint one device as Master of VSF.

This command is not supported by the switch.

11.1.1.9 vsf auto-merge enable

Command: vsf auto-merge enable

no vsf auto-merge enable

Function: Enable the automatic merger function of VSF groups. The no command cancels this function.

Parameters: None.

Default: Disable.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: When two VSF groups have the correct connection because of some reasons, the connection method is that use the respective VSF port to connect and there is no vsf domain and vsf member id conflict, then the up of the port, VSF creating and binding will trigger the two VSF groups to merge automatically in the process of connection. In the connection, through the comparing of the priorities and member id, the VSF groups which failed to elect will restart and join in the VSF groups which successfully elected after restarting.

This command is not supported by the switch.

11.1.1.10 vsf member description

Command: vsf member <*member-id*> description <*text*>

no vsf member <*member-id*> description

Function: write some description to the member. This message will only write into the master document. No command delete that description.

Parameters: <*member-id*>： VSF member number **<*text*>：** user enter description

Default: No description in the VSF.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: Under the VSF operation mode, adding message is more easy for management. Foe example, in one network that exist of more than one VSF, or they are separate, using this method can more easy to separate them.

This command is not supported by the switch.

11.1.1.11 vsf link delay

Command: vsf link delay<*interval*>

no vsf link delay

Function: Configure the down delaying reporting function of the VSF link, using for avoid link to split and merge due to changing in short period of time. The **no** command will set the time for delay report to default value.

Parameters: <*interval*>： The VSF link down time for delay report, default valueas 0, it reports immediately.

Default: The time value is not configured as default. The value is 0.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: After configure the vsf link delay, if the VSF link status fromup to down, the port will not report to the system for this changing. After the time for configured, if the VSF link still at the down status, port will reportto the system. And the system will act. If the VSF link status from down to up, link layer will report to the system immediately. That command will become effective.

This command is not supported by the switch.

11.1.1.12 vsf mac-address persistent

Command: vsf mac-address persistent <*timer* | *always*>

no vsf mac-address persistent

Function: Configure VSF split group MAC address retention time. **No** command deletes the MAC address retention time.

Parameters: <*timer*>： Configure VSF bridge MAC retains time as 6 minutes. It means that after the master leave the VSF, the VSF bridge MAC address will remain unchang for 6 minutes. If the master cannot return to VSF within 6 minutes, the new elected master MAC bridge will become

the VSF bridge MAC; **<*always*>:** Always configure bridge MAC address forever, no matter whether the master leave or no, VSF bridge MAC will never change.

Default: Do not configure the bridge MAC retain time

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: Since VSF as a virtual facility to communicate to other media and it has the unique MAC bridge, become the VSF bridge MAC. Usually, master's bridge MAC will become the VSF bridge MAC. Bridge MAC collosion will cause the communication disorder; bridge MAC switching will cut the flow. Therefore, need to configure bridge MAC retain time. This can let the splitting occour can still depends on the user decision to retain or remove the VSF bridge MAC and the retain time Set up the timer. The master leave the VSF, the VSF bridge MAC address will remain unchang for 6 minutes. If the master cannot return to VSF within 6 minutes, the new elected CPU-MAC bridge will become the VSF bridge MAC; configure always,master leave the VSF, VSF will not restart. It will use the original CPU-MAC MAC as VSF MAC. If the VSF restarts, then using the new selected master CPU-MAC as MAC. After restart, command does not effective, need to configure again.

This command is not supported by the switch.

11.1.2 Configuration and Debugging of VSF Conflict Detection

11.1.2.1 vsf mad lacp enable

Command: vsf mad lacp enable

no vsf mad lacp enable

Function: Open the particular port-channel to support the LACP MAD detection function.**No** command will close the LACP MAD function on the port-channel LACP MAD

Parameters: None.

Default: Disable.

Command Mode: port-channelPort Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: This command can only be used at VSF operation mode; configure particular port-channel as LACP MAD collision detection group, the group member send the TLV message of

MAD.

Example: Enable the lacp mad detection function on port-channel1.

Switch(config)#interface port-channel 1

Switch(config-if-port-channel1)# vsf mad lacp enable

This command is not supported by the switch.

11.1.2.2 vsf mad bfd enable

Command: vsf mad bfd enable

no vsf mad bfd enable

Function: Open the interface to support BFD MAD detection function. The **No** command will closing the particular interface BFD MAD detection function.

Parameters: None.

Default: Disable.

Command Mode: Interface Configuration Mode.

Operation Mode: VSF Operation Mode and Network Management Port Configuration Mode.

VSF Role: VSF Master.

Usage Guide: This command can only be used at VSF operation mode; configure particular port to support the BFD MAD detection function.

Example: Enable the BFD MAD detection function of interface vlan 2.

Switch(config)# interface vlan 2

Switch(config-if-vlan2)# vsf mad bfd enable

11.1.2.3 vsf mad ip address

Command: vsf mad ip address *<ip-address>* *<ip-mask>* member *<member-number>*

no vsf mad ip address *<ip-address>* *<ip-mask>* member *<member-number>*

Function: Appoint the particular establish member facility corresponding to BFD conversation.

Parameters: ***<ip-address>*** : IP address, ***<ip-mask>*** : IP address mask, ***<member-number>***: Member facilities number, the range is 1-16.

Default: MAD address is not configured.

Command Mode: Interface Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: This command can only be used at VSF operation mode, this commandcan also establish configuration address to conversation to outlying address.

Example: Create the BFD conversation of the member device on interface vlan 2.

```
Switch(config)# interface vlan 2
Switch(config-if-vlan2)# vsf mad ip address 2.1.1.1 255.255.255.0 member 1
Switch(config-if-vlan2)# vsf mad ip address 2.1.1.2 255.255.255.0 member 2
```

11.1.2.4 vsf mad exclude

Command: vsf mad exclude

no vsf mad exclude

Function: When the facilities ente into the recovery status, the port that configure this command can avoid closing and continuous transmitting. No command is delete the MAD retention port configuration.

Parameters: None.

Default: MAD retention port is not configured.

Command Mode: Port Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: VSF split off, the network will present of 2 global configuration entirety the same facilities. This facilities connect to the network may cause network berak down. In order to prevent this happen, the system will have multi Active detection, at the end will only retain one Active facility, th others will enter into Recovery status. Also, it will close all the operation ports that are on the Recovery status. Using this command can appoint which port is not closed and reserve the right to the user.

Example: Configure the MAD keeping port on port2/1/4.

```
Switch(config)# inte e 2/1/4
Switch (config-if-ethernet2/1/4)#vsf mad exclude
```

11.1.2.5 vsf mad restore

Command: vsf mad restore

Function: This command will recover the VSF which at Recovery state to the normal working status.

Parameters: None.

Default: restore is not configured.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: VSF link broken will have Active collision, the original VSF willsplit into 2 Active VSF. In order to prevent the collision in the network, VSF system will through multi Active detection machinism, putting one of the VSF status as Active (continuous for work), other VSFs just amend as Recovery status (which cannot tackle with the operation messages). If the VSF that at Active status has broke down, at this moment, can using this command to change the VSF which is at Recovery state to normal working status.

Example: Recover the VSF which is at Recovery state to the normal working status.

Switch(config)#vsf mad restore

11.1.2.6 show mad config

Command: show mad config

Function: Show status of VSF MAD configuration, through this command can check the LACP MAD and BFD MAD configuration

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: None.

11.1.3 VSF Debugging

11.1.3.1 show running-config

Command: show running-config

Function: Check the entire current configuration message.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: Independent Operation Mode.VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: After the VSF function, this command will put the VSF related configuration

message together and place in the top for display.

Example:

Switch#show running-config

11.1.3.2 show vsf

Command: show vsf

Function: Display the related message to all facilities in the VSF, including theVSF master, backup master, VSF CPU-MAC, VSF bridge MAC, description of facilities, the priority of member, whether to check the edition can in-phase, the configuration message that in the preserving function of bridge MAC address, after the merge of VSF whether the function are workable, VSF domain etc.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: This command can only be used under the VSF mode, through the VSF protocol to obtain the role election message. Throughout the reading of each configuration document vsf.cfg to obtain the configuration message, bridge MAC, CPU-MAC etc message display.

Example:

```
Switch# sho vsf
Switch    SlotID    Role    Priority    CPU-Mac                Description
--------------------------------------------------------------------------------
2         M1        M       1           00-03-0f-0f-66-b4      (null)
2         7         S       1           00-03-0f-0f-66-b4      (null)
The Bridge Mac of the VSF is: 00-03-0f-0f-66-b4
Auto Merge: yes
Mac Persistent: off
Domain ID: 1
```

11.1.3.3 show vsf topology

Command: show vsf topology

Function: Display the current vsf topology message.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: VSF merge or leave of the member in the VSF, all of this will touch off protocol operation and calculate the new topology structure. Throughout this command, it can obtain current topology information.

Example:

```
Switch# show vsf topology
Switch    VSF-Port1                 Neighbor VSF-Port2          Neighbor
2         Ethernet2/7/3(inactive)   --       --                 --
```

11.1.3.4 show vsf-config

Command: show vsf-config

Function: According to the order of the facilities to display the VSF configuration message, member id, priority of the member and the VSF port information of member.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: When the VSF stand-alone facility formed, will collect the VSF configuration of that machine. If the VSF contains of several of machines, it will send the collection request to other facilities and collect entire VSF configuration information.

Example: 。

```
Switch# show vsf config
MemberID    Priority    VSF-Port1          VSF-Port2
2           1           Ethernet2/7/3      --
```

11.1.3.5 show mad config

Command: show mad config

Function: Checking the current VSF mad detection configuration.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: This command can only be use under the VSF operation mode. Displays whether LACP, BFD are opened and obtins which port has open these functions.

Example:

Switch# show mad config

Current lacp MAD status: Disable

Current bfd MAD status: Detecting

Reserved ports:

Reserved ports(defaults):

interface Ethernet2/7/3

MAD lacp enabled aggregation port:

MAD BFD enabled interface:

Interface Vlan10

vsf mad ip address 10.1.1.1 255.255.255.0 member 1

vsf mad ip address 10.1.1.2 255.255.255.0 member 2

Display Message	Explaination
Current lacp MAD status	Show the current status of lacp MAD
Current bfd MAD status	Show the current status of BFD MAD
Reserved ports	The reserved ports user configured
Reserved ports(defaults)	Default reserved port (not need for configuration, default)
MAD lacp enabled aggregation port	Enable LACP MAD aggregate port
MAD BFD enabled interface	Enable BFD MAD port

11.1.3.6 show vsf cpu-database all-member brief-information

Command: show vsf cpu-database all-member brief-information

Function: Display all members' brief message in CPU database.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: Display all members' brief message in CPU database.

Example:

Switch# show vsf cpu-database all-member brief-information

Vsf cpu database include 1 member:

Member 2 : cpu key:00-03-0f-0f-66-b4, PRI:1

Master is : 2, Standby is : 0

11.1.3.7 show vsf cpu-database member basic-information

Command: show vsf cpu-database [member <*1-16*>| basic information]

Function: Display entire vsf or particular member CPU database basic information.

Parameters: < *member* >: VSF member, **<1-16>:** VSF member member id.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: Display entire vsf or particular member CPU database basic information

Example:

Switch# show vsf cpu-database member 2 basic-information

Vsf cpu database member 2 basic information:

Key: 00-03-0f-0f-66-b4

CPU-MAC: 00-03-0f-0f-66-b4

Member ID: 2

Domain ID: 1

Sequence Num: 4

Master Prioriy: 1

Units Num: 1

Dest unit: 1

Dest port: 0

Unit prefer module id: 2

Unit require module id num: 1

Vsf port num: 1

Flags: 131072

Vsf port index 1:

Unit: 0

port: 1

Weight: 0

Bflag: 1

11.1.3.8 show vsf cpu-database member running-information

Command: show vsf cpu-database [member <*1-16*>| running-information]

Function: Display CPU database operation information.

Parameters: < *member* >: VSF member, **<1-16>:** VSF member member id.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: Display entire or particular member operation information in CPU database.

Example:

Switch# show vsf cpu-database member 1 running-information

%Member 1 not exist in the cpu-database!

Switch# show vsf cpu-database member 2 running-information

Vsf cpu database member 2 running information:

Flags: 1

Tx unit: 0

Tx port: 0

Dest module: 2

Dest port: 0

Module ID: 2

Topo index: 0

Vsf port index 1 link info:

Flags: 0

Tx cpu key:

Tx port-group: 0

Rx cpu key:

Rx port-group: 0

11.1.3.9 show vsf cpu-database member port-information

Command: show vsf cpu-database [member <*1-16*>| port-information]

Function: Display CPU database VSF basic information.

Parameters: < *member* >: VSF member, **<1-16>:** VSF member member id.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: Show the VSF basic information of the entire or the appointed VSF member in CPU database.

Example:

Switch# show vsf cpu-database member 2 port-information

Vsf cpu database member 2 port information:

Vsf port index 1:

Unit: 0

port: 1

Weight: 0

Bflag: 1

11.1.3.10 show vsf cpu-database member port-link-information

Command: show vsf cpu-database [member <*1-16*>| port-link-information]

Function: Display CPU database VSF port connection message.

Parameters: < *member* >: VSF member, **<1-16>:** VSF member member id.

Default: None.

Command Mode: Admin and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guide: None.

Example:

Switch# show vsf cpu-database port-link-information

Vsf cpu database member 1 include 2 vsf port:

Vsf port index 1 link info:

Flags:1

Tx cpu key:00-01-05-11-11-11

Tx stk idx:1

Rx cpu key: 00-01-05-11-11-11

Rx cpu key:1

Vsf port index 2 link info:

Flags:1

Tx cpu key:00-01-05-11-11-12

Tx stk idx:2

Rx cpu key: 00-01-05-11-11-12

Rx cpu key:2

11.1.3.11 show slot

Command: show [member <member-id>] slot <**slot-id>**

Function: Show basic information of each chip.

Parameter: ***<mem-id>*** is the member device number under the VSF mode, range is 1 to 16; ***<slot-id>*** is the number of the slot the chip resides, all the slots are 1 for the cassette devices.

Default: All chip information will be listed by default if mem-id and slot-id are not specified
Command Mode: Admin Mode.
Example:
Switch#show member 13 slot 1

----------member :13----------
Inserted : YES
Module type : Switch
Work mode : STANDBY MASTER
Work state : RUNNING
Software package version : 7.0.3.0(R0075.0011)
Bootrom version : 7.2.2
CPLD version : N/A
Hardware version : 1.0.1
Part number : N110900062
Manufacture date : 2011/03/10
Temperature : 39C/102F
Uptime : 0 weeks, 0 days, 1 hours, 37 minutes

11.1.3.12 debug vsf packet detail <alive | all | config | member-infor | probe | routing | topo>

Command: debug vsf packet detail <alive | all | config | member-infor | probe | routing | topo>

no debug vsf packet detail <alive | all | config | member-infor | probe | r routing | topo>

Function: Enable all kinds of VSF protocol packets viewing on-off. The no command disables it.

Parameters: ***<alive>***：keep-alive packets; ***<all>***：enable all VSF protocol packets; ***<config>***：Configure the information packet, this parameter means the packets interaction in viewing the config. In this stage, VSF members achieves the necessary information of master election through packets interaction to elect the master and standby master; ***<member-infor>***：member information packets; ***<probe>***：VSF member detection packets, it is used to detect the connection information of all the VSF ports; ***<routing>***：VSF member information spreading packets, the information includes: local VSF port information, the modid information needed, number of chips information, Master election priority, CPUDB status information and the chip number and port number information which reach this CPU; ***<topo>***：Topology analysis packets, the task in the stage of topology analysis is that Master calculates the network without loop according to the

topology information and distributes the Module ID for all members. It will calculate the relationship between each member VSF port and the destination Module ID and then Master issues these results to each member.

Default: Disable.

Command Mode: Admin Mode.

VSF Role: VSF Master, member and line card.

Usage Guide: The VSF groups will go through the stages of discovery and topology analysis in forming. At different stages, the device will be in different status, such as discovery. The device goes through the sub-stages of probe, routing and config respectively. Through this debug on-off, the details of the corresponding protocol packets in different stages can be selected inquiried.

11.1.3.13 debug vsf packet

Command: debug vsf packet <all | receive | send> vsf-port <vsf-port-number>

no debug vsf packet <all | receive | send> vsf-port <vsf-port-number>

Function: Open the VSF packets debug on-off. The no command will close this debug function.

Parameters: <*receive*>: Enable the VSF packets debug on-off received; **<*send*>:** Enable the VSF packets debug on-off sent; **<*all*>:** Enable the received and sent; **<*vsf-port-id*>:** VSF port number.

Default: Disable.

Command Mode: Admin Mode.

VSF Role: VSF Master, Member and Slave.

Usage Guide: After open the VSF packets debug on-off, it can see the VSF protocol message receive.

11.1.3.14 debug vsf event

Command: debug vsf event

no debug vsf event

Function: Open the switch of VSF event debug information. **No** command is closing this debug function

Parameters: None.

Default: Disable.

Command Mode: Admin Mode.

VSF Role: VSF Master, Member and Slave.

Usage Guide: After open the on-off of VSF event debug information, the VSF operates to the defined events in all stages, it can provide corresponding feedback to the user.

11.1.3.15 debug vsf error

Command: debug vsf error

no debug vsf error

Function: Open the switch of the VSF debug on-off. **No** command is closing the debug function.

Parameters: None.

Default: None.

Default: Disable.

Command Mode: Admin Mode.

VSF Role: VSF Master, Member and Slave.

Usage Guide: After open the debug, it can display the error messages for all stages during the VSF.

Chapter 12 Commands for DataCenter

12.1 Commands for MC-LAG

12.1.1 evpn nve mac-address

Command: evpn nve mac-address FF-FF-FF-FF-FF-FF
no evpn nve mac-address

Function: Configure the MAC address of VTEP globally.

Parameters: FF-FF-FF-FF-FF-FF: The MAC address of VTEP.

Command Mode: Global Mode.

Default: CPU MAC address of mc-lag master.

Usage Guide: In the scenario of establishing vxlan distributed gateway using BGP evpn, when deploying mc-lag vxlan dual homing access, it is necessary to configure the same VTEP MAC address on the two devices constituting vxlan dual homing access to ensure normal traffic forwarding on the gateway in vxlan network; The no command is used to restore the default VTEP MAC address.

Example: Configure the MAC address of VTEP as 00-01-02-03-04-05.

Switch(config)#evpn nve mac-address 00-01-02-03-04-05

12.1.2 mac-address

Command: mac-address XX-XX-XX-XX-XX-XX
no mac-address

Function: Configure the MAC address of the gateway interface.

Parameters: XX-XX-XX-XX-XX-XX: The MAC address of the gateway interface.

Command Mode: VLAN interface mode, NVI interface mode.

Default: None.

Usage Guide: When the MC-LAG device is used as a Layer 3 gateway, the gateway interfaces of the two devices on the same network segment need to be configured with the same MAC address; The no command deletes the configured MAC address.

Examples: Configure the MAC address of the gateway interface VLAN 10 as 02-02-02-02-02-02.

switch(config)#interface vlan 10

switch(config-if-vlan10)#mac-address 02-02-02-02-02-02

12.1.3 mclag

Command: [no] mclag

Function: Enter mc-lag configuration mode.

Parameters: None.

Command Mode: Global Mode.

Default: None.

Usage Guide: Enter the mc-lag configuration mode after executing mclag; The no command deletes the configuration under mclag and exits the mc-lag configuration mode.

Examples: Enter mc-lag configuration mode.

```
switch(config)#mclag
switch(config-mclag)#
```

12.1.4 mclag domain-id

Command: mclag domain-id <1-128>

no mclag domain-id

Function: Configure mc-lag domain ID.

Parameters: Domain ID range: 1-128.

Command Mode: MC-LAG Mode.

Default: None.

Usage Guide: The domain IDs of the two devices constituting mc-lag must be consistent; The no command is used to delete the domain ID configuration.

Examples: Configure mc-lag domain ID to 10.

```
Switch(config-mclag)#mclag domain-id 10
```

12.1.5 mclag priority

Command: mclag priority <1-256>

no mclag priority

Function: Configure mc-lag domain priority.

Parameters: Domain priority range: 1-256.

Command: MC-LAG Mode.

Default: 128.

Usage Guide: Configure the mc-lag domain priority. The smaller the value, the higher the priority. The equipment with high priority becomes the mc-lag master equipment; The no command restores the default domain priority.

Example: Configure mc-lag domain priority to 100.

```
switch(config-mclag)#mclag priority 100
```

12.1.6 mclag enable

Command: [no] mclag enable

Function: Enable mc-lag function.

Parameters: None.

Command Mode: MC-LAG Mode.

Default: None.

Usage Guide: Enable mc-lag function; The no command is used to disable the mc-lag function.
Example: Enable mc-lag function.
switch(config-mclag)#mclag enable

12.1.7 mclag group

Command: [no] mclag group
Function: Configure port group to join mc-lag group.
Parameters: None.
Command Mode: Port-channel Port Mode.
Default: None.
Usage Guide: Configure port group to join mc-lag group; The no command is used to configure the port group to leave the mc-lag group.
Example: Configure port group 10 to join mc-lag group.
switch(config-if-port-channel10)#mclag group

12.1.8 mclag local-ip

Command: mclag local-ip A.B.C.D
no mclag local-ip
Function: Configure the IP address of the layer 3 interface of the local mc-lag control link.
Parameters: A.B.C.D IP address.
Command Mode: MC-LAG Mode.
Default: None.
Usage Guide: Configure the IP address of the layer 3 interface of the local mc-lag control link; The no command is used to cancel the configuration of the local IP address.
Examples: Configure the IP address of the layer 3 interface of the local mc-lag control link as 20.4.4.4.
switch(config-mclag)#mclag local-ip 20.4.4.4

12.1.9 mclag peer-ip

Command: mclag peer-ip A.B.C.D
no mclag peer-ip
Function: Configure the IP address of the layer 3 interface of the peer's mc-lag control link.
Parameters: A.B.C.D IP address.
Command Mode: MC-LAG Mode.
Default: None.
Usage Guide: Configure the IP address of the layer 3 interface of the peer's mc-lag control link; The no command is used to cancel the configuration of the peer's IP address.
Examples: Configure the IP address of the layer 3 interface of the peer's mc-lag control link as 20.2.2.2.
switch(config-mclag)#mclag peer-ip 20.2.2.2

12.1.10 ip address

Command: ip address <ipaddress> <mask> [secondary] [mc-lag]

no ip address <ipaddress> <mask> [secondary] [mc-lag]

Function: Configure an independent IPv4 address for the MC-LAG on Layer 3 gateway.

Parameter: Parameter **<ipaddress>** IP address, dot decimal format; Parameter **<mask>** IP address masking;Parameter **[secondary]**Indicates that the configured IP address is a secondary IP address;Parameter **[mc-lag]**The secondary address is an independent external IPv4 address of the MC-LAG Layer 3 gateway

Command mode: VLAN interface Mode

Default: None.

Usage Guide: Only one ip address mc-lag can be configured for a VLAN interface, The secondary IP address of MC-LAG must be on the same network segment as the primary IP address.The no command is used to unset the configuration.

Example: Set The independent external IPv4 address of MC-LAG on the VLAN 10 interface with 10.10.1.3.

Switch(config-if-vlan10)#ip address 10.10.1.3 255.255.255.0 secondary mclag

12.1.11 ipv6 address

Command: ipv6 address <ipv6address | prefix-length> [eui-64] [mc-lag]

no ipv6 address <ipv6address | prefix-length> [eui-64] [mc-lag]

Function: Configure an independent IPv6 address for the MC-LAG on Layer 3 gateway.

Parameter: Parameter ***<ipv6-address>*** is the prefix of IPv6 address, parameter ***<prefix-length>*** is the prefix length of IPv6 address, which is between 3-128, **eui-64** means IPv6 address is generated automatically based on eui64 interface identifier of the interface; Parameter **[mc-lag]**The secondary address is an independent external IPv6 address of the MC-LAG Layer 3 gateway

Command mode: VLAN interface Mode

Default: None.

Usage Guide: Only one ipv6 MC-LAG global unicast address and one MC-LAG linklocal address can be configured for a VLAN interface. The ipv6 address of MC-LAG must be on the same network segment as one of the other IPv6 addresses. The no command is used to unset the configuration.

Example: Set The independent external IPv6 unicast address of MC-LAG on the VLAN 10 interface with 2022::3.

Switch(config-if-vlan10)#ipv6 address 2022::3/64 mclag

Set The independent external IPv6 linklocal address of MC-LAG on the VLAN 10 interface with fe80::3

Switch(config-if-vlan10)#ipv6 address fe80::3/64 mclag

12.1.12 mclag dad link

Command: mclag dad link local <X.X.X.X> peer < X.X.X.X >

no mclag dad link local <X.X.X.X> peer < X.X.X.X >

Function: Configure the local interface IP address of the active-master detection link and the IP address of the peer device.

Parameter: Parameter **local <X.X.X.X>** is local interface IP address, Parameter **peer <X.X.X.X>** is local interface IP address

Command mode: MC-LAG Configuration Mode

Default: None.

Usage Guide: The dual-master detection function requires routing is reachable.

Example: Set the local interface IP address of the active-master detection link with 24.24.1.1, and the IP address of the peer device with 24.24.1.2.

Switch(config-mclag)#mclag dad link local 24.24.1.1 peer 24.24.1.2

12.1.13 error-down exclude

Command: error-down exclude

no error-down exclude

Function: Configure that the local physical port and port-group do not error-down.

Parameter: Parameter **error-down** is disable the Slave port while MC-LAG detected dual-active; **exclude** means exclude this port.

Command mode: Interface Configuration Mode

Default: None.

Usage Guide: The ports of Slave device configed error-down exclude will not be error-down while MC-LAG detected dual-active.

Example: Set the port ethernet1/0/1 error-down exclude.

Switch(config-if-ethernet1/0/1)#error-down exclude

12.1.14 mclag up-delay

Command: mclag up-delay <interval>

no mc-lag up-delay <interval>

Function: Configure the MC-LAG ports delay to UP.

Parameter: Parameter **up-delay** is MC-LAG ports delay to up; Parameter **<interval>** is the time.The unit of time is seconds.

Command mode: MC-LAG Configuration Mode

Default: 120s.

Usage Guide: Scenarios for control link fault recovery, you can configure the delay time for the MC-LAG port to UP to improve the failback performance.

Example: Set the port ethernet1/0/1 up-delay time with 60s.

Switch(config-mclag)#mclag up-delay 60

12.1.15 mclag probe-interval

Command: mclag probe-interval <interval>

no mclag probe-interval <interval>

Function: Configure the MC-LAG probe interval.

Parameter: Parameter **probe-interval** is MC-LAG keepalive packet send interval; Parameter **<interval>** is the time, 2-90s.

Command mode: MC-LAG Configuration Mode

Default: 60s.

Usage Guide: Configure the MC-LAG probe interva, if there is no echo packet or control packet received after two probe-intervals, the MC-LAG changes to the INACTIVE state.

Example: Set the MC-LAG probe interva with 30s.

Switch(config-mclag)#mclag probe-interval 30

12.1.16 show mclag

Command: show mclag

Function: Show mc-lag configuration and status information.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: None.

Example: Show mc-lag configuration and status information.

```
Switch#show mclag
mclag domain_id    : 10
mclag priority         : 128
mclag local system_id    : 90-3c-b3-95-0e-d7
mclag peer system_id    : 90-3c-b3-95-10-eb
mclag domain state    : MDS_READY
mclag ctrlink state    : MCLAG_CTL_ACTIVE
mclag tunlink state    : MCLAG_TUN_UP
mclag master       : LOCAL
```

12.1.17 show mclag group

Command: show mclag group (<1-128> |)

Function: Show mc-lag group configuration and status information.

Parameters: Group ID range: 1-128.

Command Mode: Admin Mode.

Default: None.

Usage Guide: None.

Example: Show mc-lag group configuration and status information.

```
Switch#show mclag group
*********mclag group info     :*********
group id:1
group state:ACTIVE
local link num:1
portname                    status
Ethernet1/0/21              aggregate
peer link num:1
peer-portname               status
Ethernet1/0/21              aggregate
```

12.1.18 switchport mclag data link

Command: [no] switchport mclag data link

Function: Configure the local mc-lag data link port.

Parameters: None.

Command Mode: Port Mode, Port-channel Port Mode

Default: None.

Usage Guide: Configure the local mc-lag data link port; The no command is used to cancel the configuration of the local data link port.

Example: Configure Ethernet 1/6/1 as the local mc-lag data link port.

```
Switch(config-if-ethernet1/6/1)#switchport mclag data link
```

12.1.19 virtual-equipment-group ID

Command: [no] virtual-equipment-group <ID>

Function: Configure VEG group.

Parameters: ID of virtual equipment group, range: 1-1.

Command Mode: Global Mode.

Default: None.

Usage Guide: Configure the VEG group. MC-LAG needs to be associated with the VEG group to synchronize mac/arp/nd entries.The no command is used to unconfigured a VEG group.

Example: Configure VEG group 1.

Switch(config)#virtual-equipment-group 1

12.1.20 virtual-equipment-group ID

Command: [no] virtual-equipment-group <ID>

Function: Associate VEG group with mc-lag.

Parameters: ID of virtual equipment group, range: 1-1.

Command Mode: MC-LAG Mode.

Default: None.

Usage Guide: Configure the VEG group to associate with mc-lag, and realize the synchronization of MAC / ARP / ND table entries between two mc-lag devices through the VEG function. At the same time, the source IP and remote IP configured under the VEG will be deleted, and the local IP and peer IP configured on mc-lag will be automatically associated; The no command is used to disassociate the VEG group with mc-lag.

Example: Associate VEG group 1 with mc-lag.

Switch(config-mclag)#virtual-equipment-group 1

12.1.21 virtual-equipment-group ID

Command: [no] virtual-equipment-group <ID>

Function: Configure the gateway interface to bind the VEG group.

Parameters: ID of virtual equipment group, range: 1-1.

Command Mode: VLAN interface mode, NVI interface mode.

Default: None.

Usage Guide: Configure the gateway interface to bind the VEG group; The no command is used to unbind the gateway interface to the VEG group.

Example: Configure interface Vlan4 to bind VEG group 1.

Switch(config)#interface vlan 4

Switch(config-if-vlan4)#virtual-equipment-group 1

12.2 Commands for NETCONF

12.2.1 netconf server enable

Commands：netconf server enable

no netconf server enable

Function：Enable netconf function; The no operation of this command is to disable the netconf function.

Command mode：Global configuration mode.

Default：Not configured by default.

Usage Guide：none

Example：start netconf

Switch(config)# netconf server enable

netconf server is enabled

12.2.2 show netconf session

Commands：show netconf session

Function：Use this command to view the session information of netconf.

Command mode：Privileged mode or global configuration mode.

Default：Not configured by default.

Usage Guide：You need to enable the netconf function and connect the client to view the current session information. When using the netconf server to connect to the client, pay attention to ensuring network connectivity.

Example：View netconf session information

Switch(config)# show netconf session

session_id:1

transport:netconf-ssh

username:test

source-host:172.30.8.120

login-time:2021-07-20T15:46:40+02:00

in-rpcs:0

in-bad-rpcs:0

out-rpc-errors:0

out-notifications:0

12.2.3 show netconf tcp

Commands：show netconf tcp

Function：Use this command to view user information connected to netconf.

Command mode：Privileged mode or global configuration mode.

Default：Not configured by default.

Usage Guide： You need to enable the netconf function and connect the client to view the current user information. When using the netconf server to connect to the client, pay attention to ensuring network connectivity.

Example： View user information connected to netconf

Switch(config)# show netconf tcp

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State	IF	VRF
0.0.0.0	830	0.0.0.0	*	LISTEN	0	0
172.17.100.34	830	172.30.8.120	57924	ESTABLISHED	3527	0

12.3 Commands for Telemetry

12.3.1 Telemetry

Command: telemetry

Function: Create telemetry mode.

Default: Telemetry is not configured.

Command Mode: Config mode.

Usage Guide: Enter the telemetry mode and configure all the configurations of the telemetry function.

Example: Enter the telemetry mode.

Switch(config)#telemetry

Switch(config-telemetry)#exit

12.3.2 grpc-sever

Command: grpc server x.x.x.x port <10000-57999>

no grpc server

Function: Configure the server address and tcp listening port for dynamic subscription.

Parameter: x.x.x.x: ipv4 address;

<10000-57999>: tcp listening port.

Default: Telemetry is not configured.

Command Mode: Telemetry mode.

Usage Guide: This command can only be configured in telemetry mode, and ip needs to be the local IP address accessible by the client.

Example:

Switch(config-telemetry)#grpc server 192.168.1.1 port 10002

Switch(config-telemetry)#no grpc server

12.3.3 destination-group

Command: destination-group WORD

no destination-group WORD

Function: Configure the name of the destination group for static subscriptions.

Parameter: WORD: A string of length 64 or less.

Default: Telemetry is not configured.

Command Mode: Telemetry mode.

Usage Guide: This command can only be configured in telemetry mode, the string length cannot exceed 64, and a maximum of 5 groups can be configured.

Example:

Switch(config-telemetry)#destination-group abcdefgh
Switch(config-telemetry-dest-group-abcdefgh)#
Switch(config-telemetry)#no destination-group abcdefgh

12.3.4 destination-group ipv4-address

Command: ipv4-address x.x.x.x port <1-65535>

no ipv4-address x.x.x.x port <1-65535>

Function: Configure the target collector ip and tcp port in the destination group of the static subscription in telemetry.

Parameter: x.x.x.x: ipv4 address;

<**1-65535**>: tcp listening port.

Default: Telemetry is not configured.

Command Mode: destination-group mode.

Usage Guide: This command can only be configured in telemetry mode.

Example:

Switch(config-telemetry)#destination-group abcdefgh
Switch(config-telemetry-dest-group-abcdefgh)#ipv4-address 172.17.30.96 port 50002
Switch(config-telemetry-dest-group-abcdefgh)#no ipv4-address 172.17.30.96 port 50002

12.3.5 sensor-group

Command: sensor-group WORD

no sensor-group WORD

Function: Configure the name of the sampling group.

Parameter: WORD: A string of length 64 or less.

Default: Telemetry is not configured.

Command Mode: Telemetry mode.

Usage Guide: This command can only be configured in telemetry mode, the string length cannot exceed 64, and a maximum of 5 groups can be configured.

Example:

Switch(config-telemetry)#sensor-group abcdefgh
Switch(config-telemetry-sen-group-abcdefgh)#
Switch(config-telemetry)#no sensor-group abcdefgh

12.3.6 sensor-group path memoryInfo

Command: sensor-path memoryInfo (| (op-type (eq | ge | gt | le | lt) op-value <1-100> (| ((and | or) op-type (eq | ge | gt | le | lt) op-value <1-100>))))

no sensor-path memoryInfo

Function: Configure the sensor paths and constraints in the sensor group of static subscriptions in telemetry.

Parameter: op-type: Configure the constraints of the sampling path.

op-value: Parameters that configure the constraints of the sampling path.

Default: Telemetry is not configured.

Command Mode: Telemetry mode.

Usage Guide: This command can only be configured in sensor group mode in telemetry mode. Restrictions can be configured in combination. To configure a new restriction, you need to delete the original restriction, and and, or or, ge is greater than or equal to, le is less than or equal to, and eq is equal to , gt is greater than, lt is less than.

Example:

Switch(config-telemetry)#sensor-group abcdefgh

Switch(config-telemetry-sen-group-abcdefgh)#sensor-path MemoryInfo op-type le op-value 10 or op-type ge op-value 19

Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path memoryInfo

12.3.7 sensor-group path cpuInfo

Command: sensor-path cpuInfo (| (op-type (eq | ge | gt | le | lt) op-value <1-100> (| ((and | or) op-type (eq | ge | gt | le | lt) op-value <1-100>))))

no sensor-path cpuInfo

Function: Configure the sensor paths and constraints in the sensor group of static subscriptions in telemetry.

Parameter: op-type: Configure the constraints of the sampling path.

op-value: Parameters that configure the constraints of the sampling path.

Default: Telemetry is not configured.

Command Mode: Telemetry mode.

Usage Guide: This command can only be configured in sensor group mode in telemetry mode. Restrictions can be configured in combination. To configure a new restriction, you need to delete the original restriction, and and, or or, ge is greater than or equal to, le is less than or equal to, and eq is equal to , gt is greater than, lt is less than.

Example:

Switch(config-telemetry)#sensor-group abcdefgh

Switch(config-telemetry-sen-group-abcdefgh)#sensor-path cpuInfo op-type le op-value 10 or op-type ge op-value 19

Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path cpuInfo

12.3.8 sensor-group path ifStatistics

Command: sensor-path ifStatistics ((ethernet | port-channel) IFNAME|)
no sensor-path ifStatistics ((ethernet | port-channel) IFNAME|)
Function: Configure the sensor paths and constraints in the sensor group of static subscriptions in telemetry.
Parameter: ethernet : Configure the ethernet port in the sensor path.
port-channel: Configure the lag port in the sensor path.
IFNAME: Port name.
Default: Telemetry is not configured.
Command Mode: Telemetry mode.
Usage Guide: This command can be configured only in sensor group mode. Without the interface parameter, all Layer 2 ports and lag ports are sampled.
Example:
Switch(config-telemetry)#sensor-group abcdefgh
Switch(config-telemetry-sen-group-abcdefgh)#sensor-path ifStatistics ethernet 1/0/1
Switch(config-telemetry-sen-group-abcdefgh)#sensor-path ifStatistics port-channel 1
Switch(config-telemetry-sen-group-abcdefgh)#sensor-path ifStatistics
Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path ifStatistics
Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path ifStatistics ethernet 1/0/1
Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path ifStatistics port-channel 1

12.3.9 subscription

Command: subscription WORD
no subscription WORD
Function: Configure subscription groups.
Parameter: WORD: A string of length 64 or less.
Default: Telemetry is not configured.
Command Mode: Telemetry mode.
Usage Guide: This command can only be configured in telemetry mode, the string length cannot exceed 64, and a maximum of 5 groups can be configured.
Example:
Switch(config-telemetry)#subscription abcdefgh
Switch(config-telemetry-sub-group-abcdefgh)#
Switch(config-telemetry)#no subscription abcdefgh

12.3.10 subscription destination-group

Command: destination-group WORD
no destination-group WORD
Function: Configure the name of the associated destination group.
Parameter: WORD: destination-group name.

Default: Telemetry is not configured.
Command Mode: Telemetry mode.
Usage Guide: This command can only be configured in telemetry mode, the length of the string does not exceed 64, and the destination group needs to be configured in advance before it can be bound to the subscription group.
Example:
Switch(config-telemetry)#destination-group 1
Switch(config-telemetry-dest-group-1)#exit
Switch(config-telemetry)#subscription 2
Switch(config-telemetry-sub-group-2)#destination-group 1
Switch(config-telemetry-sub-group-2)#no destination-group 1

12.3.11 subscription sensor-group

Command: sensor-group WORD sample-interval <10000-1800000>
no sensor-group WORD
Function: Configure the associated sensor group and sample interval.
Parameter: WORD: sensor group name.
sample-interva: **10000ms-1800000ms**
Default: Telemetry is not configured.
Command Mode: Telemetry mode.
Usage Guide: This command can only be configured in telemetry mode, the string length does not exceed 64, and the sensor group needs to be configured in advance before it can be bound to the subscription group. The actual configurable values of the sampling interval are 10s, 30s, 60s, 180s, 300s, 900s, 1800s.
Example:
Switch(config-telemetry)#sensor-group 1
Switch(config-telemetry-sen-group-1)#exit
Switch(config-telemetry)#subscription 2
Switch(config-telemetry-sub-group-2)#sensor-group 1 sample-interval 10000
Switch(config-telemetry-sub-group-2)#no sensor-group 1

12.3.12 tun interface vlan

Commands：tun interface vlan <vlan-id | WORD>
no tun interface vlan <vlan-id | WORD>
Function：When using the device business port as a management port, it is necessary to enable the Tun function on the VLAN where the business port is located.
Parameters: <vlan id>is the VLAN ID of an established VLAN, with a value range of 1 to 4094.
<WORLD>Multiple VLAN combinations or ranges, such as 100, 200, 300-400.
Command mode：Global configuration mode.

Default： Not configured by default.

Usage Guide： When the business port is used as the telemetry management port, enable the tun function.

Example： Use 192.168.60.100 of interface vlan 100 as the telemetry management IP and enable tun functionality.

```
Switch(config)#interface Vlan100
Switch(config)#ip address 192.168.60.100 255.255.255.0
Switch(config)#interface ethernet 3/0/1
Switch(config-if-ethernet3/0/1)#switchport access vlan 100
Switch(config-if-ethernet3/0/1)#exit
Switch(config)#tun interface vlan 100
Switch(Config)#
```

12.3.13 show telemetry subscription

Command: show telemetry subscription

Function: Displays all configurations for static subscriptions in telemetry.

Parameter: null

Default: Telemetry is not configured.

Command Mode: All mode.

Usage Guide: This command can be configured only in telemetry mode, and will display all configurations of the destination group, sensor group, and subscription group in the current static subscription.

Example:

```
Switch(config)#telemetry
Switch(config-telemetry)#destination-group 1
Switch(config-telemetry-dest-group-1)#ipv4-address 172.17.9.26 port 50002
Switch(config-telemetry-dest-group-1)#exit
Switch(config-telemetry)#sensor-group 2
Switch(config-telemetry-sen-group-2)#sensor-path ifStatistics
Switch(config-telemetry-sen-group-2)#sensor-path cpuInfo
Switch(config-telemetry-sen-group-2)#sensor-path memoryInfo
Switch(config-telemetry-sen-group-2)#exit
Switch(config-telemetry)#subscription 3
Switch(config-telemetry-sub-group-3)#destination-group 1
Switch(config-telemetry-sub-group-3)#sensor-group 2 sample-interval 10000
Switch(config-telemetry-sub-group-3)#
Switch(config-telemetry-sub-group-3)#
Switch(config-telemetry-sub-group-3)#show telemetry subscription

------------------------------------------------------
destination_group: 1
```

destination_ip_addr: 172.17.9.26:50002

---
sensor_group: 2
sensor_group_path: ifStatistics
sensor_group_path: MemoryInfo
sensor_group_path: CpuInfo

---
subscription_group: 3
subscription_destination_group: 1
subscription_sensor_group: 2
subscription_sample_interval: 10000 ms

Switch(config-telemetry-sub-group-3)#

12.3.14 show telemetry dynamic-subscription

Command: show telemetry dynamic-subscription
Function: Displays all configurations of dynamic subscriptions in the telemetry function.
Parameter: null
Default: Telemetry is not configured.
Command Mode: All mode.
Usage Guide: This command can only be configured in telemetry mode, and will display information about all connected clients in the current dynamic subscription.
Example:
Switch(config)#telemetry
Switch(config-telemetry)#grpc server 172.17.100.235 port 50002
Switch(config-telemetry)#show telemetry dynamic-subscription
---
grpc server 172.17.100.235 port 50002

Ip-port :172.30.9.26:50002
Sensor-path:CpuInfo;MemoryInfo;IfStatistics
Sample-interval:10000 ms

12.4 VXLAN Commands

12.4.1 arp proxy-answer enable

Command: [no] arp proxy-answer enable
Function: Enable arp proxy-answer funciton
Parameter: None
Command Mode: NVI mode
Default: Arp proxy-answer function is disabled by default
Usage Guide: This configuration can only take effect after arp suppression is enabled. Configure this function to support proxy-answer of arp requests that match the suppression table, and reduce ARP packet flooding and the transmission to the remote end.
Example: Enable arp proxy-answer in NVI instance 10

```
Switch(config)# nvi 10
Switch(config-nvi)#arp proxy-answer enable
```

12.4.2 arp suppression enable

Command: [no] arp suppression enable
Function: Arp flood suppression
Parameter: None
Command Mode: NVI mode
Default: Arp flood suppression function is disabled by default
Usage Guide: Configuring this function can reduce the flooding of ARP packets sent by broadcast.
Example: Enable arp flood suppression in NVI instance 10

```
Switch(config)# nvi 10
Switch(config-nvi)# arp suppression enable
```

12.4.3 arp suppress-drop

Command: [no] arp suppress-drop
Function: Arp flood suppress drop
Parameter: None
Command Mode: NVI mode
Default: Arp flood suppression function is disabled by default
Usage Guide: Configuring this function can reduce the flooding of ARP packets sent by broadcast. and drop arp packets.
Example: Enable arp flood suppression in NVI instance 10

Switch(config)# nvi 10
Switch(config-nvi)# arp suppression enable

12.4.4 arp suppression table kat

Command: [no] arp suppression table kat <1-3600>
Function: Arp suppression table entry lifetime
Parameter: <1-3600> s
Command Mode: Global mode
Default: 1100
Usage Guide: Arp suppression table entry lifetime. The creation time or the last update time of the entry is the starting time, the entry will be deleted after expiration.
Example: Configure the lifetime of ARP suppression table entries to 1000s
Switch(config)# arp suppression table kat 1000

12.4.5 clear nvi statistics

Command: clear nvi [<nvi-id>] statistics
Function: Clear packet statistics in the network virtual instance
Parameter: *<nvi-id>: N*etwork virtual instance ID
Command Mode: Admin mode
Default: None
Usage Guide: Clear packet statistics in the network virtual instance. Default for all nvi-id, nvi-id can also be specified.
Example: Clear packet statistics in NVI instance 10
Switch# clear nvi 10 statistics

12.4.6 description

Command: [no] description <NAME>
Function: Configure NVI description information
Parameter: Specify the name of the network virtual instance
Command Mode: NVI mode
Default: None
Usage Guide: Configure description information for NVI to facilitate memory and identification.
Example: Configure the description information as school in NVI instance 10
Switch(config)# nvi 10
Switch(config-nvi)# description school

12.4.7 description

Command: [no] description <NAME>
Function: Configure NVE description information
Parameter: Descriptive information of the NVE tunnel
Command Mode: NVE interface mode
Default: None
Usage Guide: Configure description information for NVE tunnel to facilitate memory and identification.
Example: Configure the description information as group1 in NVE tunnel 1

```
Switch(config)# interface nve 1
Switch(config-if-nve1)# description group1
```

12.4.8 destination

Command: [no]destination <ip-address>
Function: Configure the destination address of the VXLAN tunnel
Parameter: Specify the destination IP address of the VTEP (VXLAN Tunnel Endpoints)
Command Mode: NVE interface mode
Default: None
Usage Guide: Manually specify the tunnel destination IP address(Remote VTEP), used with the source command to establish a vxlan tunnel. You can specify the address of the vlan interface or the Loopback interface. It is recommended to use the address of the Loopback interface.
Example: Manually configure the source ip to 1.1.1.1 and the destination ip to 2.2.2.2 in NVE tunnel 1.

```
Switch(config)# interface nve 1
Switch(config-if-nve1)# source 1.1.1.1
Switch(config-if-nve1)# destination 2.2.2.2
```

12.4.9 flooding disable

Command: [no] flooding disable
Function: Disable the flooding function of the vxlan tunnel in NVI
Parameter: None
Command Mode: NVI mode
Default: The flooding function of all tunnels in NVI is enabled by default
Usage Guide: By default, after VTEP receives a unicast data frame with an unknownnnnn destination MAC address from the local site, it will flood the data frame on all VXLAN tunnels in the VXLAN network except the receiving interface, and send the data frame to all sites within. If users do not want to flood into the VXLAN tunnel, they can manually disable the flooding function of the VXLAN tunnel through this command.

Example: Disable the flooding function under NVI instance 10

```
Switch(config)# nvi 10
Switch(config-nvi)# flooding disable
```

12.4.10 interface nve

Command: [no] interface nve <nve-id>
Function: Create NVE tunnel interface
Parameter: <nve-id>: NVE tunnel interface ID, range 1-400
Command Mode: Global mode
Default: There is no nve tunnel interface by default
Usage Guide: Create a nve tunnel interface and enter the nve interface configuration mode. The no command will delete the specified NVE interface and all configurations under that interface.
Example: Create NVE tunnel interface 1

```
Switch(config)# interface nve 1
Switch(config-if-nve1)#
```

12.4.11 interface nvi-interface

Command: [no] interface nvi-interface <nvi-interface-id>
Function: Create NVI virtual interface
Parameter: <*nvi-interface-id>:* Network virtual instance ID, range 1~2048
Command Mode: Global mode
Default: There is no NVI virtual interface on the device
Usage Guide: Create an associated NVI virtual interface for the virtual switching instance NVI. The nvi-id must be created before creating the interface.
Example: Create NVI virtual interface 10

```
Switch(config)#interface nvi-interface 10
Switch(config-if-nvi-interface10)#
```

12.4.12 ip address

Command: [no] ip address ip-address mask (secondary|)
Function: Configure the IP address of the NVI virtual interface
Parameter:

ip-address: Specify the IP address of the NVI virtual interface
mask: Specify IP address mask
secondary: Configure as a secondary address

Command Mode: NVI interface mode

Default: No IP address

Usage Guide: Configure the IP address of the NVI virtual interface, which is the gateway address when the device is used as the VXLAN IP gateway.

Example: Configure ip address 10.1.1.1 under NVI virtual interface 10

Switch(config)# interface nvi-interface 10

Switch(config-if-nvi-interface10)# ip address 10.1.1.1 255.255.255.0

12.4.13 ipv6 address

Command: [no] ipv6 address X:X::X:X/M

Function: Configure the IPv6 address of the NVI virtual interface

Parameter: *X:X::X:X/M s*pecify the IPv6 address of the NVI virtual interface

Command Mode: NVI interface mode

Default: No IPv6 address

Usage Guide: Configure the IPv6 address of the NVI virtual interface, which is the gateway address when the device is used as the VXLAN IPv6 gateway.

Example: Configure ipv6 address 2010::1/64 under NVI virtual interface 10

Switch(config)# interface nvi-interface 10

Switch(config-if-nvi-interface10)# ipv6 address 2010::1/64

12.4.14 join nvi

Command: [no] join nvi <nvi-id>

Function: Configure the VXLAN tunnel interface to associate with nvi

Parameter: *<nvi-id>: N*etwork virtual instance ID, range 1~3838

Command Mode: NVE interface mode

Default: The vxlan tunnel interface does not join any network virtual instance

Usage Guide: The same vxlan tunnel interface can join different network virtual instances at the same time, and the same virtual switching instance can be associated with multiple vxlan tunnel interfaces.The nvi added at both ends of the tunnel can be different, but the vxlan-id bound to nvi must be the same.

Example: Bind tunnel interface nve 1 to nvi instance 10

Switch(config)# interface nve 1
Switch(config-if-nve1)# join nvi 10

12.4.15 mac-address

Command: [no] mac-address FF-FF-FF-FF-FF-FF

Function: Configure the mac address of the NVI virtual interface
Parameter: *FF-FF-FF-FF-FF-FF :* specify the mac address of the NVI virtual interface
Command Mode: NVI interface mode
Default: The default mac address of the device
Usage Guide: For distributed gateways, the MAC addresses of all gateway interfaces on the same network segment need to be configured to the same mac.
Example: Configure the mac address as 02-02-02-02-02-02 under the NVI virtual interface 10

Switch(config)# interface nvi-interface 10
Switch(config-if-nvi-interface10)# mac-address 02-02-02-02-02-02

12.4.16 mac-address-table static address nvi

Command: [no] mac-address-table static address {mac-address} nvi <nvi-id> interface nve <nve-id>
Function: Configure remote static MAC address
Parameter:

mac-address：MAC address
nvi-id：Network virtual instance ID
nve-id：VXLAN tunnel interface corresponding to the remote MAC address

Command Mode: Global mode
Default: None
Usage Guide: Configure the remote static mac address on the specified nvi instance and tunnel interface. The specified tunnel interface must be a statically created VXLAN tunnel interface. When the tunnel is deleted or modified to another type of tunnel, this configuration will be deleted at the same time.
Example: Configure the remote static mac address 00-00-00-00-00-01 on nvi instance 10 and tunnel interface nve 1.
Switch(config)# mac-address-table static address 00-00-00-00-00-01 nvi 10 interface nve 1

12.4.17 nd proxy-answer enable

Command: [no] nd proxy-answer enable
Function: Enable nd proxy-answer funciton
Parameter: None
Command Mode: NVI mode
Default: Nd proxy-answer function is disabled by default
Usage Guide: This configuration can only take effect after nd suppression is enabled. This function can be configured to proxy-answer the ns packets matching the suppression table, and reduce the flooding of the nd packets sent by multicast and the transmission to the remote end.
Example:

Switch(config)# nvi 10

Switch(config-nvi)#nd proxy-answer enable

12.4.18 nd suppression enable

Command: [no] nd suppression enable
Function: Nd flood suppression
Parameter: None
Command Mode: NVI mode
Default: Nd flood suppression function is disabled by default
Usage Guide: Configuring this function can reduce the flooding of nd packets sent by multicast
Example: Enable nd flood suppression in NVI instance 10

Switch(config)# nvi 10
Switch(config-nvi)# nd suppression enable

12.4.19 nd suppress-drop

Command: [no] nd suppress-drop
Function: Nd flood suppression drop
Parameter: None
Command Mode: NVI mode
Default: Nd flood suppression function is disabled by default
Usage Guide: Configuring this function can reduce the flooding of nd packets sent by multicast,and drop nd packets.
Example: Enable nd flood suppression in NVI instance 10

Switch(config)# nvi 10
Switch(config-nvi)# nd suppression enable

12.4.20 nd suppression table kat

Command: [no] nd suppression table kat <1-3600>
Function: Nd suppression table entry lifetime
Parameter: <1-3600> s
Command Mode: Global mode
Default: 1100
Usage Guide: Nd suppression table entry lifetime. The creation time or the last update time of the entry is the starting time, the entry will be deleted after expiration.
Example: Configure the lifetime of nd suppression table entries to 1000s
Switch(config)# nd suppression table kat 1000

12.4.21 nve mode

Command: nve mode vxlan
Function: Configure the mode of the NVE tunnel interface
Parameter: None
Command Mode: NVE interface mode
Default: None
Usage Guide: Currently only supports vxlan mode
Example: Configure tunnel interface nve 1 to vxlan mode

```
Switch(config)# interface nve 1
Switch(config-if-nve1)#nve mode vxlan
```

12.4.22 nvi

Command: [no] nvi <nvi-id>
Function: Configure network virtual instance
Parameter: *<nvi-id>: N*etwork virtual instance ID, range 1~2048
Command Mode: Global mode
Default: There is no network virtual instance by default
Usage Guide: Create a network virtual instance and enter the NVI configuration mode or directly enter the existing NVI configuration mode. The no command deletes this network virtual instance and all dynamic data configuration information related to this NVI, etc. If a nve tunnel interface is manually bound to the nvi instance, you need to manually unbind the nve tunnel interface before deleting the nvi instance.
Example: Create nvi 10 and enter nvi configuration mode

```
Switch(config)# nvi 10
Switch(config-nvi)#
```

12.4.23 remote ip

Command: [no] remote ip <ip-address>
Function: Specify the IP address of the remote device for VEG communication.
Parameter: ip-address: the IP address for VEG communication(only supports ipv4)
Command Mode: VEG mode
Default: None
Usage Guide: Configure the communication IP address of the remote device in VEG, up to 5
Example: Configure the communication IP address of the remote device as 2.2.2.2

```
Switch(config)#virtual-equipment-group 1
Switch(config-veg1)#remote ip 2.2.2.2
```

12.4.24 show interface nve

Command: show interface nve [<nve-id>]

Function: Show nve tunnel interface information and statistics on the number of sent and received packets and bytes.

Parameter: <nve-id>: NVE tunnel interface ID, range 1-400

Command Mode: Admin mode

Default: None

Usage Guide: Show nve tunnel interface information and statistics on the number of sent and received packets and bytes. Default for all nve-id, nve-id can also be specified.

Example:

```
Switch# show interface nve 200
NVE200 is up(0), line protocol is up, dev index is 16001
Device flag 0x91(UP P2P NOARP)
Time since last status change:0w-1d-20h-4m-19s    (158659 seconds)
Tunnel source 3.3.3.3, destination 2.2.2.2
   Input unicast packets statistics:
         0 input packets, 0 bytes
   Output unicast packets statistics:
         0 output packets, 0 bytes
```

Displayed information	Explanation
source	Tunnel source IP
destination	Tunnel destination IP
Input unicast packets statistics	Number of packets and bytes received
Output unicast packets statistics	Number of packets and bytes sent

12.4.25 show interface nvi-interface

Command: show interface nvi-interface <nvi-interface-id>

Function: Show information about the nvi virtual interface

Parameter: *nvi-interface-id:* specify the number of the NVI virtual interface, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show information about the nvi virtual interface

Example:

```
Switch# show interface nvi-interface 10
      Nvi-interface is up(0), line protocol is up, dev index is 11012
        Device flag 0x1003(UP BROADCAST MULTICAST)
        Time since last status change:0w-1d-22h-2m-40s    (165760 seconds)
        IPv4 address is:
          12.0.0.1              255.255.255.0         (Primary)
```

VRF Bind: Not Bind

Hardware is EtherSVI, address is 00-22-2d-00-00-01

MTU is 1500 bytes , BW is 0 Kbit

12.4.26 show ipv6 interface nvi-interface

Command: show ipv6 interface nvi-interface <nvi-interface-id>

Function: Show information about the nvi virtual interface (for ipv6)

Parameter: *nvi-interface-id: s*pecify the number of the NVI virtual interface, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show information about the nvi virtual interface (for ipv6)

Example:

Switch# show ipv6 interface nvi-interface 10

Nvi-interface is up(0), line protocol is up, dev index is 11012

Device flag 0x1003(UP BROADCAST MULTICAST)

IPv6 is enabled

Link-local address(es):

fe80::222:2dff:fe00:1 PERMANENT

Site-local address(es):

Global unicast address(es):

Joined group address(es):

ff02::1

ff02::1:ff00:1

MTU is 1500 bytes

ND DAD is enabled, number of DAD attempts is 1

ND managed_config_flag is unset

ND other_config_flag is unset

ND NS interval is 1 second(s)

ND router advertisements is disabled

ND RA min-interval is 200 second(s)

ND RA max-interval is 600 second(s)

ND RA hoplimit is 64

ND RA lifetime is 1800 second(s)

ND RA MTU is 1500

ND advertised reachable time is 30000 millisecond(s)

ND advertised retransmit time is 1000 millisecond(s)

ND advertised default router preference is Medium

12.4.27 show nvi arp suppression

Command: show nvi [<nvi-id>] arp suppression

Function: Show the arp suppression entry information in the network virtual instance

Parameter: *<nvi-id>:* Network virtual instance ID, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show the arp suppression entry information in the network virtual instance. Default for all nvi-id, nvi-id can also be specified.

Example:

Switch# show nvi arp suppression

Address	Hardware Addr	Port	svid	Age-time(sec)
10.1.1.1	00-00-00-00-00-08	nve1	10	10s
20.1.1.1	00-00-00-00-00-09	Local	0	static
30.1.1.1	00-00-00-00-00-0f	nve2	20	12s

Displayed information	Explanation
Address	ip address
Hardware Addr	mac address
Port	nvex: tunnel interface name Local: local port
svid	vlan id
Age-time(sec)	static means no aging

12.4.28 show nvi detail

Command: show nvi [<nvi-id>] detail

Function: Show detailed information of network virtual instances

Parameter: *<nvi-id>:* Network virtual instance ID, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show detailed information of network virtual instances. Default for all nvi-id, nvi-id can also be specified.

Example:

Switch# show nvi 10 detail

NVI: 10

description:

vxlan-id: 10

udp destination-port number：4789

split-horizon: enable

flooding tunnel: enable

tunnel list:

Nve name	state	source	destination
Nve1	UP	12.0.0.1	12.0.0.2

Displayed information	Explanation
NVI	Network virtual instance ID
description	Descriptive information of NVI
vxlan-id	vxlan id
udp destination-port number	The destination UDP port number of the vxlan packet header
split-horizon	Whether split horizon is on
flooding tunnel	Whether the flooding function of the vxlan tunnel is enabled
Nve name	Tunnel interface name
state	Tunnel interface status
source	Tunnel source address
destination	Tunnel destination address

12.4.29 show nvi nd suppression

Command: show nvi [<nvi-id>] nd suppression

Function: Show the nd suppression entry information in the network virtual instance

Parameter: *<nvi-id>:* Network virtual instance ID, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show the nd suppression entry information in the network virtual instance. Default for all nvi-id, nvi-id can also be specified.

Example:

Switch# show nvi nd suppression

Address	Hardware Addr	Port	svid	Age-time(sec)
2010::1	00-00-00-00-00-08	nve1	10	10s
2020::1	00-00-00-00-00-09	Local	0	static
2030::1	00-00-00-00-00-0f	nve2	20	12s

Displayed information	Explanation
Address	ipv6 address
Hardware Addr	mac address

Port	nvex: tunnel interface name Local: local port
svid	vlan id
Age-time(sec)	static means no aging

12.4.30 show nvi nve tunnel

Command: show nvi [<nvi-id>] nve tunnel

Function: Show tunnel information of virtual switching instance

Parameter: *<nvi-id>:* Network virtual instance ID, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show tunnel information of virtual switching instance. Default for all nvi-id, nvi-id can also be specified.

Example:

```
Switch# show nvi nve tunnel
NVI 10：vxlan-id 10
Nve name    state    source     destination
Nve1           up       1.1.1.1    2.2.2.2
Nve2           up       1.1.1.1    3.3.3.3

NVI 20：vxlan-id 20
Nve name    state    source     destination
Nve1           up       1.1.1.1    2.2.2.2
Nve3           up       1.1.1.1    4.4.4.4
Nve4           up       5.5.5.5    6.6.6.6
```

Displayed information	Explanation
NVI	Network virtual instance ID
vxlan-id	vxlan id
Nve name	Tunnel interface name
state	Tunnel interface status
source	Tunnel source address
destination	Tunnel destination address

12.4.31 show nvi statistics

Command: show nvi [<nvi-id>] statistics

Function: Show packet statistics in the network virtual instance

Parameter: *<nvi-id>:* Network virtual instance ID, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show packet statistics in the network virtual instance. Default for all nvi-id, nvi-id can also be specified.

Example:

```
Switch# show nvi 10 statistics
nvi 10 vxlan-id 10:
Item            Packets                 Bytes
Input            0                       0
Output          0                       0
```

Displayed information	Explanation
NVI	Network virtual instance ID
vxlan-id	vxlan id
Input Packets Bytes	Number of packets and bytes received
Output Packets Bytes	Number of packets and bytes send

12.4.32 show virtual-equipment-group ID

Command: show virtual-equipment-group <ID>

Function: Show virtual equipment group information

Parameter: ID：virtual equipment group(VEG) ID, range 1-1

Command Mode: Admin mode

Default: None

Usage Guide: Show the IP address and connection status of VEG members.

Example:

```
Switch(config-veg1)#show virtual-equipment-group 1
Virtual equipment group 1
  source ip 1.1.1.1
  remote ip 2.2.2.2 not connected
```

12.4.33 show virtual-equipment-group ID service

Command: show virtual-equipment-group <ID> service [interface nvi-interface <nvi-interface-id> (arp|nd)]

Function: Show VEG's synchronization service content

Parameter: ID：virtual equipment group(VEG) ID, range 1-1

*nvi-interface-id: s*pecify the number of the NVI virtual interface, range 1~3838

(arp|nd): service type, including arp and nd

Command Mode: Admin mode

Default: None

Usage Guide: Show all services of VEG or the service of specified type on the nvi interface.

Example:

```
Switch(config-veg1)#show virtual-equipment-group 1 service
sync service name arp-Nvi-interface10
     local entry num : 0 .
   remote ip 2.2.2.2 not connected
     peer service waiting for remote peer service ready .
sync service name nd-Nvi-interface10
     local entry num : 0 .
   remote ip 2.2.2.2 not connected
     peer service waiting for remote peer service ready .
```

12.4.34 show vxlan mac-address-table

Command: show vxlan mac-address-table [nvi <nvi-id>|]

Function: Show the MAC address table entry information in the network virtual instance

Parameter: *<nvi-id>:* Network virtual instance ID, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show the MAC address table entry information in the network virtual instance. Default for all nvi-id, nvi-id can also be specified.

Example:

```
Switch# show vxlan mac-address-table
Read mac address table....
Nvi-id  Mac Address          Type    Creator   Ports
----   -------------------- ------- ---------- -------------------------
4      00-00-00-02-44-23    DYNAMIC Hardware   Ethernet1/0/1
4      00-00-00-00-00-22    DYNAMIC Hardware   Nve1
4      00-00-00-00-00-33    STATIC  User       Nve2
```

Displayed information	Explanation
Nvi-id	Network virtual instance ID
Mac Address	MAC address
Type	MAC address type
Creator	Hardware:Hardware learning User: Manual configuration
Ports	Port name

12.4.35 show vxlan mac-address-table count

Command: show vxlan mac-address-table count [nvi <nvi-id>|]

Function: Show the number of MAC address table entries in the network virtual instance

Parameter: <nvi-id>: Network virtual instance ID, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show the number of MAC address table entries in the network virtual instance. Default for all nvi-id, nvi-id can also be specified.

Example:

```
Switch# show vxlan mac-address-table count
nvi-id                  Mac count
------------------ ----------------------------
10                      16
30                      16
```

Displayed information	Explanation
Nvi-id	Network virtual instance ID
Mac count	Number of MAC address table entries

12.4.36 source

Command: [no] source WORD|<ip-address>

Function: Configure the source address of the VXLAN tunnel

Parameter: Specify the source IP address of the VTEP (VXLAN Tunnel Endpoints)

Command Mode: NVE interface mode

Default: None

Usage Guide: Manually specify the tunnel source IP address(Local VTEP), used with the destination command to establish a vxlan tunnel. You can specify the address of the vlan interface or the Loopback interface. It is recommended to use the address of the Loopback interface.

Example: Manually configure the source ip to 1.1.1.1 in NVE tunnel 1.

```
Switch(config)# interface nve 1
Switch(config-if-nve1)# source 1.1.1.1
```

12.4.37 source ip

Command: source ip <ip-address>

Function: Specify the IP address of the local device for VEG communication.

Parameter: ip-address: the IP address for VEG communication(only supports ipv4)

Command Mode: VEG mode
Default: None
Usage Guide: Configure the communication IP address of the local device in VEG.
Example:
Switch(config)#virtual-equipment-group 1
Switch(config-veg1)#source ip 1.1.1.1

12.4.38 virtual-equipment-group ID

Command: [no] virtual-equipment-group <ID>
Function: Configure virtual equipment group ID
Parameter: ID：virtual equipment group ID, range 1-1
Command Mode: Global mode
Default: None
Usage Guide: Multiple devices can be associated to the virtual group by specifying the source ip and remote ip of the virtual equipment group.
Example:
Switch(config)#virtual-equipment-group 1
Switch(config-veg1)#

12.4.39 vxlan remote arp-learning disable

Command: [no] vxlan remote arp-learning disable
Function: Disable remote ARP automatic learning function
Parameter: None
Command Mode: Global mode
Default: The remote ARP automatic learning function is enabled by default
Usage Guide: Configure whether the remote ARP automatic learning function is enabled.
Example:

Switch(config)# vxlan remote arp-learning disable

12.4.40 vxlan remote mac-address-learning disable

Command: [no] vxlan remote mac-address-learning disable
Function: Disable remote mac address automatic learning function
Parameter: None
Command Mode: Global mode
Default: The remote mac address automatic learning function is enabled by default
Usage Guide: Configure whether the remote mac address automatic learning function is enabled.

Example:
Switch(config)# vxlan remote mac-address-learning disable

12.4.41 vxlan remote nd-learning disable

Command: [no] vxlan remote arp-learning disable
Function: Disable remote nd automatic learning function
Parameter: None
Command Mode: Global mode
Default: The remote nd automatic learning function is enabled by default
Usage Guide: Configure whether the remote nd automatic learning function is enabled.
Example:

Switch(config)# vxlan remote nd-learning disable

12.4.42 vxlan udp destination-port-number

Command: [no] vxlan udp destination-port-number <1-65535>
Function: Configure the destination UDP port number of the vxlan packet header
Parameter: Port number range: 1-65535
Command Mode: Global mode
Default: 4789
Usage Guide: Configure the destination UDP port number of the vxlan packet header
Example: Configure the destination udp port number of the vxlan packet header to 5000.
Switch(config)# vxlan udp destination-port-number 5000

12.4.43 vxlan-id

Command: vxlan-id <vxlan-id>
Function: Configure VXLAN Network Indentifier and associate it with the network virtual instance.
Parameter: vxlan-id: VXLAN Network Indentifier, range:1~16777215
Command Mode: NVI mode
Default: There is no vxlan-id configuration by default
Usage Guide: The NVI broadcast domain in the VXLAN (Virtual eXtensible Local Area Network) network is a virtual broadcast domain, which must be bound to NVI through the command vxlan-id. The relationship between vxlan-id and NVI is one-to-one, and vxlan-id is carried through NVI. After this command is configured, it can not be modified. One vxlan-id can only be bound to one nvi, and one nvi can only be bound to one vxlan-id.
Example: Configure vxlan id to 5000 under NVI instance 10

```
Switch(config)# nvi 10
Switch(config-nvi)# vxlan-id 5000
```

12.4.44 xconnect nvi

Command: [no] xconnect nvi <nvi-id> {mode {ethernet| vlan svid <vid>}| }

Function: Configure the vxlan access mapping relationship of the access port

Parameter:

nvi-id: Network virtual instance ID, range 1~2048

{ethernet| vlan}: Vxlan access mapping mode, including ethernet and vlan

vid: Outer VLAN ID in packets, range: 1~4094

Command Mode: Port mode

Default: None

Usage Guide: Configure the port to bind the nvi instance, including two modes of ethernet and vlan. When the mode and the following parameters are not specified during configuration, the default is ethernet mode. In ethernet mode, one port can only be associated with one nvi instance.

Example: Ethernet 1/0/1 is associated with nvi instance 10, specifying vlan mode and vlan id 10.

```
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# xconnect nvi 10 mode vlan svid 10
```

12.5 EVPN Commands

12.5.1 address-family l2vpn evpn

Command: address-family l2vpn evpn

Function: Enter EVPN address family configuration mode

Parameter: None

Command Mode: BGP mode

Default: None

Usage Guide: Enter EVPN address family configuration mode.

Example: Enter EVPN address family configuration mode.

```
Switch(config-router)#address-family l2vpn evpn
Switch(config-router-af)#
```

12.5.2 distributed-gateway enable

Command: [no] distributed-gateway enable

Function: Configure the gateway interface as a distributed gateway interface

Parameter: None
Command Mode: NVI interface mode
Default: The interface is a centralized gateway interface by default.
Usage Guide: Configure the gateway interface as a distributed gateway interface. The VRF bound to the NVI interface must have been configured with L3VNI.
Example: Configure nvi interface 10 as a distributed gateway interface
Switch(config)#interface nvi-interface 10
Switch(config-if-nvi-interface10)#distributed-gateway enable

12.5.3 dup-addr-detection

Command: [no] dup-addr-detection [max-moves <max-moves>] [detect-time <time>]
Function: Configure duplicate MAC address detection threshold
Parameter: <max-moves>: The maximum number of MAC address migrations within the timeout period, range: <2-1000>
<time>: timeout period, range: <2-1800> s
Command Mode: EVI mode
Default: max-moves is 5，time is 180
Usage Guide: When the device detects that a certain MAC address has migrated, it will start the duplicate address detection timer. Within the timeout period, if the device detects that the MAC address has migrated max-moves times, it will consider this MAC address as a duplicate MAC address and issue an alarm.
Example: If mac migration occurs 10 times within 300s, an alarm will be issued.
Switch(config-nvi-evpn)#dup-addr-detection max-moves 10 detect-time 300

12.5.4 enable/disable

Command: enable/disable
Function: Enable/disable EVPN instance in NVI
Parameter: None
Command Mode: EVI mode
Default: diable
Usage Guide: Enable EVPN instance in NVI to generate related Type2 and Type3 routes. The RD must be configured before enabling the EVPN instance. Disable the EVPN instance in NVI to delete the related Type2 and Type3 routes.
Example: Enable EVPN instance in NVI
Switch(config-nvi-evpn)#enable

12.5.5 esi

Command: [no] esi <id>
Function: Configure the ESI of the interface
Parameter: <id>: the ESI of the interface, the format is 00xx.xxxx.xxxx.xxxx.xxxx
Command Mode: Port mode
Default: None
Usage Guide: Configure the ESI of the interface. In a single-homing environment, ESI is always 0 and no configuration is required. In a multi-homing environment, the interfaces of multiple PEs connected to the same CE must be configured with the same ESI.
Example: Configure esi for interface ethernet1/0/1 as 0012.1212.1212.1212.1212
Switch#(config-if-ethernet1/0/1)#esi 0012.1212.1212.1212.1212

12.5.6 evpn

Command: [no] evpn
Function: Create an EVPN instance associated with the NVI
Parameter: None
Command Mode: NVI mode
Default: No evpn instance is associated with nvi by default
Usage Guide: Create an EVPN instance associated with NVI and enter EVI configuration mode. The VXLAN-ID of NVI and evpn nve source-address must have been configured before configuring this command. If you delete the EVPN instance associated with the NVI, the entries associated with it will also be deleted, including the local MAC-VRF and the EVPN routes advertised by this device, etc.
Example: Create an EVPN instance associated with NVI 10
Switch(config)# nvi 10
Switch(config-nvi)#evpn

12.5.7 evpn nve source-address

Command: [no] evpn nve source-address <ip-address>
Function: Configure the NVE source IP address of EVPN instance
Parameter: <ip-address>：NVE source IP address of the EVPN instance
Command Mode: Global mode
Default: None
Usage Guide: Configure the NVE source IP address of EVPN instance. This address is used for the next hop address of the EVPN route sent out and the Originating Router's IP in NLRI, which is used to establish a VXLAN tunnel. The source address of the EVPN instance must use the local layer 3 interface address, and the loopback interface address is recommended. Only one NVE source address can be configured in the system. After configuration, the address can not be modified. If you need to modify it, you need to delete and reconfigure it. If you delete this configuration, you will be prompted to delete all EVPN configurations.

Example: Configure the NVE source address of EVPN instance as 2.2.2.2
Switch(config)#evpn nve source-address 2.2.2.2

12.5.8 evpn nvi-vlan-mapping-monitor disable

Command: [no] evpn nvi-vlan-mapping-monitor disable
Function: Disable the function of ingress vlan mapping to eti-id to realize the vlan-based access model of EVPN.
Parameter: None
Command Mode: Global mode
Default: Enabled by default
Usage Guide: After configuring this command, the eti-id fields of EVPN routes generated locally or learned are all 0. When enabled by default, the vlan configuration of the access port will be identified and mapped to the eti-id fields of the EVPN routes.
Example:
Switch(config)#evpn nvi-vlan-mapping-monitor disable

12.5.9 evpn timer df-delay

Command: [no] evpn timer df-delay <delay-value>
Function: Configure the delay time for designated forwarder(DF) election
Parameter: <delay-value>: delay time, range: 1-120
Command Mode: Global mode
Default: 3s
Usage Guide: In the multi-homing access network, the PE starts the DF election delay timer after sending the Type 4 route, and performs DF election when the timer expires. This command is used to configure the delay time of the election, that is, the timeout period of the timer. The no command is used to restore the default configuration.
Example: Configure the DF election delay time to 5s
Switch(config)#evpn timer df-delay 5

12.5.10 evpn-exit

Command: evpn-exit
Function: Exit EVI mode
Parameter: None
Command Mode: EVI mode
Default: None
Usage Guide: Exit EVI mode
Example:

```
Switch(config-nvi-evpn)#evpn-exit
Switch(config-nvi)#
```

12.5.11 exit-address-family

Command: exit-address-family
Function: Exit BGP EVPN address family configuration mode
Parameter: None
Command Mode: BGP EVPN address family mode
Default: None
Usage Guide: Exit BGP EVPN address family configuration mode, and return to BGP configuration mode.
Example: Exit BGP EVPN address family configuration mode

```
Switch(config-router-af)#exit-address-family
Switch(config-router)#
```

12.5.12 ip vrf forwarding

Command: [no] ip vrf forwarding <vrf-name>
Function: Configure the L3VPN instance associated with the nvi layer 3 gateway interface
Parameter: <vrf-name>: Name of the L3VPN instance
Command Mode: NVI interface mode
Default: None
Usage Guide: Configure the L3VPN instance associated with the NVI interface. The no command is used to cancel the association between the nvi interface and the L3VPN instance, delete the configured IP address and related routes.
Example: Configure nvi virtual interface 10 to associate with vrf a1

```
Switch(config)#interface nvi-interface 10
Switch(config-if-nvi-interface10)#ip vrf forwarding a1
```

12.5.13 l3-vni

Command: [no] l3-vni <vxlan-id>
Function: Configure the VNI of the L3VPN instance
Parameter: vxlan-id: VXLAN Network Indentifier, range:1~16777215
Command Mode: Vrf mode
Default: None
Usage Guide: Configure the VNI of L3VPN instance to establish a VXLAN layer 3 tunnel, which only needs to be configured in the distributed gateway. After configuration, EVPN Type2 and Type5 routes will be used to advertise VPN routes between PEs. Only one VNI can be configured

on a L3VPN instance, and the same L3VPN instance on different PEs should be configured with the same VNI. When deleting the VNI of L3VPN instance, the VXLAN tunnel associated with this VNI and the route related to this tunnel will be deleted at the same time.

Example: Configure the L3VPN instance to associate with vxlan-id 100

Switch(config-vrf)#l3-vni 100

12.5.14 rd

Command: [no] rd <ASN:nn_or_IP-address:nn>

Function: Configure the route distinguisher of the EVPN instance

Parameter: <ASN:nn_or_IP-address:nn>: The value of the route distinguisher. It can be the AS number + the unique identifier in the AS, or the Router ID + the unique identifier in the device.

Command Mode: EVI mode

Default: None

Usage Guide: Configure the route distinguisher of the EVPN instance. The route distinguisher is only used to distinguish EVPN routes, and only one route distinguisher can be configured for each EVPN instance. After the EVPN instance is enabled, the route distinguisher can not be deleted or modified. The value of RD is unique among all evi.

Example: Configure the rd of the EVPN instance to 20:20

Switch(config)# nvi 10

Switch(config-nvi)#evpn

Switch(config-nvi-evpn)#rd 20:20

12.5.15 route-target

Command: [no] route-target {import | export | both} <rt-value>

Function: Configure the route target of the EVPN instance

Parameter: {import | export | both}: Configure Import Route-Targe、Export Route-Targe or both.

<rt-value>: The value of route-target

Command Mode: EVI mode

Default: None

Usage Guide: Configure the route target of the EVPN instance which is used to filter EVPN routes. When the intersection of the route target of the EVPN route in the received BGP message and the import route-target of a certain EVI is not empty, the route will be imported to the MAC-VRF of the EVI. When the device advertises the EVPN route of an EVI, it will carry the export route-target of the EVI. Both import route-target and export route-target can be configured with multiple. After the EVPN instance is enabled, the route target can not be modified or deleted.

Example: Configure the route target of the EVPN instance to both 1:1

Switch(config)# nvi 10

Switch(config-nvi)#evpn

Switch(config-nvi-evpn)#route-target both 1:1

12.5.16 neighbor activate

Command: [no] neighbor {<ip-address>|<TAG>} activate

Function: Declare EVPN capability to peers

Parameter: <ip-address>: IPv4 address of the BGP peer

<TAG>: The name of the peer group

Command Mode: BGP EVPN address family mode

Default: None

Usage Guide: Declare EVPN capability to peers. If the peer also has EVPN capability, the EVPN route will be sent to the peer later.

Example: Declare EVPN capability to neighbor 1.1.1.1

Switch(config-router-af)# neighbor 1.1.1.1 activate

12.5.17 neighbor route-reflector-client

Command: [no] neighbor {<ip-address>|<TAG>} route-reflector-client

Function: Configure the route reflector client

Parameter: <ip-address>: IPv4 address of the BGP peer

<TAG>: The name of the peer group

Command Mode: BGP EVPN address family mode

Default: None

Usage Guide: Configure the route reflector client

Example: Configure neighbor 3.3.3.3 as the route reflector client

Switch(config-router-af)# neighbor 3.3.3.3 route-reflector-client

12.5.18 show evpn es

Command: show evpn es all|<esi> [detail]

Function: Show information about the ethernet segment(ES)

Parameter: <esi>: the ESI of the ES, the format is 00xx.xxxx.xxxx.xxxx.xxxx

detail: Show details

Command Mode: Admin mode

Default: None

Usage Guide: Show the relevant information of the specified ES, the all parameter is used to show the information of all ES.

Example: Show detailed information about all ES

Switch#show evpn es all detail

Ethernet Segment 0001.0000.0011.0000.0001 (LOCAL)

State: DF Done
NVE list:
1.1.1.1 Flags: 0x0
2.2.2.2 Flags: 0x0
Route Distinguisher: 1.1.1.1:2908
ES Import Route-Target:
Link Name: Ethernet1/0/11
Link State: Up
DF infomation:
1.1.1.1 EVI(10) : DF
Ethernet Segment 0011.2222.3333.4444.4444 (REMOTE)
State: Remote
NVE list:
2.2.2.2 Flags: 0x0

Displayed information	Explanation
Ethernet Segment	Ethernet Segment (Including LOCAL and REMOTE)
State	Designated forwarder election status
NVE list	NVE interface list
Route Distinguisher	Route Distinguisher of the EVPN instance
ES Import Route-Target	ES Import Route-Target
Link Name	Port name
Link State	Port link status
DF infomation	Information about the designated forwarder

12.5.19 show evpn mac-ip

Command: show evpn mac-ip all|nvi <nvi-id>
Function: Show mac and ip information learned by evpn
Parameter: <nvi-id>: Network virtual instance ID, range 1~2048
Command Mode: Admin mode
Default: None
Usage Guide: Show mac and ip information learned by evpn
Example:
Switch#show evpn mac-ip all

VXLAN_ID	MAC	ETH_TAG_ID	SEQ_NUM	STICKY	ESI
IP ADDRESS			DST NVE		FLAGS
20	00-10-94-00-fa-d2	20	0	FALSE	0000.0000.0000.0000.0000
N/A			3.3.3.3		R

```
20          00-10-94-00-fa-d3   20          0           FALSE     0000.0000.0000.0000.0000
 N/A                                        3.3.3.3               R
20          00-10-94-00-fa-d4   20          0           FALSE     0000.0000.0000.0000.0000
 N/A                                        3.3.3.3               R
20          00-10-94-00-fa-d5   20          0           FALSE     0000.0000.0000.0000.0000
```

Displayed information	Explanation
VXLAN_ID	Vxlan ID
MAC	Mac address learned by EVPN
ETH_TAG_ID	The ethernet tag ID of the forwarding instance associated with the MAC/IP learned by EVPN
SEQ_NUM	Sequence number used to record the number of mac migration
STICKY	Whether it is a MAC protected entry
ESI	ESI carried by MAC/IP learned by EVPN
IP ADDRESS	IP address of MAC/IP learned by EVPN
DST NVE	Next hop NVE address
FLAGS	L: Local entry R: Remote entry S: Synchronized local entries A: Synchronized remote alias path

12.5.20 show evpn mac-mobility

Command: show evpn mac-mobility

Function: Show information about MAC migration

Parameter: None

Command Mode: Admin mode

Default: None

Usage Guide: Show information about MAC migration, including the migrated MAC address, the number of mac migration and current status(Detecting or Suppression).

Example:

```
Switch# show evpn mac-mobility
EVPN Instance (NVI 10)
  00-00-00-00-00-01 2 Detecting
  00-00-00-00-00-02 6 Suppression
```

12.5.21 show evpn nvi

Command: show evpn nvi all|<nvi-id>

Function: Show global information about the EVPN instance

Parameter: *<nvi-id>:* Network virtual instance ID, range 1~3838

Command Mode: Admin mode

Default: None

Usage Guide: Show the EVPN instance information associated with the specified NVI

Example: Show the EVPN instance information associated with NVI 10

```
Switch#show evpn nvi 10
EVPN Instance (NVI 10)
  Encapsolution VXLAN
  VNI: 10
  Status: ACTIVE
  Route Distinguisher: 2:2
  Import Route Target
    RT: 1:1
    RT: 3:3
  Export Route Target
    RT: 2:2
  NVE Source Address: 2.2.2.2 (GLOBAL_USED)
  Duplication MAC-Address Detect
    Detect time: 300            Max moves: 10
```

Displayed information	Explanation
VNI	Vxlan id
Status	Status of the EVPN instance(ACTIVE or CONFIG)
Route Distinguisher	Route Distinguisher of the EVPN instance
Import Route Target	Import Route Target List
Export Route Target	Export Route Target List
NVE Source Address	NVE Source Address of the EVPN instance
Duplication MAC-Address Detect	Duplication MAC address detection threshold

12.5.22 show ip bgp evpn

Command: show ip bgp evpn {all|type-1|type-2|type-3|type-4|type-5}

Function: Show information about EVPN routes

Parameter: {all|type-1|type-2|type-3|type-4|type-5}: The type of the route, all means to show all types of EVPN routes

Command Mode: Admin mode

Default: None

Usage Guide: Show information about EVPN routes

Example: Show all types of EVPN routes

```
Switch#show ip bgp evpn all
BGP local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

network format description
RT-1:[RT][ESI][ETID]
RT-2:[RT][ETID][MAC][IPv4/v6]
RT-3:[RT][ETID][IPv4/v6]
RT-4:[RT][ESI][IPv4/v6]
RT-5:[RT][ETID][Prefix len][Prefix]
Route Distinguisher 1:3837

    Network          Next Hop            Metric     LocPrf     Weight Path
*>i[1][00ff.ffff.ffff.ffff.ffff][0]
                     11.1.1.1                       100        0      ?
*>i[3][3837][11.1.1.1]
                     11.1.1.1                       100        0      ?

Route Distinguisher 11111:3837
    Network          Next Hop            Metric     LocPrf     Weight Path
*>i[5][0][16][101.1.0.0]
                     11.1.1.1                       100        0      ?
*>i[5][0][64][1001::]
                     11.1.1.1                       100        0      ?

Route Distinguisher 11.1.1.1:13427
    Network          Next Hop            Metric     LocPrf     Weight Path
*>i[1][00ff.ffff.ffff.ffff.ffff][4294967295]
                     11.1.1.1                       100        0      ?
*>i[2][300][2203-0000-000d][]
                     11.1.1.1                       100        0      ?
*>i[2][300][2203-0000-000d][30.30.1.112]
                     11.1.1.1                       100        0      ?
*>i[4][00ff.ffff.ffff.ffff.ffff][11.1.1.1]
                     11.1.1.1                       100        0      ?
```

Chapter 13 Commands for IPv6

13.1 DHCPv6

13.1.1 clear ipv6 dhcp binding

Command: clear ipv6 dhcp binding [<*ipv6-address*>] [pd <*ipv6-prefix* | *prefix-length*>]

Function: To clear one specified DHCPv6 assigned address binding record or all the IPv6 address binding records.

Parameter: ***<ipv6-address>*** is the specified IPv6 address with binding record; ***<ipv6-prefix| prefix-length>*** is the specified IPv6 prefix with binding record; To clear all IPv6 address binding record if there is no specified record.

Command Mode: Admin Configuration Mode.

Usage Guide: DHCPv6 IPv6 address binding information can be displayed through the command **show ipv6 dhcp binding**. If DHCPv6 client does not use the DHCPv6 allocated IPv6 address but when the life time of the IPv6 address does not end, the DHCPv6 server will not remove its bind for this address. In this situation, the address binding information can be removed manually through this command; and if no parameter is appended, this command will remove all the address binding information, then all addresses and prefix will be assigned again in the DHCPv6 address pool.

Example: To delete all binding record of IPv6 address and prefix.

Switch#clear ipv6 dhcp binding

Relative Command: show ipv6 dhcp binding

13.1.2 clear ipv6 dhcp conflict

Command: clear ipv6 dhcp conflict [<*address*>]

Function: Clear the address with the conflict record in address conflict log.

Parameter: ***<address>*** is the specified address with the conflict record, no specified address will clear all conflict records.

Command mode: Admin Mode

Usage Guide: With **show ipv6 dhcp conflict** command, the user can check the conflict in which IP addresses. With this command, the user can clears the conflict record of an address. If no specified address will clear the conflict record of all addresses in log. After the conflict records are cleared in log, these addresses can be used by DHCPv6 server again.

Example: When administrator checks the conflict logs, administrator discovers that address 2001::1 with the conflict record is not used, so its record will be cleared from address conflict files.

Switch#clear ipv6 dhcp conflict 2001::1

13.1.3 clear ipv6 dhcp statistics

Command: clear ipv6 dhcp statistics

Function: Clear the statistic records of DHCPv6 packets, the statistic counter of DHCPv6 packets is cleared.

Parameter: None.

Command mode: Admin Mode

Usage Guide: With **show ipv6 dhcp statistics** command, the user can check the statistic information of the counter for DHCPv6 packets, all statistic information is an accumulative value. With this command will clear the counter to check the debugging conveniently.

Example: Clear the counter of DHCPv6 packets.

Switch#clear ipv6 dhcp statistics

Relative Command: show ipv6 dhcp statistics

13.1.4 debug ipv6 dhcp client packet

Command: debug ipv6 dhcp client {event | packet}

no debug ipv6 dhcp client {event | packet}

Function: To enable the debugging messages for protocol packets of DHCPv6 prefix delegation client, the no form of this command will disable the debugging information.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch**#** debug ipv6 dhcp client packet

13.1.5 debug ipv6 dhcp detail

Command: debug ipv6 dhcp detail

no debug ipv6 dhcp detail

Function: To display the debug information of all kinds of packets received or sent by DHCPv6, the no form of this command disabled this function.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch# debug ipv6 dhcp detail

13.1.6 debug ipv6 dhcp relay packet

Command: debug ipv6 dhcp relay packet

no debug ipv6 dhcp relay packet

Function: To enable the debugging information for protocol packets of DHCPv6 relay, the no form of this command will disable the debugging.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch# debug ipv6 dhcp relay packet

13.1.7 debug ipv6 dhcp server

Command: debug ipv6 dhcp server { event | packet }

no debug ipv6 dhcp server { event | packet }

Function: To enable the debugging information of DHCPv6 server, the no form of this command will disable the debugging.

Parameter: event is to enable debugging messages for DHCPv6 server events, such as address allocation; packet is for debugging messages of protocol packets of DHCPv6 server.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch#debug ipv6 dhcp server packet

13.1.8 dns-server

Command: dns-server *<ipv6-address>*

no dns-server *<ipv6-address>*

Function: To configure the IPv6 address of the DNS server for DHCPv6 client; the no form of this command will remove the DNS configuration.

Parameter: *<ipv6-address>* is the IPv6 address of DNS Server.

Default: No configured address pool of DNS Server by default.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Usage Guide: For each address pool, at most three DNS server can be configured, and the addresses of the DNS server must be valid IPv6 addresses.

Example: To configure the DNS Server address of DHCPv6 client as 2001:da8::1.

Switch(dhcp-1-config)#dns-server 2001:da8::1

13.1.9 domain-name

Command: domain-name *<domain-name>*

no domain-name *<domain-name>*

Function: To configure domain name of DHCPv6 client; the no form of this command will delete the domain name.

Parameter: *<domain-name>* is the domain name, less than 32 characters.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Default: The domain name parameter of address pool is not configured by default.

Usage Guide: At most 3 domain names can be configured for each address pool.

Example: To set the domain name of DHCPv6 client as www.google.com

Switch(dhcp-1-config)#domain-name www.google.com

13.1.10 excluded-address

Command: excluded-address *<ipv6-address> <ipv6-address>*

no excluded-address *<ipv6-address> <ipv6-address>*

Function: To configure the specified IPv6 address to be excluded from the address pool, the excluded address will not be allocated to any hosts; the no form of this command will remove the configuration.

Parameter: *<ipv6-address>* is the IPv6 address to be excluded from being allocated to hosts in the address pool.

Default: Disabled

Command Mode: DHCPv6 address pool configuration mode.

Usage Guide: This command is used to preserve the specified address from DHCPv6 address allocation.

Example: To configure to exclude 2001:da8:123::1 2001:da8:123::2 from DHCPv6 address allocation.

Switch(dhcpv6-1-config)#excluded-address 2001:da8:123::1 2001:da8:123::2

13.1.11 ipv6 address

Command: ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

no ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

Function: To configure the specified interface to use prefix delegation for address allocation. The no form of this command will disable the using of prefix delegation for address allocation.

Parameters: *<prefix-name>* is a string with its length no more than 32, designating or manual configuring the name of the address prefix defined in the prefix pool. ***<ipv6-prefix/prefix-length>*** is latter part of the IPv6 address excluding the address prefix, as well as its length.

Command Mode: Interface Configuration Mode.

Default: No global address is configured for interfaces by default.

Usage Guide: The IPv6 address of an interface falls into two parts: ***<prefix-name>*** and ***<ipv6-prefix>/<prefix-length>***. If routing advertisement has been enabled, the first 64 bits of the addresses will be advertised. The address generated by ***<prefix-name>*** and ***<ipv6-prefix/prefix-length>*** combination will be removed, and the advertising of the prefix will be disabled. Only one ***<ipv6-prefix/prefix-length>*** can be configured for one prefix name.

Example: If the prefix name my-prefix designates 2001:da8:221::/48, then the following command will add the address 2001:da8:221:2008::2008 to interface VLAN1.

Switch(Config-if-Vlan1)# ipv6 address my-prefix 0:0:0:2008::2008/64

13.1.12 ipv6 dhcp client pd

Command: ipv6 dhcp client pd *<prefix-name>* [rapid-commit]

no ipv6 dhcp client pd

Function: To configure DHCPv6 prefix delegation client for the specified interface. The no form of this command will disable the DHCPv6 prefix delegation client and remove the allocated address

prefix.

Parameters: <*prefix-name*> is the string with its length no more than 32, which designates the name of the address prefix. If **rapid-commit** optional is specified and the prefix delegation server enables the rapid-commit function, then the prefix delegation server will reply the prefix delegation client with the REPLY message directly. And the prefix delegation request will be accomplished by exchanging messages once.

Command Mode: Interface Configuration Mode.

Default: DHCPv6 prefix delegation client is not enabled by default.

Usage Guide: This command is used to configure the prefix delegation client on the specified interface, an interface with prefix delegation client enabled will send SOLICIT packets to try to get address prefix from the server. If the prefix is retrieved correctly, the address prefix in the global address pool can be used by the **ipv6 address** command to generate a valid IPv6 address. This command is exclusive with **ipv6 dhcp server** and **ipv6 dhcp relay destination**. If the prefix delegation client is disabled for an interface, then the address prefix which is get from this interface through prefix delegation client, will be removed from the global address pool. Also the interface address which is generated by the prefix delegation client will be removed, and routing advertisement with the prefix will be disabled. If any general prefix has been configured by the **ipv6 general-prefix** command, the same prefix learnt from prefix delegation will be disagreed.

Example:

Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit

13.1.13 ipv6 dhcp client pd hint

Command: ipv6 dhcp client pd hint *<prefix|prefix-length>*

no ipv6 dhcp client pd hint *<prefix|prefix-length>*

Function: Designate the prefix demanded by the client and its length. The no operation of this command will delete that prefix and its length from the specified interface.

Parameters: *<prefix|prefix-length>* means the prefix demanded by the client and its length.

Command Mode: Interface Configure Mode.

Default Settings: There is no such configuration in the system by default.

Usage Guide: The system designates a prefix and its length on the interface for a client. If client prefix-proxy demanding function is enabled on the interface and hint function is enabled on the switch, the user will have prior claim to the prefix it demands and the prefix length when the server allocates them. Only one hint prefix is allowed in the system.

Examples:

Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48

13.1.14 ipv6 dhcp pool

Command: ipv6 dhcp pool *<poolname>*

no ipv6 dhcp pool *<poolname>*

Function: To configure the address pool for DHCPv6, and enter the DHCPv6 address pool configuration mode. In this mode, information such as the address prefix to be allocated, the DNS

server addresses, and domain names, can be configured for the DHCPv6 client. The no form of this command will remove the configuration of the address pool.

Parameter: < *poolname*> is the address pool name of DHCPv6 with its length no more than 32.

Default: Any DHCPv6 address pool are not configured by default.

Command Mode: Global Mode.

Usage Guide: This command should be launched in global configuration mode, and falls in DHCPv6 address pool configuration mode if launched successfully. To remove a configured address pool, interface bindings related to the address pool, as well as the related address bindings will be removed.

Example: To define an address pool, named 1.

Switch(config)#ipv6 dhcp pool 1

13.1.15 ipv6 dhcp relay destination

Command: ipv6 dhcp relay destination {[*<ipv6-address>*] [interface { *<interface-name>* | vlan *<1-4096>* }] }

no ipv6 dhcp relay destination { [*<ipv6-address>*] [interface { *<interface-name>* | vlan *<1-4096>* }] }

Function: To configure the destination to which the DHCPv6 relay forwards the DHCPv6 requests from the clients, the destination should be the address of an external DHCPv6 relay or the DHCPv6 server. The no form of this command will remove the configuration.

Parameters: *<ipv6-address>* is the address of the destination to which the DHCPv6 relay forwards; ***<interface-name>*** or VLAN is the interface name or VLAN id which is used for forwarding of DHCPv6 requests, ***<interface-name>*** should be a lay three VLAN name, and the VLAN id is limited between 1 and 4096. If ***<ipv6-addess>*** is a global unicast address, the **interface** parameter should not be configured; If ***<ipv6-address>*** is an local address, the **interface** parameter is required be configured; The destination address for the DHCPv6 server will be the multicast address of **ALL_DHCP_Servers (FF05::1:3)**, if the interface parameter is configured only.

Command Mode: Interface Configuration Mode.

Default: By default, destination address for DHCPv6 relay is not configured.

Usage Guide: This command is used to configure the DHCPv6 relay for the specified interface, the address should be the address of another DHCPv6 relay or the address DHCPv6 server. At most three relay addresses can be configured for an interface. To be mentioned, the DHCPv6 relay stops working only if all the relay destination address configurations have been removed. This command is mutually exclusive to "**ipv6 dhcp server**" and "**ipv6 dhcp client pd**" commands.

Example:

Switch(Config-if-Vlan1)#ipv6 dhcp relay destination 2001:da8::1

13.1.16 ipv6 dhcp server

Command: ipv6 dhcp server *<poolname>* [preference *<value>*] [rapid-commit] [allow-hint]

no ipv6 dhcp server *<poolname>*

Function: This command configures the address pool which will be allocated by the DHCPv6

server through the specified interface. The no form of this command will remove the address pool configuration.

Parameters: <*poolname*> is a string with its length less than 32, which designates the name of the address pool which is associated with the specified interface. If the **rapid-commit** option has been specified, the DHCPv6 server send a REPLY packet to the client immediately after receiving the SOLICIT packet. If the **preference** option has been specified, **<*value*>** will be the priority of the DHCPv6 server, with its value allowed between 0 and 255, and with 0 by default, the bigger the preference value is, the higher the priority of the DHCPv6 server. If the **allow-hint** option has been specified, the client expected value of parameters will be appended in its request packets.

Command Mode: Interface Configuration Mode.

Default: DHCPv6 address pool based on port is not configured by default.

Usage Guide: This command configure the DHCPv6 address pool which is applied by the DHCPv6 server for the specified interface, as well as optional parameters. One VLAN can bind many DHCPv6 address pools and assign the address for DHCPv6 request packet from direct-link and relay delegation.

Example:

Switch(Config-if-Vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint

13.1.17 ipv6 general-prefix

Command: ipv6 general-prefix *<prefix-name> <ipv6-prefix/prefix-length>*

no ipv6 general-prefix *<prefix-name>*

Function: To define an IPv6 general prefix. The no form of this command will delete the configuration.

Parameter: *<prefix-name>* is a character string less than 32 characters, to use as IPv6 general prefix name. ***<ipv6-prefix/prefix-length>*** is defined as IPv6 general prefix.

Command Mode: Global Mode.

Default: IPv6 general prefix is not configured by default.

Usage Guide: If IPv6 general prefix is configured, the interface will use the configured prefix for IPv6 address generating. Commonly, the general prefix is used for enterprise IPv6 prefix, and when entering an IPv6 address, users can simply add the address suffix of to the name of the general prefix. The configured address prefix will be reserved in the general address prefix pool. At most 8 general prefix can be configured at the same time. When trying to remove a configured general prefix name, the operation will fail if any interfaces used the configured prefix. Only one general prefix for a prefix name. The general prefix can not use the same prefix definition with prefixes learnt from prefix delegation.

Example: To set the prefix of 2001:da8:221::/48 to general prefix my-prefix.

Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48

13.1.18 ipv6 local pool

Command: ipv6 local pool *<poolname> <prefix/prefix-length> <assigned-length>*

no ipv6 local pool *<poolname>*

Function: To configure the address pool for prefix delegation. The no form of this command will remove the IPv6 prefix delegation configuration.

Parameters: ***<poolname>*** is the name for the IPv6 address pool of the prefix delegation, the length name string should be less than 32. ***<prefix/prefix-length>*** is the address prefix and its length of the prefix delegation. ***<assigned-length>*** is the length of the prefix in the address pool which can be retrieved by the client, the assigned prefix length should be no less than the value of ***<prefix-length>***

Command Mode: Global Mode.

Default: No IPv6 prefix delegation address pool is configured by default.

Usage Guide: This command should be used with the "**prefix delegation pool**" command to allocate address prefixes to the clients. If IPv6 prefix delegation is removed, the associated "**prefix delegation**" command will be in-effective either.

13.1.19 lifetime

Command: lifetime {*<valid-time>* | infinity} {*<preferred-time>* | infinity}

no lifetime

Function: To configure the life time for the addresses or the address prefixes allocated by DHCPv6. The no form of this command will restore the default setting.

Parameters: ***<valid-time>*** **and** ***<preferred-time>*** are the valid life time and preferred life time respectively for the allocated IPv6 addresses in the local address pool. Its value is allowed to be between 1 and 31536000 in seconds, and ***<preferred-time>*** should never be bigger than ***<valid-time>***. The **infinity** parameter designates the maximum life time.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Default: The default valid life time and preferred life time are 2592000 seconds (30 days) and 604800 seconds (7 days) respectively.

Example: To configure the valid life time as 1000 seconds, and the preferred life time as 600 seconds.

Switch(dhcpv6-1-1config)#lifetime 1000 600

13.1.20 network-address

Command: network-address *<ipv6-pool-start-address>* {*<ipv6-pool-end-address>* | *<prefix-length>*} [eui-64]

no network-address

Function: To configure the DHCPv6 address pool; the no form of this command will remove the address pool configuration.

Parameters: ***<ipv6-pool-start-adderss>*** is the start of the address pool; ***<ipv6-pool-end-address>*** is the end of the address pool; ***<prefix-length>*** is the length of the address prefix, which is allowed to be between 3 and 128, and 64 by default, the size of the pool will be determined by ***<prefix-length>*** if it has been specified. ***<ipv6-pool-end-address>*** and ***<prefix-length>*** alternative options to determine the size of the IPv6 address pool. If ***<prefix-length>*** is 64 and the **eui-64** option has been configured, the DHCPv6 server will allocate IPv6 addresses according to the

EUI-64 standard, or the DHCPv6 server will be allocating addresses sequentially.

Default: No address pool is configured by default.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Usage Guide: This command configures the address pool for the DHCPv6 server to allocate addresses, only one address range can be configured for each address pool. To be noticed, if the DHCPv6 server has been enabled, and the length of the IPv6 address prefix has been configured, the length of the prefix in the address pool should be no less than the length of the prefix of the IPv6 address of the respective layer three interfaces in the switch. If ***<ipv6-pool-end-address>*** is bigger than ***<ipv6-pool-start-address>***, this command returns at once.

Example: To configure the address range for address pool as 2001:da8:123::100-2001:da8:123::200.

Switch(dhcpv6-1-config)#network-address 2001:da8:123::100 2001:da8:123::200

Relative Command: excluded-address

13.1.21 prefix-delegation

Command: prefix-delegation *<ipv6-prefix/prefix-length> <client-DUID>* [iaid *<iaid>*] [lifetime {<valid-time> | infinity} {*<preferred-time>* | infinity}]

no prefix-delegation *<ipv6-prefix/prefix-length> <client-DUID>* [iaid *<iaid>*]

Function: To configure dedicated prefix delegation for the specified user. The no form of this command will remove the dedicated prefix delegation.

Parameters: *<ipv6-prefix/prefix-length>* is the length of the prefix to be allocated to the client. ***<client-DUID>*** is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters. ***<iaid>*** is the value to be appended in the IA_PD field of the clients' requests. ***<valid-time>*** and ***<preferred-time>*** are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000. However, **<preferred-time>** should never be bigger ***than*** <valid-time>. If not configured, the ***default*** <valid-time> will be 2592000, ***while*** <preferred-time> will be 604800. The **infinity** parameter means the life time is infinity.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Default: Disabled.

Usage Guide: This command configures the specified IPv6 address prefix to bind with the specified client. If no IAID is configured, any IA of any clients will be able get this address prefix. At most eight static binding address prefix can be configured for each address pool. For prefix delegation, static binding is of higher priority than the prefix address pool.

Example: The following command will allocate 2001:da8::/48 to the client with DUID as 0001000600000005000BBFAA2408, and IAID as 12.

Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48 0001000600000005000BBFAA2408 iaid 12

13.1.22 prefix-delegation add static route

This command is not supported by the switch.

13.1.23 prefix-delegation pool

Command: prefix-delegation pool *<poolname>* [lifetime *{<valid-time>* / **infinity} {*<preferred-time>* | **infinity}]**

no prefix-delegation pool *<poolname>*

Function: To configure prefix delegation name used by DHCPv6 address pool. The no form of this command deletes the configuration.

Parameters: *<poolname>* is the name of the address prefix pool, the length name string should be less than 32. ***<valid-time>*** and ***<preferred-time>*** are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000.However, ***<preferred-time>*** should never be bigger **than <**valid-time>. If not configured, the **default <valid-time**> will be 2592000, **while <preferred-time**> will be 604800. The **infinity** parameter means the life time is infinity.

Command Mode: DHCPv6 address pool configuration mode.

Default: The prefix delegation name used by DHCPv6 address pool is not configured.

Usage Guide: This command configures the name of the address prefix pool for address allocation. If configured, the addresses in the prefix address pool will be allocated to the clients. This command can be used in association with the **ipv6 local pool** command. For one address pool, only one prefix delegation pool can be bound. When trying to remove the prefix name configuration, the prefix delegation service of the server will be unavailable, if both the address pool is not associated with the prefix delegation pool and no static prefix delegation binding is enabled.

Example:

Switch(dhcpv6-1-config)#prefix-delegation pool abc

13.1.24 service dhcpv6

Command: service dhcpv6

no service dhcpv6

Function: To enable DHCPv6 server function; the no form of this command disables the configuration.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: The DHCPv6 services include DHCPv6 server function, DHCPv6 relay function, DHCPv6 prefix delegation function. All of the above services are configured on ports. Only when DHCPv6 server function is enabled, the IP address assignment of DHCPv6 client, DHCPv6 relay and DHCPv6 prefix delegation functions enabled can be configured on ports.

Example: To enable DHCPv6 server.

Switch(config)#service dhcpv6

13.1.25 show ipv6 dhcp

Command: show ipv6 dhcp
Function: To show the enable switch and DUID of DHCPv6 service.
Command Mode: Admin and Configuration Mode.
Usage Guide: To show the enable switch and DUID of DHCPv6 service, server identifier options only use DUID of DUID-LLT type.
Example:
Switch#show ipv6 dhcp
DHCPv6 is enabled
LLT DUID is <00:01:00:01:43:b7:1b:81:00:03:0f:01:5f:9d>
LL DUID is <00:03:00:01:00:03:0f:01:5f:9d>

13.1.26 show ipv6 dhcp binding

Command: show ipv6 dhcp binding [*<ipv6-address>*| pd *<ipv6-prefix|prefix-length>*|count]
Function: To show all the address and prefix binding information of DHCPv6.
Parameter: ***<ipv6-address>*** is the specified IPv6 address; **count** show the number of DHCPv6 address bindings.
Command Mode: Admin and Configuration Mode.
Usage Guide: To show all the address and prefix binding information of DHCPv6, include type, DUID, IAID, prefix, valid time and so on.
Example:
Switch#show ipv6 dhcp binding
Client: iatype IANA, iaid 0x0e001d92
DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83
IANA leased address: 2001:da8::10
Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
Lease obtained at %Jan 01 01:34:44 1970
Lease expires at %Jan 31 01:34:44 1970 (2592000 seconds left)

The number of DHCPv6 bindings is 1

13.1.27 show ipv6 dhcp conflict

Command: show ipv6 dhcp conflict
Function: Show the log for the address that have a conflict record.
Command mode: Admin and Configuration Mode.
Example:
Switch# show ipv6 dhcp conflict

13.1.28 show ipv6 dhcp interface

Command: show ipv6 dhcp interface [<*interface-name*>]

Function: To show the information for DHCPv6 interface.

Parameter: ***<interface-name>*** is the name and number of interface, if the***<interface-name>*** parameter is not provided, then all the DHCPv6 interface information will be shown.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the information for DHCPv6 interface, include Port Mode (Prefix delegation client、DHCPv6 server、DHCPv6 relay) , and the relative conformation information under all kinds of mode.

Example:

Switch**#**show ipv6 dhcp interface vlan10
Vlan10 is in server mode
Using pool: poolv6
Preference value: 20
Rapid-Commit is disabled

13.1.29 show ipv6 dhcp pool

Command: show ipv6 dhcp pool [<*poolname*>]

Function: To show the DHCPv6 address pool information.

Parameter: ***<poolname>*** is the DHCPv6 address pool name which configured already, and the length less than 32 characters. If the ***<poolname>*** parameter is not provided, then all the DHCPv6 address pool information will be shown.

Command Mode: Admin and Configuration Mode.

Usage Guide: To display the configuration and dynamic assignment information for DHCPv6 address pool, include the name of DHCPv6 address pool, the prefix of DHCPv6 address pool, excluded address, DNS server configuration, relative prefix information and so on. To display assigned address binding number of address pool that is used as address assignment server. To display assigned prefix number of address pool that is used as prefix delegation server.

Example:

Switch**#**show ipv6 dhcp pool poolv6

13.1.30 show ipv6 dhcp statistics

Command: show ipv6 dhcp statistics

Function: To show the statistic of all kinds of DHCPv6 packets by DHCPv6 server.

Command Mode: Admin and Configuration Mode.

Example:

Switch#show ipv6 dhcp server statistics
Address pools 1
Active bindings 0
Expiried bindings 0
Malformed message 0

```
Message                 Received
DHCP6SOLICIT             0
DHCP6ADVERTISE          0
DHCP6REQUEST             0
DHCP6REPLY               0
DHCP6RENEW               0
DHCP6REBIND              0
DHCP6RELEASE            0
DHCP6DECLINE             0
DHCP6CONFIRM             0
DHCP6RECONFIGURE        0
DHCP6INFORMREQ           0
DHCP6RELAYFORW           0
DHCP6RELAYREPLY         0

Message                 Send
DHCP6SOLICIT             0
DHCP6ADVERTISE          0
DHCP6REQUEST             0
DHCP6REPLY               0
DHCP6RENEW               0
DHCP6REBIND              0
DHCP6RELEASE            0
DHCP6DECLINE            0
DHCP6CONFIRM             0
DHCP6RECONFIGURE        0
DHCP6INFORMREQ           0
DHCP6RELAYFORW           0
DHCP6RELAYREPLY         0
```

Show information	Explanation
Address pools	To configure the number of DHCPv6 address pools;
Active bindings	The number of auto assign addresses;
Expiried bindings	The number of expiried bindings;
Malformed message	The number of malformed messages;
Message Received	The statistic of received DHCPv6 packets.
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.
DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.

DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.
DHCP6RELAYREPLY	The number of DHCPv6 RELAYREPLY packets.
Message Send	The statistic of sending DHCPv6 packets
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.
DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.
DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.

13.1.31 show ipv6 general-prefix

Command: show ipv6 general-prefix

Function: To show the IPv6 general prefix pool information.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the IPv6 general prefix pool information, include the prefix number in general prefix pool, the name of every prefix, the interface of prefix obtained, and the prefix value.

Example:

Switch#show ipv6 general-prefix

13.1.32 show ipv6 local pool

Command: show ipv6 local pool

Function: To show the statistic information of DHCPv6 prefix pool.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the statistic information of DHCPv6 prefix pool, include the name of prefix pool, the prefix and prefix length as well as assigned prefix length, the number of assigned prefix and information in DHCPv6 address pool.

Example:

Switch#show ipv6 local pool

Pool	Prefix	Free	In use
a	2010::1/48	65536	0

13.2 DHCPv6 option37, 38

13.2.1 Commands for DHCPv6 option37, 38

13.2.1.1 address range

Command: address range <*start-ip*> <*end-ip*>

no address range <*start-ip*> <*end-ip*>

Function: This command is used to set address range for a DHCPv6 class in DHCPv6 address pool configuration mode, the no command is used to remove the address range. The prefix/plen form is not supported.

Parameters: start-ip, defines the start address of the address pool

end-ip, defines the end address of the address pool

Default: None.

Command Mode: DHCPv6 address pool class configuration mode

Usage Guide: It is necessary to check the address range assigned to class in order to make sure that it doesn't exceed the address range of relevant address pool. A class is assigned a single address range and the address range assigned to different class in the same address pool can overlap. If you do not use this command to assign address range for a DHCPv6 class, then the range for it will be the whole subnet of the address pool by default.

Example: Associate a DHCPv6 class named CLASS1 to dhcpv6 pool 1 and assign the address range from 2001:da8:100:1::2 to 2001:da8:100:1::30 for CLASS1.

Switch(Config)#ipv6 dhcp pool 1

Switch(dhcp-1-config)#class CLASS1

Switch(dhcp-1-class-CLASS1-config)#address range 2001:da8:100:1::2 2001:da8:100:1::30

13.2.1.2 class

Command: class <*class-name*>

no class <*class-name*>

Function: This command associates class to address pool in DHCPv6 address pool configuration mode and enters class configuration mode in address pool. Use the no command to remove the link.

Parameters: class-name, the name of DHCPv6 class.

Default: None.

Command Mode: DHCPv6 address pool configuration mode

Usage Guide: It is recommended to define this class first using global command of IPv6 DHCP class. No class will be created if you input a class name which doesn't exist.
Example: Associate the DHCPv6 class named CLASS1 to dhcpv6 pool 1.
Switch(Config)#ipv6 dhcp pool 1
Switch(dhcp-1-config)#class CLASS1

13.2.1.3 ipv6 dhcp class

Command: ipv6 dhcp class <*class-name*>
no ipv6 dhcp class <*class-name*>
Function: This command defines a DHCPv6 class and enters DHCPv6 class configuration mode, the no operation of this command removes this DHCPv6 class.
Parameters: class-name, the name of DHCPv6 class which is a string with a length of less than 32
Default: None.
Command Mode: Global configuration mode
Usage Guide: Configure a group of option 37 or option 38, or configure option 37 and option 38 simultaneously in a DHCPv6 class. This command can be used when the server supports DHCPv6 class only.
Example: Define a DHCPv6 class named CLASS1.
Switch(Config)# ipv6 dhcp class CLASS1

13.2.1.4 ipv6 dhcp relay remote-id

Command: ipv6 dhcp relay remote-id <*remote-id*>
no ipv6 dhcp relay remote-id
Function: This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the remote-id in user-defined option 37 and it is a string with a length of less than 128. The no operation of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address.
Parameters: remote-id, user-defined content of option 37.
Default: Using vlan MAC address as remote-id content by default such as "00-01-ac-12-23" with '-' hyphen.
Command Mode: Interface configuration mode
Usage Guide: Because the option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify the remote-id content based on server condition when default remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.
Example: Enable abc as the remote-id of DHCPv6 option 37.
Switch(Config-if-vlan1)# ipv6 dhcp relay remote-id abc

13.2.1.5 ipv6 dhcp relay remote-id option

Command: ipv6 dhcp relay remote-id option

no ipv6 dhcp relay remote-id option

Function: This command enables switch relay to support the option 37, the no form of this command disables it.

Parameters: None.

Default: Disable the relay option 37.

Command Mode: Global configuration mode

Usage Guide: Only after this command is configured, DHCPv6 relay agent can add option 37 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that DHCPv6 service has been enabled before execute this command.

Example: Enable the switch relay to support option 37.

Switch(Config)#service dhcpv6

Switch(Config)#ipv6 dhcp relay remote-id option

13.2.1.6 ipv6 dhcp relay subscriber-id

Command: ipv6 dhcp relay subscriber-id <subscriber-id>

no ipv6 dhcp relay subscriber-id

Function: This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the subscriber-id in user-defined option 38 and it is a string with a length of less than 128. The no operation of this command restores subscriber-id in option 38 to vlan name together with port name such as "Vlan2+Ethernet1/0/2".

Parameters: subscriber-id, user-defined content of option 38

Default: Set subscriber-id in option 38 to vlan name together with port name.

Command Mode: Interface configuration mode

Usage Guide: Because the option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify the subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as the subscriber-id in option 38 by default.

Example: Enable abc as the subscriber-id of DHCPv6 option 38.

Switch(Config-if-vlan1)# ipv6 dhcp relay subscriber-id abc

13.2.1.7 ipv6 dhcp relay subscriber-id option

Command: ipv6 dhcp relay subscriber-id option

no ipv6 dhcp relay subscriber-id option

Function: This command enables switch relay to support the option 38, the no form of this command disables it.

Parameters: None.

Default: Disable the relay option 38.

Command Mode: Global configuration mode

Usage Guide: Only after this command is configured, DHCPv6 relay agent can add option 38 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that DHCPv6 service has been enabled before execute this command. The option 38 of switch relay is disabled

by default.

Example: Enable the switch relay to support option 38.

Switch(Config)#service dhcpv6

Switch(Config)#ipv6 dhcp relay subscriber-id option

13.2.1.8 ipv6 dhcp relay subscriber-id select delimiter

Command: ipv6 dhcp relay subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |)

no ipv6 dhcp relay subscriber-id select delimiter

Function: Configures user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name.

Parameters: (**sp | sv | pv | spv**): a selection in combinations of slot, port and vlan, among which **sp** represents slot and port, **sv** represents slot and vlan, **pv** represents port and vlan, and **spv** represents slot, port and vlan.

WORD: the delimiter between slot, port and vlan which ranges among (#|.|,|;|:|/|space). Note that there're two **delimiter WORDs** here, of which the former is the delimiter between slot and port and the latter is the one between port and vlan.

Default: Null.

Command Mode: Global configuration mode

Usage Guide: The command has no effect on ports with self-defined subscriber-id. If user redefines the subscriber-id of the port after using the command, the user-defined one prevails. This configuration is null by default.

Example:

Switch(config)# ipv6 dhcp relay subscriber-id select sp delimiter #

13.2.1.9 ipv6 dhcp server remote-id option

Command: ipv6 dhcp server remote-id option

no ipv6 dhcp server remote-id option

Function: This command enables DHCPv6 server to support the identification of option 37, the no form of this command disables it.

Parameters: None.

Default: Do not support option 37.

Command Mode: Global configuration mode

Usage Guide: Configure this command if option 37 options is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. Option 37 is not supported by default.

Example: Enable the DHCPv6 server to support option 37.

Switch(Config)# ipv6 dhcp server remote-id option

13.2.1.10 ipv6 dhcp server select relay-forw

Command: ipv6 dhcp server select relay-forw

no ipv6 dhcp server select relay-forw

Function: This command enables the DHCPv6 server to support selections when multiple option 37 or option 38 options exist and the option 37 and option 38 of relay-forw in the innermost layer are selected. The no operation of it restores the default configuration, i.e. selecting option 37 and option 38 of the original packets.

Parameters: None.

Default: Selecting option 37 and option 38 of the original packets.

Command Mode: Interface configuration mode

Usage Guide: Make sure that the server has been enabled to support option 37 and option 38 before use this command. The system selects option 37 and option 38 of the original packets by default.

Example: Configure that the vlan1 interface of DHCPv6 server selects option 37 and option 38 of relay-forw in the innermost layer.

Switch(Config-if-vlan1)# ipv6 dhcp server select relay-forw

13.2.1.11 ipv6 dhcp server subscriber-id option

Command: ipv6 dhcp server subscriber-id option

no ipv6 dhcp server subscriber-id option

Function: This command enables DHCPv6 server to support the identification of option 38, the no operation of this command disables it.

Parameters: None.

Default: Do not support option 38.

Command Mode: Global configuration mode

Usage Guide: Configure this command if option 38 is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. option 38 is not supported by default.

Example: Enable DHCPv6 server to support option 38.

Switch(Config)# ipv6 dhcp server subscriber-id option

13.2.1.12 ipv6 dhcp snooping information option remote-id format

This command is not supported by the switch.

13.2.1.13 ipv6 dhcp snooping information option subscriber-id format

Command: ipv6 dhcp snooping information option subscriber-id format {hex | acsii }

Function: Configure the default subscribe-id format of the switch DHCPv6 snooping option38.

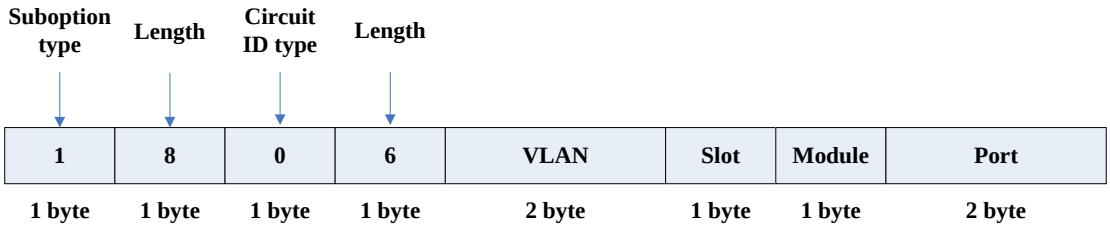
Parameters: hex means that the subscriber-id is the hexadecimal VLAN and port information;

acsii means that the subscriber-id is the ACSII VLAN and port information.

Default: The default subscriber-id format of option38 is acsii.

Command Mode: Global configuration mode

Usage Guide: The ACSII VLAN and port information is as Vlan1+Ethernet1/0/11. The hexadecimal VLAN and port information is defined as below:



The VLAN field is written with the switch VLAN ID. For the rackmount switch, Slot means the slot number; for the cassette switch, it is 1. The default module is 0. Port means the port number and starts from 1.

Example: Configure the subscribe-id format of the switch DHCPv6 snooping option38 as the hexadecimal format.

Switch(config)#ipv6 dhcp snooping information option subscriber-id format hex

13.2.1.14 ipv6 dhcp snooping remote-id

Command: ipv6 dhcp snooping remote-id <*remote-id*>

no ipv6 dhcp snooping remote-id

Function: This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the content of remote-id in user-defined option 37 and it is a string with a length of less than 128. The no form of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address.

Parameters: remote-id, user-defined content of option 37.

Default: Using vlan MAC address as remote-id content by default such as “00-01-ac-12-23” with ‘-’ hyphen.

Command Mode: Port mode

Usage Guide: Because option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify remote-id content based on server condition when standard remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.

Example: Enable abc as remote-id of DHCPv6 option 37.

Switch(Config-if-Ethernet1/0/1)# ipv6 dhcp snooping remote-id abc

13.2.1.15 ipv6 dhcp snooping remote-id option

Command: ipv6 dhcp snooping remote-id option

no ipv6 dhcp snooping remote-id option

Function: This command enables DHCPv6 SNOOPING to support option 37, the no form of this command disables it.

Parameters: None.

Default: Disable.

Command Mode: Global configuration mode

Usage Guide: Only after this command is configured, DHCPv6 SNOOPING can add option 37 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before execute this command. The system disables option 37 of DHCPv6 SNOOPING by default.

Example: Enable option 37 in DHCPv6 SNOOPING.

Switch(Config)#ipv6 dhcp snooping enable

Switch(Config)#ipv6 dhcp snooping remote-id option

13.2.1.16 ipv6 dhcp snooping remote-id policy

Command: ipv6 dhcp snooping remote-id policy {drop | keep | replace}

no ipv6 dhcp snooping remote-id policy

Function: This command is used to configure the reforward policy of the system when receiving DHCPv6 packets with option 37, among which the **drop** mode means that the system simply discards it with option 37, **keep** mode means that the system keeps option 37 unchanged and forwards the packets to the server and **replace** mode means that the system replaces option 37 of current packets with its own before forwarding it to the server. The no operation of this command sets reforward policy of DHCPv6 packets with option 37 as replace.

Parameters: None.

Default: Using replace mode to replace option 37 of current packets with system's own.

Command Mode: Global configuration mode

Usage Guide: Since DHCPv6 client packets may already include option 37 information, corresponding processing policy of DHCPv6 SNOOPING is required to develop. If the forwarding policy is set as **replace**, option 37 has to be enabled in advance. Use replace mode to replace option 37 of current packets with system's own by default.

Example: Configure the reforward policy of DHCPv6 packets with option 37 as keep for DHCPv6 SNOOPING.

Switch(Config)# ipv6 dhcp snooping remote-id policy keep

13.2.1.17 ipv6 dhcp snooping subscriber-id

Command: ipv6 dhcp snooping subscriber-id <subscriber-id>

no ipv6 dhcp snooping subscriber-id

Function: This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the content of subscriber-id in user-defined option 38 and it is a string with a length of less than 128. The no operation of this command restores subscriber-id in option 38 to vlan name together with port name such as "Vlan2+Ethernet1/0/2".

Parameters: subscriber-id, user-defined content of option 38

Default: Set subscriber-id in option 38 to vlan name together with port name.

Command Mode: Port mode

Usage Guide: Because option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as subscriber-id in option 38 by default.

Example: Enable abc as subscriber-id of DHCPv6 option 38.

Switch(Config-if-Ethernet1/0/1)#ipv6 dhcp snooping subscriber-id abc

13.2.1.18 ipv6 dhcp snooping subscriber-id option

Command: ipv6 dhcp snooping subscriber-id option

no ipv6 dhcp snooping subscriber-id option

Function: This command enables DHCPv6 SNOOPING to support option 38, the no form of this command disables it.

Parameters: None.

Default: Disable option 38 of DHCPv6 SNOOPING.

Command Mode: Global configuration mode

Usage Guide: Only after this command is configured, DHCPv6 SNOOPING can add option 38 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before executing this command. The system disables option 38 of DHCPv6 SNOOPING by default.

Example: Enable option 38 in DHCPv6 SNOOPING.

Switch(Config)#ipv6 dhcp snooping enable

Switch(Config)#ipv6 dhcp snooping subscriber-id option

13.2.1.19 ipv6 dhcp snooping subscriber-id policy

Command: ipv6 dhcp snooping subscriber-id policy {drop | keep | replace}

no ipv6 dhcp snooping subscriber-id policy

Function: This command is used to set the reforward policy of the system when receiving DHCPv6 packets with option 38, among which the **drop** mode means that the system simply discards it with option 38, **keep** mode means that the system keeps option 38 unchanged and forwards the packets to the server and **replace** mode means that the system replaces option 38 of current packets with its own before forwarding it to the server. The no operation of this command sets the reforward policy of DHCPv6 packets with option 38 as replace.

Parameters: None.

Default: Using replace mode to replace option 38 of current packets with system's own.

Command Mode: Global configuration mode

Usage Guide: Since DHCPv6 client packets may already include option 38 information, corresponding processing policy of DHCPv6 SNOOPING is requested to develop. If the reforward policy is set as **replace**, option 38 has to be enabled in advance. The system disables option 38 of

DHCPv6 SNOOPING by default.

Example: Set the reforward policy of DHCPv6 packets with option 38 as keep for DHCPv6 SNOOPING.

Switch(Config)# ipv6 dhcp snooping subscriber-id policy keep

13.2.1.20 ipv6 dhcp snooping subscriber-id select delimiter

Command: ipv6 dhcp snooping subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |)

no ipv6 dhcp snooping subscriber-id select delimiter

Function: Configure user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name.

Parameters: (**sp | sv | pv | spv**), a selection from combinations of slot, port and vlan, among which **sp** represents slot and port, **sv** represents slot and vlan, **pv** represents port and vlan, and **spv** represents slot, port and vlan.

WORD, the delimiter between slot, port and vlan which ranges among (#|.|,|;|:|/|space). Note that there're two delimiter WORDs here, of which the former is the delimiter between slot and port while the latter is that between port and vlan.

Default: Null.

Command Mode: Global configuration mode

Usage Guide: This command has no effect on ports with self-defined subscriber-id. If a user redefines subscriber-id of the port after configuring the command, the user-defined one prevails. This configuration is null by default.

Example:

Swithc(config)# ipv6 dhcp snooping subscriber-id select sv delimiter #

13.2.1.21 ipv6 dhcp use class

Command: ipv6 dhcp use class

no ipv6 dhcp use class

Function: This command enables DHCPv6 server to support DHCPv6 class during address assignment, the no operation of this command disables it without removing the relative DHCPv6 class information that has been configured.

Parameters: None.

Default: DHCPv6 server supports DHCPv6 class during address assignment.

Command Mode: Global configuration mode

Usage Guide: By default, DHCPv6 servers support DHCPv6 class during address assignment and the no form of this command doesn’t remove DHCPv6 class information that has been configured. Make sure that DHCPv6 service has been enabled before using this command. DHCPv6 server supports DHCPv6 class during address assignment by default.

Example: Configure DHCPv6 server to support DHCPv6 class during address assignment.

Switch(Config)# ipv6 dhcp use class

13.2.1.22 remote-id subscriber-id

Command: {remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*]}
no {remote-id [*] <remote-id> [*] | subscriber-id [*] < subscriber-id> [*]}

Function: This command configures option 37 and option 38 that match the class in IPv6 DHCP class configuration mode.

Parameters: <remote-id>, a string with a length ranging from 1 to 128 bytes is used to match remote-id in option 37.

<subscriber-id>, a string with a length ranging from 1 to 128 bytes is used to match subscriber-id in option 38.

[*], match zero or more characters.

Default: None.

Command Mode: IPv6 DHCP Class configuration mode

Usage Guide: This command configures a mode which matches with the already-defined DHCPv6 class, and a DHCPv6 class may configure multiple commands. If this command is ignored and no mode configured in IPv6 DHCP Class mode, any remote-id or subscriber-id is considered to match with the DHCPv6 class, however, remote-id or subscriber-id must exist in DHCPv6 packet.

Example: Configure some remote-id or subscriber-id belonging to DHCPv6 class named CLASS1.

```
Switch(Config)# ipv6 dhcp class CLASS1
Switch(Dhcpv6-class)#remote-id abc* subscriber-id bcd*
Switch(Dhcpv6-class)#remote-id edf*
Switch(Dhcpv6-class)#subscriber *mmn
```

13.2.2 Commands for Monitoring and Debugging

13.2.2.1 debug ipv6 dhcp detail

Command: debug ipv6 dhcp detail

Function: Display the debug about detailed content of various packets sent and received by DHCPv6. If packets with option 37 and option 38, they will also be displayed. This command is applied in the server side as well as the relay side.

Parameters: None.

Command Mode: Admin mode

Usage Guide: Enable/disable the display of detailed debug about packets sent and received by DHCPv6.

Example:

```
Switch# debug ipv6 dhcp detail
%Jan 01 01:38:45 2006 DHCPv6 DETAILS: contents of SOLICIT packet
%Jan 01 01:38:45 2006        transaction-ID: 0x00b2d47c
%Jan 01 01:38:45 2006      elapsed time option(8), option-len 2
%Jan 01 01:38:45 2006        elapsed time: 0
%Jan 01 01:38:45 2006      client ID option(1), option-len 14
```

%Jan 01 01:38:45 2006 DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83
%Jan 01 01:38:45 2006 identity association option(3), option-len 12
%Jan 01 01:38:45 2006 IANA: 0x0e001d92, T1 0, T2 0
%Jan 01 01:38:45 2006 vendor class option(16), option-len 14
%Jan 01 01:38:45 2006 enterprise number : 311
%Jan 01 01:38:45 2006 option request option(6), option-len 6
%Jan 01 01:38:45 2006 requested-option: domain search list
%Jan 01 01:38:45 2006 requested-option: DNS server list
%Jan 01 01:38:45 2006 requested-option: vendor specific info
%Jan 01 01:38:45 2006 remote-id option(37), option-len 14
%Jan 01 01:38:45 2006 remote-id : 0x0a0b0c
%Jan 01 01:38:45 2006 subscriber-id option(38), option-len 16
%Jan 01 01:38:45 2006 subscriber-id : 0x0a0b0c0d

13.2.2.2 debug ipv6 dhcp relay packet

Command: debug ip dhcp relay packet
Function: Display the information of relay packet processing.
Parameters: None.
Command Mode: Admin mode
Usage Guide: This command is used to display the process of relay packet processed by relay agent together with the action information of option 37 and option 38.
Example:
Switch# debug ip dhcpv6 relay packet
%May 19 16:45:34 2010 DHCPv6 RELAY PACKET: received msg0 from <fe80::211:22ff:fe33:4455> on <Vlan8>
%May 19 16:45:34 2010 DHCPv6 RELAY PACKET: add subscriber-id option “Vlan8+Ethernet1/0/12”

13.2.2.3 debug ipv6 dhcp snooping packet

Command: debug ipv6 dhcp snooping packet
Function: Debug the packets of DHCPv6 SNOOPING. Corresponding information will also be displayed when adding or deleting option 37 and option 38.
Parameters: None.
Command Mode: Admin mode
Usage Guide: Enable/disable the information of DHCPv6 packets processed by DHCPv6 Snooping, including the type of received packet, source MAC and destination MAC, client DUID, i.e. the client identification, IA address, preferred lifetime, valid lifetime, and packet discard and so on.
Example:
switch#debug ipv6 dhcp snooping packet
dhcpv6 snooping packet debug is on
switch#%Jan 05 00:26:40 2006 DHCP6SNP EVENT: Parse packet SOLICIT from fe80::200:ff:fe00:1

src MAC 00-00-00-00-00-01 interface Ethernet1/0/23 vlan 24
%Jan 05 00:26:40 2006 DHCP6SNP PACKET: Receive DHCPv6 packet SOLICIT from fe80::200:ff:fe00:1
src MAC 00-00-00-00-00-01, dst MAC 33-33-00-01-00-02,
interface Ethernet1/0/23 vlan 24,
transaction-ID 6137412, smac host flag 0, dmac host flag 0
%Jan 05 00:26:40 2006 DHCP6SNP PACKET: Forward packet SOLICIT (protocol 0x37)
%Jan 05 00:26:40 2006 DHCP6SNP PACKET: to vlan 24 except port Ethernet1/0/23 (designPort flag 0)
%Jan 05 00:26:40 2006 DHCP6SNP PACKET: and return packet to network stack
switch#

13.2.2.4 show ipv6 dhcp relay option

Command: show ipv6 dhcp relay option
Function: Display the configuration of system relay agent, including the enable switch for option 37 and option 38.
Parameters: None.
Command Mode: Admin mode
Usage Guide: Use this command to check relay agents' configuration status for option 37 and option 38.
Example:
Switch#show ipv6 dhcp relay option
remote-id option enable
subscriber-id option enable
Interface Vlan 1: remote-id option configure "abc"

13.2.2.5 show ipv6 dhcp snooping option

Command: show ipv6 dhcp snooping option
Function: Display the configuration information of system snooping, including the enable switch for option 37 and option 38.
Parameters: None.
Command Mode: Admin mode
Usage Guide: Use this command to check snooping configuration status for option 37 and option 38.
Example:
Switch#show ipv6 dhcp snooping option
remote-id option enable
subscriber-id option enable
The slot port vlan select option is : port and vlan
The delimiter is : #

13.3 Prevent ND Spoofing

13.3.1 ipv6 nd-security updateprotect

Command: ipv6 nd-security updateprotect

no ipv6 nd-security updateprotect

Function: Forbid ND automatic update function of IPv6 Version, the no command resets ND automatic update function.

Parameter: None

Default: ND update normally.

Command Mode: Global Mode/ Interface configuration

User Guide: Forbid ND table automatic update, the ND packets conflicting with current ND item (e.g. with same IP but different MAC or port) will be droped, the others will be received to update aging timer or create a new item; so, the current ND item keep unchanged and the new item can still be learned.

Example:

Switch(Config-if-Vlan1)#ipv6 nd -security updateprotect

Switch(config)#ipv6 nd -security updateprotect

13.3.2 ipv6 nd-security learnprotect

Command: ipv6 nd-security learnprotect

no ipv6 nd-security learnprotect

Function: Forbid ND learning function of IPv6 Version, the no command re-enables ND learning function.

Parameter: None.

Default: ND learning enabled.

Command Mode: Global Mode/ Interface Configuration.

Usage Guide: This command is for preventing the automatic learning and updating of ND. Unlike ip nd-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.

Example:

Switch(Config-if-Vlan1)#ipv6 nd -security learnprotect

Switch(config)#ipv6 nd -security learnprotect

13.3.3 ipv6 nd-security convert

Command: ipv6 nd-security convert

Function: Change all dynamic ND to static ND.

Parameter: None

Command Mode: Global Mode/ Interface Configuration

Usage Guide: This command will convert the dynamic ND entries to static ones, which, in combination with disabling automatic learning, can prevent ND binding. Once implemented, this command will lose its effect.

Example:

Switch(Config-if-Vlan1)#ipv6 nd -security convert

Switch(config)#ipv6 nd -security convert

13.4 RIPng

13.4.1 clear ipv6 route

Command: clear ipv6 rip route {*<ipv6-address >*| kernel |static | connected |rip |ospf |isis | bgp |all }

Function: Clear specific route from the RIPng route table.

Parameter: Clears the route exactly match with the destination address from the RIP route table.

<ipv6-address > is the destination address shown in hex notation with prefix length.

kernel delete kernel route from the RIPng route table

static delete static route from the RIPng route table

connected delete direct route from the RIPng route table

rip delete RIPng route from the RIPng route table only

ospf delete IPv6 OSPF route from the RIPng route table only

bgp delete IPv6 BGP route from the RIPng route table only

ISIS delete ivp6 isis route from the RIPng route table only

all delete all routes from the RIPng route table

Default: No default configuration

Command Mode: Admin mode

Usage Guide: All routes in the RIPng route table will be deleted by using this command with all parameters.

Example: Switch#clear ipv6 rip route 2001:1:1::/64

Switch#clear ipv6 rip route ospf

13.4.2 default-information originate

Command: default-information originate

no default-information originate

Function: Permit redistributing the network 0:: into RIPng. The "**no default-information originate**" disables this function.

Parameter: None

Default: Disabled

Command Mode: Router mode

Example: Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#default-information originate

13.4.3 default-metric

Command: default-metric <*value*>

no default-metric

Function: Set the default metric route value of the introduced route; the "**no default-metric**" restores the default value.

Parameter: <*value*> is the route metric value to be set, ranging between 1～16.

Default: Default route metric value is 1.

Command Mode: Router mode

Usage Guide: default-metric command is used for setting the default route metric value of the routes from other routing protocols when distributed into the RIPng routes. When using the **redistribute** commands for introducing routes from other protocols, the default route metric value specified by **default-metric** will be adopted if no specific route metric value is set.

Example: Set the default route metric value of the routes from other routing protocols when distributed into the RIPng routes as 3.

Switch(config-router)#default-metric 3

Related Command: redistribute

13.4.4 distance

Command: distance <*number*> [<*ipv6-address*>] [<*access-list-name | access-list-number*>]

no distance [<*ipv6-address*>]

Function: Set the managing distance with this command. The "**no distance [<*A.B.C.D/M*>]**" command restores the default value to 120.

Parameter: <*number*> specifies the distance value, ranging between 1-255. ***<ipv6-address>*** is the local link address or its prefix. ***<access-list-name|access-list-number>*** specifies the access-list number or name applied.

Default: The default managing distance of RIP is 120.

Command Mode: Router mode and address-family mode.

Usage Guide: In case there are routes from two different routing protocols to the same destination, the managing distance is then used for selecting routes. The less the managing distance of the route protocol is, the more reliable will be the route acquired from the protocol.

Example:

Switch#config terminal

Switch(config)#router rip
Switch(config-router)#distance 8 fe80:1111::4200:21ff:fe00:11 mylist

13.4.5 distribute-list

Command: distribute-list {*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>|vlan <*vlan-id*>]

no distribute-list {*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>|vlan <*vlan-id*>]

Function: This command uses access-list or prefix-list to filter the route renews messages sent and received. The "**no distribute-list {*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>|vlan <*vlan-id*>]**" command cancels this filter function.

Parameter: ***<access-list-name>*** is the name or access-list number to be applied. ***<prefix-list-name>*** is the name of the prefix-list to be applied. ***<ifname>*** specifies the name of interface to be applied with route filtering.

Default: Function disabled by RIPng by default.

Command Mode: Router mode

Usage Guide: The filter will be applied to all interfaces if no specific interface is set.

Example: Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#distribute-list prefix myfilter in Vlan1

13.4.6 debug ipv6 rip

Command: debug ipv6 rip [events| nsm| packet [recv|send][detail]| all]

no debug ipv6 rip [events| nsm| packet [recv|send][detail]| all]

Function: For opening various debugging switches of RIPng, showing various debugging messages. The "**no debug ipv6 rip [events| nsm| packet [recv|send][detail]| all]**" command closes the corresponding debugging switch.

Parameter: events shows the debugging message of RIPng events

nsm shows the communication messages between RIPng and NSM.

packet shows the debugging messages of RIPng data packets

recv shows the messages of the received data packets

send shows the messages of the sent data packets

detail shows the messages of the data packets received or sent.

Default: Not enabled

Command Mode: Admin mode

Example: Switch#debug ipv6 rip packet

Switch#1970/01/01 21:15:08 IMI: SEND[Ethernet1/0/4]: Send to [ff02::9]:521

1970/01/01 21:15:08 IMI: SEND[Ethernet1/0/2]: Send to [ff02::9]:521

1970/01/01 21:15:09 IMI: RECV[Ethernet1/0/4]: Receive from [fe80::20b:46ff:fe57:8e60]:521

1970/01/01 21:15:09 IMI: RECV[Ethernet1/0/4]: 3000:1:1::/64 is filtered by access-list dclist

1970/01/01 21:15:09 IMI: RECV[Ethernet1/0/4]: 3ffe:1:1::/64 is filtered by access-list dclist

1970/01/01 21:15:15 IMI: RECV[Ethernet1/0/2]: Receive from [fe80::203:fff:fe01:257c]:521

13.4.7 debug ipv6 rip redistribute message send

Command: debug ipv6 rip redistribute message send

no debug ipv6 rip redistribute message send

Function: To enable the debugging of sending messages for routing redistribution messages from OSPFv3 or other external process for RIPng. The no form of this command will disable the debugging messages.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch# debug ipv6 rip redistribute message send

Switch# no debug ipv6 rip redistribute message send

13.4.8 debug ipv6 rip redistribute route receive

Command: debug ipv6 rip redistribute route receive

no debug ipv6 rip redistribute route receive

Function: To enable the debugging switch received from NSM for redistribution of routing information for RIPng. The no form of this command will disable the debugging switch.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch#debug ipv6 rip redistribute route receive

Switch# no debug ipv6 rip redistribute route receive

13.4.9 ipv6 rip aggregate-address

Command: ipv6 rip aggregate-address X:X::X:X/M

no ipv6 rip aggregate-address X:X::X:X/M

Function: To configure IPv6 aggregation route. The no form of this command deletes the IPv6 aggregation route.

Parameter: X:X::X:X/M: IPv6 address and prefix length.

Command Mode: Router Mode or Interface Configuration Mode.

Default: No aggregation route configured.

Usage Guide: If to configure aggregation route under router mode, RIPng protocol must be enabled. If configured under interface configuration mode, RIPng protocol may not be enabled, but the aggregation route can operation after the RIPng protocol be enabled on interface.

Example: To configure aggregation route as 2001:3f:ed8::99/64 globally.
Switch(config)#router rip
Switch(config-router) #ipv6 rip agg 2001:3f:ed8::99/64

13.4.10 ipv6 rip split-horizon

Command: ipv6 rip split-horizon [poisoned]
no ipv6 rip split-horizon
Function: Permit the split horizon. The "**no ipv6 rip split-horizon**" disables the split horizon.
Parameter: [poisoned] configures split horizon with poison reverse.
Default: Split horizon with poison reverse.
Command Mode: Interface Configuration Mode.
Usage Guide: The split horizon is for preventing the routing loops, namely preventing the layer 3 switch from broadcasting a route at the interface from which the very route is learnt. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example: Switch#config terminal
Switch(config)#interface Vlan1
Switch(config-if-Vlan1)#ipv6 rip split-horizon poisoned

13.4.11 ipv6 router rip

Command: ipv6 router rip
no ipv6 router rip
Function: Enable RIPng on the interface. The "no ipv6 router rip" command disables RIPng on the interface.
Default: Not configured
Command Mode: Interface Configuration Mode.
Usage Guide: The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example: Switch#config terminal
Switch(config)#interface Vlan1
Switch(Config-if-Vlan1)#ipv6 router rip

13.4.12 neighbor

Command: neighbor <*ipv6-address*> {<*ifname*> vlan <*vlan-id*>}
no neighbor <*ipv6-address*> {<*ifname*> vlan <*vlan-id*>}
Function: Specify the destination address for fixed sending. The "**no neighbor <*ipv6-address*> <*ifname*> vlan <*vlan-id*>**" cancels the specified address defined and restores all trusted gateways.
Parameter: <*ipv6-address*> is the IPv6 Link-local address specified for sending and shown in colon hex notation without the prefix length. **<*ifname*>** is the name of interface.
Default: Not sending to any fixed destination address.

Command Mode: Router mode

Usage Guide: When used associating passive-interface command it would be able to send routing messages to specified neighbor only.

Example: Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#neighbor FE80:506::2 Vlan1

Related Command: passive-interface

13.4.13 offset-list

Command: offset-list <*access-list-number*|*access-list-name*> {in|out} <*number* >[<*ifname*>|vlan <*vlan-id*>]

no offset-list <*access-list-number*|*access-list-name*> {in|out }<*number* >[<*ifname*>|vlan <*vlan-id*>]

Function: Add an offset value on the routing metric value learnt by RIPng. The "**no offset-list <*access-list-number*|*access-list-name*> {in|out} <*number* >[<*ifname*>|vlan <*vlan-id*>]**" command disables this function.

Parameter: <*access-list-number* |*access-list-name*> is the access-list or name to be applied. **<*number*>** is the additional offset value, ranging between 0-16; **<*ifname*>** is the name of specific interface.

Default: The default offset value is the metric value of the interface defined by the system.

Command Mode: Router mode

Example: Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#offset-list 1 in 5 Vlan1

Related Command: access-list

13.4.14 passive-interface

Command: passive-interface<*ifname*>|vlan <*vlan-id*>

no passive-interface<*ifname*>|vlan <*vlan-id*>

Function: Set the RIPng layers 3 switches to block RIPng broadcast on the specified interfaces, and only send the RIPng data packet to the layer 3 switch which is configured with neighbor.

Parameter: <*ifname*> is the specific interface name.

Default: Not configured

Command Mode: Router mode

Example: Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#passive-interface Vlan1

Related Command: show ipv6 rip

13.4.15 redistribute

Command: redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]

no redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]

Function: Introduce the routes learnt from other routing protocols into RIPng.

Parameter: kernel introduce from kernel routes

connected introduce from direct routes

static introduce from static routes

ospf introduce from IPv6 OSPF routes

isis introduce from IPv6 ISIS routes

bgp introduce from IPv6 BGP routes

<value> is the metric value assigned to the introduced route, ranging between 0-16

<word> is the probe poining to the route map for introducing routes

Command Mode: Router mode

Example: Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#redistribute kernel route-map ip

13.4.16 redistribute ospf

Command: redistribute ospf [<*process-tag*>] [metric<*value*>] [route-map<*word*>]

no redistribute ospf [<*process-tag*>]

Function: To redistribute routing information from external OSPFv3 processes to RIPng process. The no form of this command will remove the introduced OSPFv3 routing entries.

Parameters: process-tag is the string tag for OSPFv3 process with maximum length limited within 15 characters. If not specified, the default process will be used.

metric<*value*> is the metric for the introduced routing entries, limited between 0 and 16.

route-map<*word*> is the pointer to the introduced routing map.

Default: Not redistributed by default.

Command Mode: RIPng Configuration Mode.

Usage Guide: None.

Example: To redistribute OSPFv3 ABC routing ro RIPng.

Switch(config)#router ipv6 rip

Switch (config-router)#redistribute ospf abc

13.4.17 route

Command: route <*ipv6-address*>

no route <*ipv6-address*>

Function: This command configures a static RIPng route. The "**no route <*ipv6-address*>**" command deletes this route.

Parameter: Specifies this destination IPv6 address prefix and its length show in colon hex

notation.

Usage Guide: The command adds a static RIPng route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIPng route database, however it could be located by using the show ipv6 rip command.

Command Mode: Router mode

Example: Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#route 3ffe:1234:5678::1/64

13.4.18 router ipv6 rip

Command: router ipv6 rip

no router ipv6 rip

Function: Enable RIPng routing process and entering RIPng mode; the "**no router ipv6 rip**" of this command disables the RIPng routing protocol.

Default: RIPng routing not running.

Command Mode: Global mode

Usage Guide: This command is for enabling the RIPng routing protocol, this command should be enabled before performing other global configuration of the RIPng protocol.

Example: Enable the RIPng protocol mode.

Switch(config)#router ipv6 rip

13.4.19 show debugging ipv6 rip

Command: show debugging ipv6 rip

Function: Show RIPng debugging status for following debugging options: nsm debugging, RIPng event debugging, RIPng packet debugging and RIPng nsm debugging.

Command Mode: Admin mode

Example:

Switch#show debugging ipv6 rip

RIPng debugging status:

RIPng event debugging is on

RIPng packet detail debugging is on

RIPng NSM debugging is on

13.4.20 show ipv6 rip interface

Command: show ipv6 rip interface

Function: Make sure the interface and line protocols is up.

Command Mode: Admin mode

Example: Switch(config)#show ipv6 rip interface

Loopback is up, line protocol is up

RIPng is not enabled on this interface

Vlan1 is up, line protocol is up
Routing Protocol: RIPng
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IPv6 interface address:
3000:1:1::1/64
fe80::203:fff:fe0c:cda/64

Displayed information	Explanations
Vlan1 is up, line protocol is up	Interface is Up
Routing Protocol: RIP	The routing protocol running on the interface is RIPng
Passive interface: Disabled	Passive-interface disabled
Split horizon: Enabled with Poisoned Reversed	The split horizon is enabled with poisoned reversed on the interface.
IP interface address: 3000:1:1::1/64 fe80::203:fff:fe01:429e/64	IPv6 address of the interface

13.4.21 show ipv6 rip redistribute

Command: show ipv6 rip redistribute
Function: Show the configuration information of redistributed other out routing to RIPng.
Parameter: None.
Default: Not shown by default.
Command Mode: Admin Mode and Configuration Mode.
Usage Guide: None.
Example:
Switch#show ipv6 rip redistribute

13.4.22 show ipv6 protocols rip

Command: show ipv6 protocols rip
Function: Show the RIPng process parameters and statistic messages.
Command Mode: Admin mode
Example: Switch(config)#show ipv6 protocols rip
Routing Protocol is "RIPng"
Sending updates every 30 seconds with +/-50%, next due in 1 second
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Ethernet1/0/4 filtered by dclist
Default redistribute metric is 1

Redistributing: static
Interface
Vlan10
Vlan2
Routing for Networks:

Displayed information	Explanations
Sending updates every 30 seconds with +/-50%, next due in 1 seconds	Sending updates every 30 seconds
Timeout after 180 seconds, garbage collect after 120 seconds	The route timeout time is 180 seconds, the garbage collect time is 120 seconds
Outgoing update filter list for all interface is not set	Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set	Incoming update filter list for all interface is not set
Default redistribution metric is 1	Default redistribution metric is 1
Redistributing: static	Redistricting the static route into the RIP routes
Interface Vlan10 Vlan2	The interfaces running RIP is Vlan 10 and Vlan 2

13.4.23 show ipv6 rip

Command: show ipv6 rip
Function: Show RIPng Routing.
Command Mode: Admin mode
Example: Switch#show ipv6 rip
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP, a - aggregate, s - suppressed

	Network	Next Hop	If	Met	Tag	Time
R	2000:1:1::/64	::	Vlan2	1	0	
R	2001:1:1::/64	fe80::203:fff:fe01:257c	Vlan2	2	0	02:40
R	3000:1:1::/64	::	Vlan10	1	0	
R	3010:1:1::/64	::	--	1	0	

Amongst R stands for RIP route, namely a RIP route with the destination network address 2001:1:1::/64, next-hop address at fe80::203:fff:fe01:257c. It is learnt from the Ethernet port VLAN2 with a metric value of 2, and still has 2 minutes 40 seconds before time out.
Equal Command: show ipv6 rip database

13.4.24 show ipv6 rip database

Command: show ipv6 rip database
Function: Show messages related to RIPng database.
Command Mode: Admin mode
Example: Switch#show ipv6 rip database
Equal Command: show ipv6 rip

13.4.25 show ipv6 rip aggregate

Command: show ipv6 rip aggregate
Function: To display the information of IPv6 aggregation route.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Default: None.
Usage Guide: This command is used to display which interface the aggregation route be configured, Metric, Count, Suppress and so on, if configured under global mode, then the interface display "----". "Metric" is metric. "Count" is the number of learned aggregation routes. "Suppress" is the times of aggregation.
Example: To display the information of IPv6 aggregation route.
Switch(config-router)#show ipv rip agg

Aggregate information of ripng

Network	Aggregated Ifname	Metric	Count	Suppress
2001::/16	Vlan1	1	2	0
2001:1::/32	----	1	2	0
2001:1:2::/60	Vlan1	1	1	1
	----	1	1	1

Displayed information	Explaination
Network	Route prefix and prefix length.
Aggregated Ifname	To configure the interface name of the aggregation route. If the route aggregated globally, then display "---".
Metric	Metric of aggregation route.
Count	The number of learned aggregation routes.
Suppress	The times of aggregated for aggregation route.

13.4.26 show ipv6 rip redistribute

Command: show ipv6 rip redistribute
Function: Show the configuration information of redistributed other out routing to RIPng.
Parameter: None.
Default: Not shown by default.

Command Mode: Admin Mode and Configuration Mode.
Usage Guide: None.
Example:
Switch#show ipv6 rip redistribute

13.4.27 timers basic

Command: timers basic <*update*> <*invalid*> <*garbage*>
no timers basic
Function: Adjust the RIP timer update, timeout, and garbage collecting time. The "**no timers basic**" command restores each parameter to their default values.
Parameter: ***<update>*** time interval of sending update packet, shown in seconds and ranging between 5-2147483647; ***<invalid>*** time period after which the RIP route is advertised dead, shown in seconds and ranging between 5-2147483647; ***<garbage>*** is the hold time in which the a route remains in the routing table after advertised dead, shown in seconds and ranging between 5-2147483647.
Default: ***<update>*** defaulted at 30; ***<invalid>*** defaulted at 180; ***<garbage>*** defaulted at120
Command Mode: Router mode
Usage Guide: The system is defaulted broadcasting RIPng update packets every 30 seconds; and the route is considered invalid after 180 seconds but still exists for another 120 seconds before it is deleted from the routing table.
Example: Set the RIP update time to 20 seconds and the timeout period to 80 seconds, the garbage collecting time to 60 seconds.
Switch(Config-Router)#timers basic 20 80 60

13.5 OSPFv3

13.5.1 area authentication-mode

Command: area (A.B.C.D|<0-4294967295>) authentication-mode (hmac-sha-256) key-id <0-65535> (0 LINE|7 WORD)
no area (A.B.C.D|<0-4294967295>) authentication-mode
Function: Configure OSPFv3 area to use RFC7166 authentication; the "**no area <*id*> authentication-mode**" command restores the default value.
Parameter: <*id*> is the area number which could be shown in digit, ranging from 0 to 4294967295, or in IP address.
(hmac-sha-256): Encryption method, currently only supports hmac-sha-256 method.
<0-65535>key-id value.
(0 WORD |7 WORD): The content of the authenticated key, if the key option is 0, specifies the plaintext key subsequently. If option 7, it will be specified as the ciphertext string encrypted with the plaintext key. The key length range is 1-128.
Default: No authentication.

Command Mode: OSPFv3 protocol mode

Usage Guide: Configure OSPFv3 area to use RFC7166 authentication. Authentication methods can also be configured in interface mode, with priority given to authentication configuration methods in the interface over those in the region. After configuring the authentication method for the interface, the authentication method for the region where the interface is located cannot affect the authentication behavior of the interface. Only one configuration of this type is allowed in a area.

Example:

Switch(config-router)# area 0 authentication-mode hmac-sha-256 key-id 1 0 qwerty

13.5.2 area default cost

Command: area <*id*> default-cost <*cost*>

no area <*id*> default-cost

Function: Configure the cost of sending to the default summary route in stub or NSSA area; the "**no area <*id*> default-cost**" command restores the default value.

Parameter: <*id*> is the area number which could be shown as digits 0～4294967295, or as an IP address; **<*cost*>** ranges between <0-16777214>

Default: Default OSPFv3 cost is 1.

Command Mode: OSPFv3 protocol mode

Usage Guide: The command is only adaptive to the ABR router connected to the stub area.

Example: Set the default-cost of area 1 to 10

Switch(config-router)#area 1 default-cost 10

13.5.3 area range

Command: area <*id*> range <ipv6*address*> [advertise| not-advertise|]

no area <*id*> range <ipv6*address*>

Function: Aggregate OSPF route on the area border. The "**no area <*id*> range <*address*>**" cancels this function.

Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

<ipv6*address*>=<*X:X::X:X/M*>,Specifies the area ipv6 network prefix and its length

advertise: Advertise this area

not-advertise : Not advertise this area

If both are not set, this area is defaulted for advertising

Default: Function not configured.

Command Mode: OSPFv3 protocol mode

Usage Guide: Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this

command on ABR. This route consists of all single networks belong to specific range.

Example:

Switch # config terminal

Switch (config)# router ipv6 ospf

Switch (config-router)# area 1 range 2000::/3

13.5.4 area stub

Command: area <*id*> stub [no-summary]

no area <*id*> stub [no-summary]

Function: Define an area to a stub area. The "**no area <*id*> stub [no-summary]**" command cancels this function.

Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IPv4 address.

no-summary: The area border routes stop sending link summary announcement to the stub area

Default: Not defined

Command Mode: OSPFv3 protocol mode

Usage Guide: Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.

Example:

Switch # config terminal

Switch (config)# router ipv6 ospf

Switch (config-router)# area 1 stub

Relevant Commands: area default-cost

13.5.5 area virtual-link

Command: area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | INTERVAL <*value*>]

no area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | INTERVAL]

Function: Configure a logical link between two backbone areas physically divided by non-backbone area. The "**no area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | INTERVAL]**" command removes this virtual-link.

Parameter: <***id***> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

<***instance-id***> is the interface instance ID ranging between 0~255 and defaulted at 0

INTERVAL*= [dead-interval***|***hello-interval***|***retransmit-interval***|***transmit-delay***]**

<*value*>: The delay or interval seconds, ranging between 1~65535

***<dead-interval>*:** A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds.

***<hello-interval>*:** The time interval before the router sends a hello group message, default is 10 seconds

***<retransmit-interval>*:** The time interval before a router retransmitting a group message, default is 5 seconds

***<transmit-delay>*:** The time delay before a router sending a group messages, 1 second by default

Default: No default configuration.

Command Mode: OSPFv3 protocol mode

Usage Guide: In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone areas routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network.

Example:

Switch#config terminal

Switch(config) #router ipv6 ospf

Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20

Switch(config-router) #area 1 virtual-link 10.10.11.50 instance-id 1

13.5.6 abr-type

Command: abr-type {cisco|ibm| standard}

no abr-type [cisco|ibm| standard]

Function: Configure an OSPF ABR type with this command. The "**no abr-type [cisco|ibm| standard]**" command restores the default.

Parameter: cisco, realize by cisco ABR; **ibm**, realize by ibm ABR; **shortcut**, specify a shortcut-ABR; **standard**, realize with standard（RFC2328）ABR.

Default: Cisco configured by default

Command Mode: OSPFv3 protocol mode

Usage Guide: For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host environment.

Example: Configure ABR as standard.

Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#abr-type standard

13.5.7 default-metric

Command: default-metric <*value*>

no default-metric

Function: The command set the default metric value of OSPF routing protocol; the "**no default-metric**" returns to the default state.

Parameter: <*value*>, metric value, ranging between 1~16777214.

Default: Built-in, metric value auto translating.

Command Mode: OSPF protocol mode

Usage Guide: When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.

Example:

Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#default-metric 100

13.5.8 debug ipv6 ospf events

Command: [no] debug ipv6 ospf events [abr|asbr|os|router|vlink]

Function: Open debugging switches showing OSPF events. The "**no debug ipv6 ospf events [abr|asbr|os|router|vlink]**" command closes this debugging switch.

Default: Closed.

Command Mode: Admin mode

Example:

Switch#debug ipv6 ospf events

1970/01/01 01:10:35 IMI: ROUTER[Process:(null)]: GC timer expire

13.5.9 debug ipv6 ospf ifsm

Command: [no] debug ipv6 ospf ifsm [status|events|timers]

Function: Open debugging switches showing the OSPF interface states; the "**[no] debug ospf ifsm [status|events|timers]**" command closes this debugging switches.

Default: Closed.

Command Mode: Admin mode

Example:

Switch#debug ipv6 ospf ifsm

1970/01/01 01:11:44 IMI: IFSM[Vlan1]: Hello timer expire

1970/01/01 01:11:44 IMI: IFSM[Vlan2]: Hello timer expire

13.5.10 debug ipv6 ospf lsa

Command: [no]debug ipv6 ospf lsa [generate|flooding|install|maxage|refresh]

Function: Open debugging switches showing showing link state announcements; the "**no debug ospf lsa [generate|flooding|install|maxage|refresh]**" closes the debugging switches.

Default: Closed.

Command Mode: Admin mode

13.5.11 debug ipv6 ospf nfsm

Command: [no] debug ipv6 ospf nfsm [status|events|timers]

Function: Open debugging switches showing showing OSPF neighbor state machine; the "**no debug ipv6 ospf nfsm [status|events|timers]**" command closes this debugging switch.

Default: Closed.

Command Mode: Admin mode

Switch#debug ipv6 ospf nfsm

1970/01/01 01:14:07 IMI: NFSM[192.168.2.3-000007d4]: LS update timer expire

1970/01/01 01:14:07 IMI: NFSM[192.168.2.1-000007d3]: LS update timer expire

1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (HelloReceived)

1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: nfsm_ignore called

1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (2-WayReceived)

13.5.12 debug ipv6 ospf nsm

Command: [no] debug ipv6 ospf nsm [interface|redistribute]

Function: Open debugging switches showing showing OSPF NSM, the "**no debug ipv6 ospf nsm [interface|redistribute]**" command closes this debugging switch.

Default: Closed.

Command Mode: Admin mode

13.5.13 debug ipv6 ospf packet

Command: [no] debug ipv6 ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | send]

Function: Open debugging switches showing OSPF packet messages; the "**no debug ipv6 ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | send]**" command closes this debugging switch.

Default: Closed.

Command Mode: Admin Mode.

13.5.14 debug ipv6 ospf redistribute message send

Command: debug ipv6 ospf redistribute message send

no debug ipv6 ospf redistribute message send

Function: To enable/disable debugging of sending command from IPv6 OSPF process redistributed to other IPv6 OSPF process routing.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch#debug ipv6 ospf redistribute message send

13.5.15 debug ipv6 ospf redistribute route receive

Command: debug ipv6 ospf redistribute route receive

no debug ipv6 ospf redistribute route receive

Function: To enable/disable debugging of received routing message from NSM for IPv6 OSPF process.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch# debug ipv6 ospf redistribute route receive

13.5.16 debug ipv6 ospf route

Command: [no] debug ipv6 ospf route [ase|ia|install|spf]

Function: Open debugging switches showing OSPF related routes; the "**[no]debug ipv6 ospf route [ase|ia|install|spf]**" command closes this debugging switch.

Default: Closed.

Command Mode: Admin mode

13.5.17 ipv6 ospf authentication-mode

Command: ipv6 ospf authentication-mode (null|(hmac-sha-256) key-id <0-65535> (0 WORD |7 WORD) (instance-id <0-255> |))

no ipv6 ospf authentication-mode

Function: Use RFC7166 authentication for OSPFv3 message specified interface; the "**no** ipv6 ospf ***<id>*** **authentication-mode**" command restores the default value.

Parameter: NULL: The interface is in unauthenticated mode.

(hmac-sha-256): Encryption method, currently only supports hmac-sha-256 method.

<0-65535>key-id value.

(0 WORD |7 WORD): The content of the authenticated key, if the key option is 0, specifies the plaintext key subsequently. If option 7, it will be specified as the ciphertext string encrypted with the plaintext key. The key length range is 1-128.

instance-id：The instance ID range is 0-255, with a default value of 0.

Default: Use areal authentication method.

Command Mode: Interface Configuration Mode.

Usage Guide: Use RFC7166 authentication for OSPFv3 message specified interface. Note that the authentication of this interface defaults to using the authentication mode of the area. If the area has configured authentication, but the interface does not require authentication, null needs to be configured. If the areais not configured with authentication, a null interface configuration is also considered as non authentication.

Example:

Switch#config terminal
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ipv6 ospf authentication-mode hmac-sha-256 key-id 100 0 asdfg

13.5.18 ipv6 ospf cost

Command: ipv6 ospf cost <*cost*> [instance-id <*id*>]
no ipv6 ospf <*cost*> [instance-id <*id*>]
Function: Specify the cost required in running OSPF protocol on the interface; the "**no ipv6 ospf cost [instance-id <*id*>]**" command restores the default value.
Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0
<cost > is the cost of OSPF protocol ranging between 1~65535.
Default: Default OSPF cost on the interface is 10.
Command Mode: Interface Configuration Mode.
Usage Guide: The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example:
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf cost 3

13.5.19 ipv6 ospf dead-interval

Command: ipv6 ospf dead-interval <*time* > [instance-id <*id*>]
no ipv6 ospf dead-interval [instance-id <*id*>]
Function: Specify the dead interval for neighboring layer 3 switch; the "**no ipv6 ospf dead-interval [instance-id <*id*>]**" command restores the default value.
Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0
<time > is the length of the adjacent layer 3 switch, in seconds, ranging between 1～65535
Default: The default dead interval is 40 seconds (normally 4 times of the hello-interval).
Command Mode: Interface Configuration Mode.
Usage Guide: If no HELLO data packet received after the **dead-interval** period then this layer 3 switch is considered inaccessible and invalid. This command modifies the dead interval value of neighboring layer 3 switch according to the actual link state. The set **dead-interval** value is written into the Hello packet and transmitted. To ensure the normal operation of the OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the **hello-interval** value. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example:
Switch#config terminal
Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf dead-interval 80

13.5.20 ipv6 ospf display route single-line

Command: [no] ipv6 ospf display route single-line

Function: show ipv6 ospf route change the display results of show ipv6 ospf route command. The "**no ipv6 ospf display route single-line**" restores to default display mode.

Default: Not configured

Command Mode: Global Mode

Usage Guide: The show ipv6 ospf route command displays the same route in several lines. This command will strict that one route will be displayed in one line.

Example:

Switch#config terminal

Switch(config)#ipv6 ospf display route single-line

13.5.21 ipv6 ospf hello-interval

Command: ipv6 ospf hello-interval <*time*> [instance-id <*id*>]

no ipv6 ospf hello-interval [instance-id <*id*>]

Function: Specify the hello-interval on the interface; the "**no ipv6 ospf hello-interval [instance-id <*id*>]**" restores the default value.

Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0

<time > is the length of the adjacent layer 3 switch, in seconds, ranging between 1～65535

Default: Default HELLO packet sending interval is 10 seconds.

Command Mode: Interface Configuration Mode.

Usage Guide: HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set **hello-interval** value will be written into the HELLO packet and transmitted. The less the **hello-interval** value is, the sooner the network topological structure is discovered as well larger the cost. The ensure the normal operation of OSPF protocol the **hello-interval** parameter between the layer 3 switches adjacent to the interface must be in accordance. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf hello-interval 20

Relevant Commands: ipv6 ospf dead-interval

13.5.22 ipv6 ospf priority

Command: ipv6 ospf priority <*priority*> [instance-id <*id*>]

no ipv6 ospf priority[instance-id *<id>*]

Function: Configure the priority when electing "Defined layer 3 switch" at the interface. The "**no ipv6 ospf [*<ip-address>*] priority**" command restores the default value.

Parameter: ***<id>*** is the interface instance ID, ranging between 0~255, and defaulted at 0

<priority> is the priority of which the valid value ranges between 0～255.

Default: The default priority when electing DR is 1.

Command Mode: Interface Configuration Mode.

Usage Guide: When two layer 3 switches connected to the same segments both want to be the "Defined layer 3 switch", the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be elected as "Defined layer 3 switch" or "Backup Defined layer 3 switch". The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure the priority of DR electing. Configure the interface vlan 1 to no election right, namely set the priority to 0.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf priority 0

13.5.23 ipv6 ospf retransmit-interval

Command: ipv6 ospf retransmit-interval *<time>* [instance-id *<id>*]

no ipv6 ospf retransmit-interval [instance-id *<id>*]

Function: Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The "**no ipv6 ospf retransmit-interval [instance-id *<id>*]**" command restores the default value.

Parameter: *<id>* is the interface instance ID, ranging between 0~255, defaulted at 0

<time> is the retransmit interval of link state announcements between the interface and adjacent layer 3 switches, shown in seconds and ranging between 1～65535.

Default: Default retransmit interval is 5 seconds.

Command Mode: Interface Configuration Mode.

Usage Guide: When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure the LSA retransmit interval of interface vlan 1 to 10 seconds.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf retransmit-interval 10

13.5.24 ipv6 ospf transmit-delay

Command: ipv6 ospf transmit-delay *<time>* [instance-id *<id>*]

no ipv6 ospf transmit-delay [instance-id *<id>*]

Function: Configure the LSA sending delay time on the interface. The "**no ipv6 ospf transmit-delay [instance-id *<id>*]**" command restores to the default.

Parameter: *<id>* is the instance ID ranging between 0~255 and defaulted at 0

<time> is the delay time of sending LSA on the interface, which is shown in seconds and ranged between 1～65535.

Default: The default delay time of send LSA on the interface is 1 second by default.

Command Mode: Interface Configuration Mode.

Usage Guide: The LSA ages by time in the layer 3 switches but not in the transmission process. So by increasing the **transmit-delay** before sending LSA so that it will be sent out. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Set the interface vlan 1 LSA sending delay to 3 seconds.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf transmit-delay 3

13.5.25 ipv6 router ospf

Command: [no] ipv6 router ospf {area *<area-id>* [instance-id *<instance-id>*]| tag *<tag>*[instance-id *<instance-id>*]}| tag *<tag>* area *<area-id>* [instance-id *<instance-id>*]}

Function: Enable ospf route on the interface; the "**no ipv6 router ospf {area *<area-id>* [instance-id *<instance-id>*]| tag *<tag>*[instance-id *<instance-id>*]}| tag *<tag>* area *<area-id>* [instance-id *<instance-id>*]}**" command cancels this configuration.

Parameter: *<area-id>* is an area ID which could be shown in digits ranging between 0～4294967295, or an IPv4 address

<instance-id> is the interface instance ID ranging between 0~255 and defaulted at 0.

<tag> ospfv3 process identifier

Default: Not configured

Command Mode: Interface Configuration Mode.

Usage Guide: To enable this command on the interface, the area id must be configured. The instance ID and instance tag are optional. The ospfv3 process allows one routing instance for each instance ID. The route can be enabled on a interface with a instance ID. If the instance IDs are different, several OSPF process can be run on one interface. However different OSPF process should not use the same instance ID The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 router ospf area 1 tag IPI instance-id 1

13.5.26 max-concurrent-dd

Command: max-concurrent-dd *<value>*

no max-concurrent-dd

Function: Configure with this command the current dd max concurrent number in the OSPF processing. The "**no max-concurrent-dd**" command restores the default.

Parameter: <*value*> ranges between ***<1-65535>,*** the capacity of concurrent dd data packet processing.

Default: No default configuration. No dd concurrent limit.

Command Mode: OSPFv3 protocol mode

Usage Guide: Specify the current dd max concurrent number in the OSPF processing.

Example: Set the max concurrent dd to 20.

Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#max-concurrent-dd 20

13.5.27 passive-interface

Command: [no] passive-interface {*<ifname>*|vlan *<vlan-id>*}

Function: Configure that the hello group not sent on specific interfaces. The "**no passive-interface{*<ifname>*|vlan *<vlan-id>*}**" command cancels this function.

Parameter: *<ifname>* is the specific name of interface.

Default: Not configured

Command Mode: OSPFv3 protocol mode

Example: Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#passive-interface vlan1

13.5.28 redistribute

Command: [no] redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>]

Function: Introduce route learnt from other routing protocols into OSPFv3.

Parameter: kernel Introduct from kernel route

connected Introduce from direct route

static Introduce from static route

rip Introduce from the RIP route

isis Introduce from ISIS route

bgp Introduce from BGP route

metric <*value*> is the introduced metric value, ranging between 0-16777214

metric-type {1|2} is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default

route-map <*word*> targets to the probe of the route map for introducing route

Command Mode: OSPFv3 protocol mode

Usage Guide: Learn and introduce other routing protocol into OSPFv3 area to generate AS-external_LSAs.

Example: Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#redistribute bgp metric 12 metric-type 1

13.5.29 redistribute ospf

Command: redistribute ospf [<*process-tag*>] [metric<*value*>] [metric-type {1|2}] [route-map<*word*>]

no redistribute ospf [<*process-tag*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>]

Function: To redistribute routing information form process-tag to this command. The no form of command cancels the redistribution of process-tag routing to this process. When input the optional parameters of metric, metric type and routermap, then restores default configuration.

Parameter: process-tag is the process ID of IPv6 OSPF process, NULL by default.

metric <*value*> is the metric for redistributed routing, range between 0 to 16777214.

metric-type {1|2} is the metric type for redistributed routing, only can be 1 or 2, and 2 by default.

route-map <*word*> is the pointer to the introduced routing map.

Default: Not redistributed any OSPFfv3 routing by default.

Command Mode: Router IPv6 OSPF Configuration Mode.

Usage Guide: When process-id is not input, that means OSPFv3 routing will be redistributed by default (Process-tag is NULL). The no form of command input the optional parameters of metric, metric-type and routermap, then restores default configuration. When not input any optional parameters that mean to delete the router of redistributed process.

Example:

Switch(config)#router ipv6 ospf

Switch(config-router)#redistribute ospf

13.5.30 router-id

Command: router-id <*router-id*>

no router-id

Function: Configure router ID for ospfv3 process. The "**no router-id**"restores ID to 0.0.0.0.

Parameter: <*router-id*>> is the router ID shown in IPv4 format.

Default: 0.0.0.0 by default.

Usage Guide: If the router-id is 0.0.0.0, the ospfv3 process can not be normally enabled. It is required to configure a router-id for ospfv3.

Command Mode: OSPFv3 protocol mode

Example: Switch#config terminal

```
Switch(config)#router ipv6 ospf
Switch(config-router)#router-id 192.168.2.1
```

13.5.31 router ipv6 ospf

Command: [no] router ipv6 ospf [*<tag>*]

Function: This command initializes the ospfv3 routing process and enters ospfv3 mode for configuring the ospfv3 routing process. The "**no router ipv6 ospf [*<tag>*]**" command stops relevant process.

Parameter: ***<tag>*** ospfv3 is the process mark which could be random strings made up of characters and digits

Command Mode: Global mode

Usage Guide: To let he ospfv3 routing process work properly, this command must be configured and ospfv3 must at least be enabled on one interface. When the tag configured by the ipv6 router ospf area command under interface mode matches with the tag of ospf process, the ospfv3 process is enabled on this interface.

Example: Switch#config terminal

```
Switch(config)#router ipv6 ospf IPI
```

13.5.32 show ipv6 ospf

Command: show ipv6 ospf [*<tag>*]

Function: Display OSPF global and area messages.

Parameter: ***<tag>*** is the process tag which is a character string.

Default: Not displayed.

Command Mode: All modes

Example:

```
Switch#show ipv6 ospf
Routing Process "OSPFv3 (*null*)" with ID 192.168.2.2
  SPF schedule delay 5 secs, Hold time between SPFs 10 secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
  Number of external LSA 0. Checksum Sum 0x0000
  Number of AS-Scoped Unknownnnnn LSA 0
  Number of LSA originated 6
  Number of LSA received 14
  Number of areas in this router is 1
      Area BACKBONE(0)
          Number of interfaces in this area is 2
          SPF algorithm executed 6 times
          Number of LSA 8.    Checksum Sum 0x43D52
          Number of Unknownnnnn LSA 0
```

13.5.33 show ipv6 ospf database

Command: show ipv6 ospf [<*tag*>] database
[router [adv-router <*advertiser_router*>]
|network [adv-router <*advertiser_router*>]
| intra-prefix [adv-router <*advertiser_router*>]
| link [adv-router <*advertiser_router*>]
| external [adv-router <*advertiser_router*>]
| inter-prefix [adv-router <*advertiser_router*>]
| inter-router [adv-router <*advertiser_router*>]]

Function: Display the OSPF link state data base message.

Parameter: ***<tag>*** is the process tag which is a character string.

<advertiser_router> is the ID of Advertising router, shown in IPv4 address format

Default: Not displayed

Command Mode: All modes

Usage Guide: According to the output messages of this command, we can view the OSPF link state database messages.

Example:

Use show ipv6 ospf database command will be able to show LSA messages of the OSPF routing protocol

For Example, the displayed messages are:

OSPFv3 Router with ID (192.168.2.2) (Process *null*)

Link-LSA (Interface Vlan1)

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix
0.0.7.211	192.168.2.2	1409	0x80000001	0x6dda	1
0.0.7.212	192.168.2.3	1357	0x80000001	0x248e	1

Link-LSA (Interface Vlan2)

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix
0.0.7.211	192.168.2.1	1450	0x80000001	0xa565	1
0.0.7.212	192.168.2.2	1399	0x80000001	0x4305	1

Router-LSA (Area 0.0.0.0)

Link State ID	ADV Router	Age	Seq#	CkSum	Link
0.0.0.0	192.168.2.1	1390	0x80000006	0x9fe2	1
0.0.0.0	192.168.2.2	1354	0x80000007	0x4af5	2
0.0.0.0	192.168.2.3	1308	0x80000004	0xbbc4	1

Network-LSA (Area 0.0.0.0)

Link State ID	ADV Router	Age	Seq#	CkSum
0.0.7.211	192.168.2.1	1390	0x80000001	0x897e
0.0.7.211	192.168.2.2	1354	0x80000001	0x9b69

Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix	Reference
0.0.0.1	192.168.2.1	1389	0x80000005	0x7e2e	1	Router-LSA
0.0.0.2	192.168.2.1	1389	0x80000001	0x22cb	1	Network-LSA
0.0.0.1	192.168.2.3	1306	0x80000002	0xd0d7	1	Router-LSA

Displayed information's	Explanations
Link-LSA (Interface Vlan1)	Link LSA messages of interface Vlan1
Router-LSA (Area 0.0.0.0)	Router LSA messages in Area 0
Network-LSA (Area 0.0.0.0)	Network LSA in Area 0
Intra-Area-Prefix-LSA (Area 0.0.0.0)	Intra-domain Prefix LSA in Area 0

13.5.34 show ipv6 ospf interface

Command: show ipv6 ospf interface *<ifname>*|vlan *<vlan-id>*

Function: Display the OSPF interface messages.

Parameter: *<ifname>* is the name of the interface.

Default: Not displayed

Command Mode: All modes

Example:

```
Switch#show ipv6 ospf interface
Loopback is up, line protocol is up
  OSPFv3 not enabled on this interface
Vlan1 is up, line protocol is up
  Interface ID 2003
  IPv6 Prefixes
    fe80::203:fff:fe01:257c/64 (Link-Local Address)
    2001:1:1::1/64
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 192.168.2.2
      Interface Address fe80::203:fff:fe01:257c
    Backup Designated Router (ID) 192.168.2.3
      Interface Address fe80::203:fff:fe01:d28
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:10
    Neighbor Count is 1, Adjacent neighbor count is 1
Vlan2 is up, line protocol is up
  Interface ID 2004
  IPv6 Prefixes
    fe80::203:fff:fe01:257c/64 (Link-Local Address)
    2000:1:1::1/64
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State Backup, Priority 1
    Designated Router (ID) 192.168.2.1
      Interface Address fe80::203:fff:fe01:429e
    Backup Designated Router (ID) 192.168.2.2
```

Interface Address fe80::203:fff:fe01:257c
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:10
Neighbor Count is 1, Adjacent neighbor count is 1

Displayed information	Explanations
Vlan1 is up, line protocol is up	Let the interface up both logically and physically
IPv6 Prefixes fe80::203:fff:fe01:257c/64 (Link-Local Address) 2001:1:1::1/64	IPv6 address of the interface and the length of the prefix
OSPFv3 Process (*null*)	Ospfv3 process the interface belongs
Area 0.0.0.1	Area the interface belongs
Instance ID 0	Instance ID is 0
Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10	Process ID; Router ID; Network Type; Cost
Transmit Delay is 1 sec, State DR, Priority 1	LAS transmission delay on the interface; state; electing the priority of the layer 3 switch.
Designated Router (ID) 192.168.2.2 Interface Address fe80::203:fff:fe01:257c	Specifying layer 3 switch
Backup Designated Router (ID) 192.168.2.3 Interface Address fe80::203:fff:fe01:d28	Back up designated layer 3 switch
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:10	OSPF protocol timer; including hello packet, poll interval packets, router dead, router retransmission.
Neighbor Count is 1, Adjacent neighbor count is 1	Numbers of the adjacent layer 3 switch; number of the layer 3 switches established with neighbor relation

13.5.35 show ipv6 ospf neighbor

Command: show ipv6 ospf [<*tag*>] neighbor [<*neighbor_id*> | <ifname> detail | detail]

Function: Show OSPF adjacent point messages.

Parameter: ***<tag>*** is process tag, which is a character string

<neighbor_id> is the neighbor ID shown in IPv4 address format

detail: Show neighbor details

<ifname> name of the interface

Default: Not displayed

Command Mode: All modes

Usage Guide: OSPF neighbor state can be checked by viewing the output of this command.

Example:

Switch#show ipv6 ospf neighbor
OSPFv3 Process (*null*)

Neighbor ID	Pri	State	Dead Time	Interface	Instance ID	
192.168.2.3	1	Full/Backup	00:00:29	Vlan1	0	
192.168.2.1	1	Full/DR	00:00:38	Vlan2	0	Vlan1

Displayed information	Explanation
Neighbor ID	Neighbor ID
Instance ID	Instance ID
Address	IP address of neighboring layer 3 switch
Interface	Interface the neighbor belongs
State	Neighbor relationship state
Pri	Priority

13.5.36 show ipv6 ospf route

Command: show ipv6 ospf [<*tag*>] route

Function: Show the OSPF route table messages.

Parameter: ***<tag>*** is the processes tag, which is a character string.

Default: Not displayed

Command Mode: All modes

Example:

```
Switch#show ipv6 ospf route
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
O  2000:1:1::/64                                  10
     directly connected, Vlan2
O  2001:1:1::/64                                  10
     directly connected, Vlan1
O  3000:1:1::/64                                  20
     via fe80::203:fff:fe01:429e, Vlan2
O  3003:1:1::/64                                  20
     via fe80::203:fff:fe01:d28, Vlan1
```

13.5.37 show ipv6 ospf redistribute

Command: show ip ospf v6 [<*process-tag*>] redistribute

Function: To display the routing message redistributed from external process of OSPF.

Parameter: IPv6 OSPF is the tag ID, to display all routing messages redistributed from external process of IPv6 OSPF if there is no parameter.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: None.

Example:

Switch#show ipv6 ospf redistribute

ospf process abc redistribute information：

ospf process def

bgp

ospf process def redistribute information：

ospf process abc

Switch#show ipv6 ospf abc redistribute

ospf process abc redistribute information：

ospf process def

bgp

13.5.38 show ipv6 ospf topology

Command: show ipv6 ospf [*<tag>*] topology [area *<area-id>*]

Function: Show messages of OSPF topology.

Parameter: ***<tag>*** is the processes tag, which is a character string.

<area-id> is an area ID which could be shown in digits ranging between 0～4294967295, or an IPv4 address.

Default: Not displayed.

Command Mode: All modes

Example:

Switch#show ipv6 ospf topology

OSPFv3 Process (*null*)

OSPFv3 paths to Area (0.0.0.0) routers

Router ID	Bits	Metric	Next-Hop	Interface
192.168.2.1		10	192.168.2.1	Vlan2
192.168.2.2		--		
192.168.2.3		10	192.168.2.3	Vlan1

13.5.39 show ipv6 ospf virtual-links

Command: show ipv6 ospf [*<tag>*] virtual-links

Function: Show OSPF virtual link messages.

Parameter: ***<tag>*** is the processes tag, which is a character string.

Default: Not displayed.

Command Mode: All modes

Example:

Switch#show ipv6 ospf virtual-links

Virtual Link VLINK1 to router 5.6.7.8 is up

Transit area 0.0.0.1 via interface Vlan1, 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

13.5.40 show ipv6 route process-detail

Command: show ipv6 route [database] process-detail
Function: Display the IP routing table with specific process ID or Tag.
Parameters: The parameter of database means displaying all the routers, no parameter means only displaying effective routers.
Command Mode: Admin mode and configure mode.
Usage Guide: None.
Example:
Switch#show ipv6 route database process-detail
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP
> - selected route, * - FIB route, p - stale info
Timers: Uptime

C*> ::1/128 via ::, Loopback, 00:29:53
O 2001::/64 [110/10] via ::, Vlan1, 00:01:07 ,process aaa
C*> 2001::/64 via ::, Vlan1, 00:02:54
O*> 2006::/64 [110/10] via ::, Vlan1, 00:01:07, process aaa
O*> 2008::/64 [110/20] via fe80::203:fff:fe01:2542, Vlan1, 00:00:54, process bbb

13.5.41 timers spf

Command: timers spf <*spf-delay*> <*spf-holdtime*>
no timers spf
Function: Adjust route calculation timer value. The "**no timers spf**" restores the relevant value to default.
Parameter: ***<spf-delay>*** 5 seconds by default
<spf-holdtime> 10 seconds by default
Command Mode: OSPFv3 protocol mode
Usage Guide: In this command the delay time between receiving topology change and SPF calculation, and further configured the hold time between two discontinuous SPF calculations.
Example: Switch#config terminal
Switch(config)#router ipv6 ospf
Switch(config-router)#timers spf 5 10

13.6 MBGP4+

13.6.1 debug ipv6 bgp redistribute message send

Command: debug ipv6 bgp redistribute message send

no debug ipv6 bgp redistribute message send

Function: To enable debugging switch of sending messages for redistribution of routing information from external process such as OSPFv3 and others to MBGP4+. The no command will disable the debugging switch.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch# debug ipv6 bgp redistribute message send

13.6.2 debug ipv6 bgp redistribute route receive

Command: debug ipv6 bgp redistribute route receive

no debug ipv6 bgp redistribute route receive

Function: To enable debugging switch of received messages from NSM for MBGP4+. The no form of this command will disable debugging switch of received messages from NSM for MBGP4+.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch# debug ipv6 bgp redistribute route receive

Switch# no debug ipv6 bgp redistribute route receive

13.6.3 redistribute ospf (MBGP4+)

Command: redistribute ospf [<*process-tag*>] [route-map<*word*>]

no redistribute ospf [<*process-tag*>]

Function: To redistribute routing information form OSPFv3 to MBGP4+. The no form of this command will remove the configuration.

Parameters: process-id is the process character string of the OSPFv3, the length is less than 15. If no process id is specified, the default process will be used.

route-map<*word*> is the pointer to the introduced routing map.

Default: Not redistributed by default.
Command Mode: BGP IPv6 Configuration Mode.
Usage Guide: None.
Example: To redistribute routing information from OSPFv3 process with the tag as ABC to MBGP4+ (as number as 1).
Switch (config)#router bgp 1
Switch (config-router)#address-family ipv6 unicast
Switch (config-router-af)#redistribute ospf abc

13.6.4 show ipv6 bgp redistribute

Command: show ipv6 bgp redistribute
Function: Show the configuration information of redistribution other out routing to MBGP4+.
Parameter: None.
Default: Not shown by default.
Command Mode: Admin Mode and Configuration Mode.
Usage Guide: None.
Example:
Switch#show ipv6 bgp redistribute

13.7 Black Hole Routing

13.7.1 ipv6 route null0

Command: ipv6 route <*ipv6-prefix*|*prefix-length*> null0 [<*precedence*>]
no ipv6 route <*ipv6-prefix*|*prefix-length*> null0
Function: To configure routing destined to the specified network to the interface of null0.
Parameters: <*ipv6-prefix*> is the IPv6 network static route addressof the destination, in dotted decimal format. **<*prefix-length*>** is the IPv6 address of the destination and the length of the prefix. **null0** is the output interface for the black hole routing. **<*precedence*>** is the route weight, ranging between 1 to 255 and 1 by default.
Default: None.
Command Mode: Global Configuration Mode.
Usage Guide: When configuring IPv6 Black Hole Routing, it is much like configuring normal static routing, but using null0 as the output interface.
Example: To configure a route to 2001:2:3:4::/64 as a Black Hole Routing.
Switch(config)#ipv6 route 2001:2:3:4::/64 null0

13.8 IPv6 Multicast Protocol

13.8.1 Multicast

13.8.1.1 show ipv6 mroute

Command: show ipv6 mroute [<GroupAddr> [<SourceAddr>]]

Function: show IPv6 software multicast route table.

Parameter: GroupAddr: show the multicast entries relative to this Group address.

SourceAddr: show the multicast route entries relative to this source address.

Default: None

Command Mode: Admin mode and global mode

Usage Guide: None.

Example: show all entries of IPv6 multicast route table

Switch(config)# show ipv6 mroute

Name: Loopback, Index: 2002, State:49

Name: Vlan1, Index: 2006, State:1043

Name: Vlan11, Index: 2007, State:1043

Name: Vlan12, Index: 2008, State:1043

Name: Tunnel1, Index: 2009, State:d1

Name: Tunnel2, Index: 0, State:0

Name: pim6reg, Index: 2010, State:c1

Name: pimreg, Index: 2011, State:c1

The total matched ip6mr active mfc entries is 1, unresolved ip6mr entries is 1

Group	Origin	Iif	Wrong	Oif:TTL
ff2f::1	2014:1:2:3::2	Tunnel1	0	2008:1
ff3f::1	2012:1:2:3::2	NULL	4	0:0

Displayed information	Explanation
Name	the name of interface
Index	the index number of interface
State	the state of interface
The total matched ipmr active mfc entries	The total matched active IP multicast route mfc （multicast forwarding cache） entries
unresolved ipmr entries	unresolved ip multicast route entries
Group	the destination address of the entries
Origin	the source address of the entries
Iif	ingress interface of the entries
Wrong	packets received from the wrong interface

13.8.2 PIM-DM6

Explain: Part SHOW and DEBUG commands is same to PIM-SM, please reference the PIM-SM command.

13.8.2.1 debug ipv6 pim timer sat

Command: debug ipv6 pim timer sat

no debug ipv6 pim timer sat

Function: Enable debug switch of PIM-DM source activity timer information in detail; the "**no debug ipv6 pim timer sat**" command disenables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example:

Switch # debug ipv6 pim timer sat

Remark: Other debug switches in PIM-DM are common in PIM-SM.

13.8.2.2 debug ipv6 pim timer srt

Command: debug ipv6 pim timer srt

no debug ipv6 pim timer srt

Function: Enable debug switch of PIM-DM state-refresh timer information in detail; the "**no debug ipv6 pim timer srt**" command disenables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the switch, and display PIM-DM state-refresh timer information in detail

Example:

Switch # debug ipv6 pim timer srt

Remark: Other debug switches in PIM-DM are common in PIM-SM.

13.8.2.3 ipv6 mroute

Command: ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> <*ifname*> <*.ifname*>

no ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> [<*ifname*> <*.ifname*>]

Function: To configure static multicast entry. This no command deletes some static multicast entries or some egress interfaces.

Parameter: ***<X:X::X:X> <X:X::X:X>*** are the source address and group address of multicast.

<ifname> <.ifname>, the first one is ingress interface, follow is egress interface.

Command Mode: Global Mode.

Default: None.

Usage Guide: The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified egress interface will be removed.

Example:

Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30

13.8.2.4 ipv6 pim bsr-border

Command: ipv6 pim bsr-border

no ipv6 pim bsr-border

Function: To configure or delete PIM6 BSR-BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

Switch(Config-if-Vlan1)#ipv6 pim bsr-border

13.8.2.5 ipv6 pim dense-mode

Command: ipv6 pim dense-mode

no ipv6 pim dense-mode

Function: Enable PIM-DM protocol on interface; the "**no ipv6 pim dense-mode**" command disenables PIM-DM protocol on interface.

Parameter: None

Default: Disable PIM-DM protocol

Command Mode: Interface Configure Mode

Usage Guide: The command will be taken effect, executing ipv6 multicast-routing in Global Mode. Don't support multicast protocol mutual operation, namely can't synchronously enable dense mode and sparse mode in one switch. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Enable PIM-DM protocol on interface vlan1.

Switch (config)#ipv6 pim multicast-routing

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 pim dense-mode

13.8.2.6 ipv6 pim dr-priority

Command: ipv6 pim dr-priority <*priority*>

no ipv6 pim dr-priority

Function: Configure, cancel and change priority value of interface DR. The same net segment border nodes vote specified router DR in this net segment through hello messages, the "no ipv6 pim dr-priority" restores default value.

Parameter: < *priority*> priority, value range from 0 to 4294967294

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Value range is from 0 to 4294967294, the bigger value, the more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Switch (config)# interface vlan 1

Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

13.8.2.7 ipv6 pim exclude-genid

Command: ipv6 pim exclude-genid

no ipv6 pim exclude-genid

Function: The command make Hello message transmitted by PIM-SM exclude Genid option, the "**no ipv6 pim exclude-genid**" restores default value.

Parameter: None

Default: Hello message includes Genid option

Command Mode: Interface Configuration Mode

Usage Guide: The command is used to interactive with old Cisco IOS Version.The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure hello messages transmitted by switch to exclude Genid option.

Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

13.8.2.8 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <*value*>

no ipv6 pim hello-holdtime

Function: Configure and cancel Holdtime item value in Hello message, the value describes neighbor overtime. If it goes over the time and does not receive hello message of the neighbor, the register of the neighbor will be delete.

Parameter: *<value>* is configure time of holdtime.

Default: Define 3.5 times of Hello_interval, and default hello_interval as 30s, so default value of hello_holdtime is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If no setting, hello time will default current 3.5 times of Hello_interval. If setting hello time is less than current hello_interval, this setting will be declined. When updating hello_interval every time, hello_holdtime will be also update based on these rules below: if

hello_holdtime does not be configured, or if hello_holdtime configured is less than current hello_interval, hello_holdtime will be modified to 3.5 times Hello_interval, otherwise, keeps configured value. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure hello holdtime setting on interface vlan1 to 10.

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10

13.8.2.9 ipv6 pim hello-interval

Command: ipv6 pim hello-interval < *interval*>

no ipv6 pim hello-interval

Function: Configure interface PIM-DM hello message interval; the "**no ipv6 pim hello-interval**" command restores default value.

Parameter: < *interval*> is interval of periodically transmitted PIM-DM hello message, value range from 1s to 18724s.

Default: Default interval of periodically transmitted PIM-DM hello message as 30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello message makes PIM-DM switch mutual location, and ensures neighbor ship. PIM-DM switch announces existence itself by periodically transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure PIM-DM hello interval on interface vlan1

Switch (config)#interface vlan1

Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20

13.8.2.10 ipv6 pim multicast-routing

Command: ipv6 pim multicast-routing

no ipv6 pim multicast-routing

Function: Globally enable PIM-DM protocol; the "**no ipv6 pim multicast-routing**" command disenables PIM-DM protocol.

Parameter: None

Default: Disable PIM-DM protocol

Command Mode: Global Mode

Usage Guide: Ipv6 pim can enable only after executing this command.

Example: Globally enable PIM-DM protocol

Switch (config)#ipv6 pim multicast-routing

13.8.2.11 ipv6 pim neighbor-filter

Command: ipv6 pim neighbor-filter <a*cess-list-name*>

no ipv6 pim neighbor-filter <a*cess-list-name*>

Function: Configure neighbor access-list. If filtered by list and connected the neighbor, the connection immediately was broken. If no connection, the connection can be established.

Parameter: ***<access-list-name>*** is an applied access-list name

Default: No neighbor filter configuration

Command Mode: Interface Configuration Mode

Usage Guide: If it is not necessary for partner to establish neighbor ship, the command can filter pim message of partner. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure access-list of pim neighbor on interface vlan1

Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01:facc

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#permit any

13.8.2.12 ipv6 pim scope-border

Command: ipv6 pim scope-border [<*500-599*>|<*acl_name*>]

no ipv6 pim scope-border

Function: To configure or delete management border of PIM6.

Parameters: <*500-599*> is the ACL number for the management border.

<acl_name> is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the management border and the ACL for the IPV6 PIM. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

Switch(Config-if-Vlan2)#ipv6 pim scope-border 503

13.8.2.13 ipv6 pim state-refresh origination-interval

Command: ipv6 pim state-refresh origination-interval <interval>

no ipv6 pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message on interface. The “no ipv6 pim state-refresh origination-interval” command restores default value.

Parameter: <*interval*> message transmission interval value is from 4s to 100s.

Default: 60s

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list ltems of all the downstream routers. The command can modify origination interval

of state-refresh messages. Usually do not modify relevant timer interval. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure transmission interval of state-refresh message on interface vlan1 to 90s.

Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval 90

13.8.2.14 show ipv6 pim interface

Command: show ipv6 pim interface [detail]

Function: Display PIM interface information.

Parameter: None

Default: None

Command Mode: Any Mode

Example:

Switch#show ipv6 pim interface

Interface VIFindex Ver/ Nbr DR

Mode Count Prior

Vlan2 0 v2/S 0 1

Address : fe80::203:fff:fee3:1244

Global Address: 2000:1:111::100

DR : this system

Vlan3 2 v2/S 0 1

Address : fe80::203:fff:fee3:1244

Global Address: 2000:10:1:13::1

DR : this system

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

13.8.2.15 show ipv6 pim mroute dense-mode

Command: show ipv6 pim mroute dense-mode [group <*X:X::X:X*>] [source <*X:X::X:X*>]

Function: Display PIM-DM message forwarding items.

Parameter: group <X:X::X:X>: displays forwarding items relevant to this multicast address

Source < X:X::X:X >: displays forwarding items relevant to this source.

Default: Do not display

Command Mode: Admin Mode

Usage Guide: The command shows PIM-DM multicast forwarding items, namely forwarding items of forward multicast packet in system FIB table.

Example: Display all of PIM-DM message forwarding items.

```
Switch(config)#show ipv6 pim mroute dense-mode
IP Multicast Routing Table

(*,G) Entries: 1
(S,G) Entries: 1

(*, ff1e::15)
  Local         ..l.....................

(2000:10:1:12::11, ff1e::15)
RPF nbr: ::
RPF idx: Vlan12
Upstream State: FORWARDING
Origin State: ORIGINATOR
  Local         .....................
  Pruned        .....................
  Asserted      .....................
  Outgoing      ..o.....................

Switch#
```

Displayed Information	Explanations
(*, ff1e::15)	(*,G) Forwaridng item
(2000:10:1:12::11, ff1e::15)	(S,G) Forwarding item
RPF nbr	Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop.
RPF idx	Interface located in RPF neighbor
Upstream State	Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream response, forwarding upstream data)
Origin State	The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)
Local	Join Local position joins interface, the interface receives IGMP Join
Pruned	PIM prunes interface, the interface receives Prune messages
Asserted	Asserted state

Outgoing	Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

13.8.2.16 show ipv6 pim neighbor

Command: show ipv6 pim neighbor [detail|]
Function: Display router neighbors.
Parameter: None
Default: None
Command Mode: Admin and configuration Mode
Usage Guide: Display multicast router neighbors maintained by the PIM.
Example:

```
Switch(config)#show ipv6 pim neighbor
Neighbor                    Interface          Uptime/Expires     Ver    DR
Address                                                                  Priority/Mode
Fe80::203:fff:fee3:1244     Vlan1              00:00:10/00:01:35  v2     1 /DR
fe80::20e:cff:fe01:facc     Vlan1              00:00:13/00:01:32  v2     1 /
```

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DR

13.8.2.17 show ipv6 pim nexthop

Command: show ipv6 pim nexthop
Function: Display the PIM buffered nexthop router in the unicast route table.
Parameter: None
Default: None
Command Mode: Admin and configuration Mode
Usage Guide: Display the PIM buffered nexthop router information.
Example:

```
Switch#show ipv6 pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable          ….
Destination          Type   Nexthop  Nexthop    Nexthop   Nexthop  Metric  Pref   Refcnt
                            Num      Addr       Ifindex   Name
```

2000:1:111::11 ..S. 1 2004 0 0 2
2000:1:111::100 .RS. 1 2004 0 0 2

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

13.8.3 PIM-SM6

13.8.3.1 clear ipv6 pim bsr rp-set

Command: clear ipv6 pim bsr rp-set *

Function: Clear all RP.

Parameters: None.

Command Mode: Admin Configuration Mode

Usage Guide: Clear all RP rapidly.

Example: Clear all RP.

Switch# clear ipv6 pim bsr rp-set *

Relative Command: show ipv6 pim bsr-router

13.8.3.2 debug ipv6 pim events

Command: debug ipv6 pim events

no debug ipv6 pim events

Function: Enable or Disable pim events debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable "pim events debug" switch and display events information about pim operation.

Example: Switch# debug ipv6 pim events

13.8.3.3 debug ipv6 pim mfc

Command: debug ipv6 pim mfc（in|out|）

no debug ipv6 pim mfc（in|out|）

Function: Enable or Disable pim mfc debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable pim mfc debug switch and display generated and transmitted multicast id's information.

Example: Switch# debug ipv6 pim mfc in

13.8.3.4 debug ipv6 pim mib

Command: debug ipv6 pim mib

no ipv6 debug pim mib

Function: Enable or Disable PIM MIB debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM MIB information by PIM MIB debug switch. It's not available now and it's for the future extension.

Example: Switch# debug ipv6 pim mib

13.8.3.5 debug ipv6 pim nexthop

Command: debug ipv6 pim nexthop

no debug ipv6 pim nexthop

Function: Enable or Disable pim nexthop debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM NEXTHOP changing information by the pim nexthop switch.

Example: Switch# debug ipv6 pim nexthop

13.8.3.6 debug ipv6 pim nsm

Command: debug ipv6 pim nsm

no debug ipv6 pim nsm

Function: Enable or Disable pim debug switch communicating with Network Services.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the communicating information between PIM and Network Services by this switch.

Example: Switch# debug ipv6 pim nsm

13.8.3.7 debug ipv6 pim packet

Command: debug ipv6 pim packet [in|out|]

no debug ipv6 pim packet [in|out|]

Function: Enable or Disable PIM debug switch.

Parameter: in display only received PIM packets

out display only transmitted PIM packets

none display both

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the received and transmitted PIM packets by this switch.

Example: Switch# debug ipv6 pim packet in

13.8.3.8 debug ipv6 pim state

Command: debug ipv6 pim state

no debug ipv6 pim state

Function: Enable or Disable PIM debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the changing information about PIM state by this switch.

Example: Switch# debug ipv6 pim state

13.8.3.9 debug ipv6 pim timer

Command: debug ipv6 pim timer

debug ipv6 pim timer assert

debug ipv6 pim timer assert at

debug ipv6 pim timer bsr bst

debug ipv6 pim timer bsr crp

debug ipv6 pim timer bsr

debug ipv6 pim timer hello ht

debug ipv6 pim timer hello nlt

debug ipv6 pim timer hello tht

debug ipv6 pim timer hello

debug ipv6 pim timer joinprune et

debug ipv6 pim timer joinprune grt

debug ipv6 pim timer joinprune jt

debug ipv6 pim timer joinprune kat
debug ipv6 pim timer joinprune ot
debug ipv6 pim timer joinprune plt
debug ipv6 pim timer joinprune ppt
debug ipv6 pim timer joinprune pt
debug ipv6 pim timer joinprune
debug ipv6 pim timer register rst
debug ipv6 pim timer register
no debug ipv6 pim timer
no debug ipv6 pim timer assert
no debug ipv6 pim timer assert at
no debug ipv6 pim timer bsr bst
no debug ipv6 pim timer bsr crp
no debug ipv6 pim timer bsr
no debug ipv6 pim timer hello ht
no debug ipv6 pim timer hello nlt
no debug ipv6 pim timer hello tht
no debug ipv6 pim timer hello
no debug ipv6 pim timer joinprune et
no debug ipv6 pim timer joinprune grt
no debug ipv6 pim timer joinprune jt
no debug ipv6 pim timer joinprune kat
no debug ipv6 pim timer joinprune ot
no debug ipv6 pim timer joinprune plt
no debug ipv6 pim timer joinprune ppt
no debug ipv6 pim timer joinprune pt
no debug ipv6 pim timer joinprune
no debug ipv6 pim timer register rst
no debug ipv6 pim timer register
no debug ipv6 pim timer

Function: Enable or Disable each PIM timer.
Parameter: None
Default: Disabled
Command Mode: Admin Mode.
Usage Guide: Enable the specified timer's debug information.
Example: Switch# debug ipv6 pim timer assert

13.8.3.10 ipv6 mroute

Command: ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> <*ifname*> <.*ifname*>
no ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> [<*ifname*> <.*ifname*>]

Function: To configure static multicast entry. This no command deletes some static multicast entries or some egress interfaces.

Parameter: ***<X:X::X:X> <X:X::X:X>*** are the source address and group address of multicast.
<ifname> ***<.ifname>***, the first one is ingress interface, follow is egress interface.
Command Mode: Global Mode.
Default: None.
Usage Guide: The ***<ifname>*** should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified egress interface will be removed.
Example:
Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30

13.8.3.11 ipv6 multicast unresolved-cache aging-time

Command: ipv6 multicast unresolved-cache aging-time <value>
no ipv6 multicast unresolved-cache aging-time
Function: Configure the cache time of kernel multicast route, the no command restores the default value.
Parameter: < value> is the configured cache time, ranging between 1 and 20s.
Default: 20s.
Command Mode: Global Configuration Mode.
Usage Guide: Configure the cache time of multicast route entry in kernel.
Example:
Switch(config)# ipv6 multicast unresolved-cache aging-time 18

13.8.3.12 ipv6 pim accept-register

Command: ipv6 pim accept-register list <a*cess-list-name*>
no ipv6 pim accept-register
Function: Filter the specified multicast group.
Parameter: <a*cess-list-name*> is the applying access-list name
Default: Permit the multicast registers from any sources to any groups
Command Mode: Global Mode
Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets. The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY, PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets. Unlike other access-list, when the access-list is configured, the default value is PERMIT.
Example: Configure the filtered register message's rule to myfilter.
Switch(config)#ipv6 pim accept-register list myfilter
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128

13.8.3.13 ipv6 pim bsr-border

Command: ipv6 pim bsr-border

no ipv6 pim bsr-border

Function: To configure or delete PIM6 BSR-BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

Switch(Config-if-Vlan1)#ipv6 pim bsr-border

13.8.3.14 ipv6 pim bsr-candidate

Command: ipv6 pim bsr-candidate {vlan <vlan_id>|tunnel <tunnel-id>|<ifname>} [<hash-mask-length>] [<priority>]

no ipv6 pim bsr-candidate {vlan <vlan_id>| tunnel <tunnel-id>|<ifname>} [<hash-mask-length>] [<priority>]

Function: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. The command "**no ipv6 pim bsr-candidate {vlan <vlan_id>| tunnel <tunnel-id>|<ifname>} [<hash-mask-length>] [<priority>]**" command disables the candidate BSR.

Parameter: <vlan_id> is VLAN ID ,the value ranges from 1 to 4094;

<tunnel_id> is tunnel ID,the value ranges from 1 to 50;

<ifname> is the specified interface name;

[*hash-mask-length*] is the specified hash mask length. It's used for the RP enable selection and ranges from 0 to 32;

[*priority*] is the candidate BSR priority and ranges from 0 to 255. If this parameter is not configured, the default priority value is 0.

Default: This switch is not a candidate BSR router

Command Mode: Global Mode

Usage Guide: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. Only this command is configured, this switch is the BSR candidate router.

Example: Globally configure the interface vlan1 as the candidate BSR-message transmitting interface.

Switch (config)# ipv6 pim bsr-candidate vlan1 30 10

13.8.3.15 ipv6 pim cisco-register-checksum

Command: ipv6 pim cisco-register-checksum [group-list <*access-list name*>]

no ipv6 pim cisco-register-checksum [group-list <*access-list name*>]

Function: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Default: Compute the checksum according to the register packet's head length default: 8

Parameter: <*access-list name*> is the applying simple access-list.

Command Mode: Global Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Switch(config)**#**ipv6 pim cisco-register-checksum group-list myfilter

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128

13.8.3.16 ipv6 pim dr-priority

Command: ipv6 pim dr-priority <*priority*>

no ipv6 pim dr-priority

Function: Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ipv6 pim dr-priority**" command restores the default value.

Parameter: <*priority*> priority, it ranges from 0 to 4294967294

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Switch (config)# interface vlan 1

Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

13.8.3.17 ipv6 pim exclude-genid

Command: ipv6 pim exclude-genid

no ipv6 pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option, the "**no ipv6 pim exclude-genid**" command restores the default value.

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel

carefully.

Example: Configure the Hello packets sent by the switch do not include GenId option.

Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

13.8.3.18 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <*value*>

no ipv6 pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbor holdtime, if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor is deleted.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s, so Holdtime's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval, this configuration is denied. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval, hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan1's Hello Holdtime to 10s

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10

13.8.3.19 ipv6 pim hello-interval

Command: ipv6 pim hello-interval <*interval*>

no ipv6 pim hello-interval

Function: Configure the interface's hello_interval of pim hello packets. The "**no ipv6 pim hello-interval**" command restores the default value.

Parameter: <*interval*> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s

Default: The default periodically transmitted pim hello packets' hello_interval is 30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello messages make pim switches oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor overtime. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure VLAN's pim-sm hello_interval.

Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20

13.8.3.20 ipv6 pim ignore-rp-set-priority

Command: ipv6 pim ignore-rp-set-priority
no ipv6 pim ignore-rp-set-priority
Function: When RP selection is carried out, this command configures the switch to enable Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.
Default: None
Parameter: None
Command Mode: Global Mode
Usage Guide: When selecting RP, PIM usually will select according to RP priority. When this command is configured, PIM will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.
Example: Configure to ignore RP priority.
Switch(config)#ipv6 pim ignore-rp-set-priority

13.8.3.21 ipv6 pim jp-timer

Command: ipv6 pim jp-timer <*value*>
no ipv6 pim jp-timer
Function: Configure to add JP timer. **no ipv6 pim jp-timer** restores the default value.
Parameter: <*value*> ranges from 10 to 65535
Default: 60s
Command Mode: Global Mode
Usage Guide: Configure the interval of transmitting J/P messages to59s.
Example: Switch(config)#ipv6 pim jp-timer 59

13.8.3.22 ipv6 pim multicast-routing

Command: ipv6 pim multicast-routing
no ipv6 pim multicast-routing
Function: Enable PIM-SM globally. The "**no ipv6 pim multicast-routing**" command disables PIM-SM globally.
Parameter: None
Default: Disabled PIM-SM protocol
Command Mode: Global Mode
Usage Guide: Inspect the changing information about pim state by this switch..
Example: Enable PIM-SM globally.
Switch (config)#ipv6 pim multicast-routing

13.8.3.23 ipv6 pim neighbor-filter

Command: ipv6 pim neighbor-filter <a*ccess-list-name*>

no ipv6 pim neighbor-filter <a*ccess-list-name*>

Function: Configure the neighbor access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this connection can't be created.

Parameter: <a*ccess-list-name*> is the applying access-list' name

Default: No neighbor filter configuration

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1, access-list 1's default is deny. In the following example, if "permit any" is not configured, deny fe80:20e:cff:fe01:facc is the same as deny any. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure VLAN's pim neighbor access-list.

Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01:facc

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#permit any

13.8.3.24 ipv6 pim register-rate-limit

Command: ipv6 pim Register-rate-limit *<limit>*

no ipv6 pim Register-rate-limit

Function: This command is used to configure the speedrate of DR sending register packets, the unit is packet/second. The "**no ipv6 pim Register-rate-limit**" command restores the default value. This configured speedrate is each（S, G）state's, not the whole systems.

Parameter: *<limit>* ranges from 1 to 65535

Default: No limit for sending speed

Command Mode: Global Mode

Usage Guide: Configure the speedrate of DR sending register packets.

Example: Configure the speedrate of DR sending register packets to 59p/s.

Switch(config)#ipv6 pim Register-rate-limit 59

13.8.3.25 ipv6 pim register-rp-reachability

Command: ipv6 pim Register-rp-reachability

no ipv6 pim Register-rp-reachability

Function: This command makes DR check the RP reachability in the process of registration.

Parameter: None

Default: Do not check.

Command Mode: Global Mode.

Usage Guide: This command configures DR whether or not to check the RP reachability.
Example: Configure the router to check the RP reachability before sending register packets.
Switch(config)# ipv6 pim Register-rp-reachability

13.8.3.26 ipv6 pim register-source

Command: ipv6 pim register-source {<*source-address*> |<*ifname*>|vlan <*vlan-id*>}
no ipv6 pim register-source
Function: This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is usually the RPF neighbor of source host direction.
Parameter: <*ifname*> is the interface name that will be the register packets source.
<*source-address*> is the interface address will be the register packets source. In the format of hex without prefix length.
<vlan-id> is the VLAN ID.
Default: Do not check.
Command Mode: Global Mode
Usage Guide: The "**no ipv6 pim register-source**" command restores the default value, no more parameter is needed. Configured address must be reachable to Register-Stop messages sent by RP. It's usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.
Example: Configure the source address of the sent register packets to vlan1's address
Switch(config)# ipv6 pim register-source Vlan1

13.8.3.27 ipv6 pim register-suppression

Command: ipv6 pim register-suppression <*value*>
no ipv6 pim register-suppression
Function: This command is to configure the value of register suppression timer, the unit is second.
Parameter: <*value*> is the timer's value, it ranges from 10 to 65535s.
Default: 60s
Command Mode: Global Mode
Usage Guide: If this value is configured at DR, it's the value of register suppression timer; if this value is configured at RP and ipv6 pim rp-register-kat is not used at RP, this command modifies Keepalive-period value. The "**no ipv6 pim register-suppression**" command restores the default value.
Example: Configure the value of register suppression timer to 30s.
Switch(config)# ipv6 pim register-suppression 30

13.8.3.28 ipv6 pim rp-address

Command: ipv6 pim rp-address <*rp-address*> [<*group-range*>]

no ipv6 pim rp-address <*rp-address*> [all|<*group-range*>]

Function: This command is to configure static RP globally or in a multicast address range. The "**no ipv6 pim rp-address**" command cancels static RP.

Parameter: <*rp-address*> is the RP address, the format is **X:X::X:X** ,**ipv6** address

<*group-range*> is the expected RP, the format is **X:X::X:X/M, ipv6** address and prefix length all the ranges

Default: This switch is not a RP static router

Command Mode: Global Mode

Usage Guide: This command is to configure static RP globally or in a multicast address range.

Example: Configure 2000:112::8 as RP address globally.

Switch (config)# ipv6 pim rp-address 2000:112::8 ff1e::/64

13.8.3.29 ipv6 pim rp-candidate

Command: ipv6 pim rp-candidate{vlan<vlan-id> |loopback<index> |<ifname>}[<group range>] [<priority>]

no ipv6 pim rp-candiate

Function: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. The "**no ipv6 pim rp-candiate**" command cancels the candidate RP.

Parameter: <vlan_id> is VLAN ID；

<index> is Loopback interface index;

<*ifname*> is the name of the interface;

<*group range*> is the group range of the candidate RP,the format is **X:X::X:X/M**, **ipv6** address and prefix length;

<*priority*> is the RP selection priority, ranges from 0 to 255, the default value is 192, the lower value has more priority

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. Only this command is configured, this switch is the RP candidate router

Example: Configure vlan1 as the sending interface of candidate RP announce messages

Switch (config)# ipv6 pim rp-candidate vlan1 100

13.8.3.30 ipv6 pim rp-register-kat

Command: ipv6 pim rp-register-kat <*vaule*>

no ipv6 pim rp-register-kat

Function: This command is to configure the KAT (KeepAlive Timer) value of the RP (S, G) items, the unit is second. The "**no ipv6 pim rp-register-kat**" command restores the default value.

Parameter: <*vaule*> is the timer value, ranges from 1 to 65535s

Default: 185s

Command Mode: Global Mode
Usage Guide: Configure rp-register-kat interval to 30s.
Example: Switch(config)# ipv6 pim rp-register-kat 30

13.8.3.31 ipv6 pim scope-border

Command: ipv6 pim scope-border [<*500-599*>|<*acl_name*>]
no ipv6 pim scope-border
Function: To configure or delete management border of PIM6.
Parameters: <*500-599*> is the ACL number for the management border.
<*acl_name*> is the ACL name for the management border.
Default: Not management border. If no ACL is specified, the default management border will be used.
Command Mode: Interface Configuration Mode.
Usage Guide: To configure the management border and the ACL for the IPV6 PIM. The multicast data flow will not be forwarded to the SCOPE-BORDER.
Example:
Switch(Config-if-Vlan2)#ipv6 pim scope-border 503

13.8.3.32 ipv6 pim sparse-mode

Command: ipv6 pim sparse-mode [passive]
no ipv6 pim sparse-mode [passive]
Function: Enable PIM-SM on the interface. **no ipv6 pim sparse-mode [passive]** disables PIM-SM.
Parameter: [*passive*] means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable MLD(reveice and transmit MLD packets).
Default: Disabled PIM-SM
Command Mode: Interface Configuration Mode
Usage Guide: Enable PIM-SM on the interface. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example: Enable PIM-SM on the interface vlan1.
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 pim sparse-mode

13.8.3.33 show ipv6 pim bsr-router

Command: show ipv6 pim bsr-router
Function: Display BSR address.
Parameter: None
Default: None
Command Mode: Admin Mode and Global Mode
Example:
Switch#show ipv6 pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 2000:1:111::100 (?)
Uptime: 00:16:00, BSR Priority: 0, Hash mask length: 126
Next bootstrap message in 00:00:10
Role: Candidate BSR
State: Elected BSR
Next Cand_RP_advertisement in 00:00:10
RP: 2000:1:111::100(Vlan2)

Displayed Information	Explanations
BSR address	Bsr-router Address
Priority	Bsr-router Priority
Hash mask length	Bsr-router hash mask length
State	The current state of this candidate BSR, Elected BSR is selected BSR

13.8.3.34 show ipv6 pim interface

Command: show ipv6 pim interface [detail]
Function: Display PIM interface information.
Parameter: None
Default: None
Command Mode: Any Mode
Example:
Switch#show ipv6 pim interface
Interface VIFindex Ver/ Nbr DR
Mode Count Prior
Vlan2 0 v2/S 0 1
Address : fe80::203:fff:fee3:1244
Global Address: 2000:1:111::100
DR : this system
Vlan3 2 v2/S 0 1
Address : fe80::203:fff:fee3:1244
Global Address: 2000:10:1:13::1
DR : this system

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode, usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority

DR	The interface's DR address

13.8.3.35 show ipv6 pim mroute sparse-mode

Command: show ipv6 pim mroute sparse-mode

Function: Display the multicast route table of PIM-SM.

Parameter: None

Default: None

Command Mode: Admin Mode and Configuration Mode

Usage Guide: Display the BSP routers in the network maintained by PIM-SM.

Example:

```
Switch#show ipv6 pim mr    group ff1e::15
IPv6 Multicast Routing Table
  (*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
  (*, ff1e::15)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
  Local         ..l.....................
  Joined        .....................
  Asserted      .....................
FCR:
  (2000:1:111::11, ff1e::15)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
  Local         .....................
  Joined        .....................
  Asserted      .....................
  Outgoing      ..o..................
  (2000:1:111::11, ff1e::15, rpt)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: NOT PRUNED
  Pruned        .....................
  Outgoing      ..o..................
```

Displayed Information	Explanations
Entries	The counts of each item
RP	Share tree's RP address
RPF nbr	RP direction or upneighbor of source direction
RPF idx	RPF nbr interface
Upstream State	Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for（S,G,rpt.）
Local	Local join interface, this interface receive IGMPJoin
Joined	PIM join interface, this interface receive J/P messages
Asserted	Asserted state
Outgoing	Final outgoing of multicast data

13.8.3.36 show ipv6 pim neighbor

Command: show ipv6 pim neighbor [detail|]

Function: Display router neighbors.

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display multicast router neighbors maintained by the PIM.

Example:

Switch(config)#show ipv6 pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
Fe80::203:fff:fee3:1244	Vlan1	00:00:10/00:01:35	v2	1 /DR
fe80::20e:cff:fe01:facc	Vlan1	00:00:13/00:01:32	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP

13.8.3.37 show ipv6 pim nexthop

Command: show ipv6 pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table.

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

Switch#show ipv6 pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable ….

Destination	Type	Nexthop Num	Nexthop Addr	..Nexthop Ifindex	Nexthop Name	Metric	Pref	Refcnt
2000:1:111::11	..S.	1		2004		0	0	2
2000:1:111::100	.RS.	1		2004		0	0	2

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can’t reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

13.8.3.38 show ipv6 pim rp-hash

Command: show ipv6 pim rp-hash X:X::X:X

Function: Display the RP address of group X:X::X:X’s merge point.

Parameter: Group address

Default: None

Command Mode: Any Mode

Usage Guide: Display the RP address corresponding to the specified group address.

Example:

Switch#show ipv6 pim rp-hash ff1e::15

RP: 2000:1:111::100

Info source: 2000:1:111::100, via bootstrap

Displayed Information	Explanations
RP	Queried group'sRP
Info source	The source of Bootstrap information

13.8.3.39 show ipv6 pim rp mapping

Command: show ipv6 pim rp mapping
Function: Display Group-to-RP Mapping and RP.
Parameter: None
Default: None
Command Mode: Any Mode
Usage Guide: Display the current RP and mapping relationship.
Example:
Switch#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
RP: 2000:1:111::100
Info source: 2000:1:111::100, via bootstrap, priority 192
Uptime: 00:10:24, expires: 00:02:06
Group(s): ff00::/8, Static
RP: 2000:1:111::100
Uptime: 00:11:01

Displayed Information	Explanations
Group(s)	Group address range of RP
Info source	Source of Bootstrap messages
Priority	Priority of Bootstrap messages

13.8.4 ANYCAST RP v6

13.8.4.1 debug ipv6 pim anycast-rp

Command: debug ipv6 pim anycast-rp
no debug ipv6 pim anycast-rp
Function: Enable the debug switch of ANYCAST RP function; the no operation of this command will disable this debug switch.
Command Mode: Admin Mode.
Default: The debug switch of ANYCAST RP is disabled by default.
Usage Guide: This command is used to enable the debug switch of ANYCAST RP of the router, it can display the information of handling PIM register packet of the switch——packet, and the information of events——event.

Example:
Switch#debug ipv6 pim anycast-rp

13.8.4.2 ipv6 pim anycast-rp

Command: ipv6 pim anycast-rp
no ipv6 pim anycast-rp
Function: Enable the ANYCAST RP of the switch; the no operation of this command is to disable the ANYCAST RP function.
Command Mode: Global Configuration Mode.
Default: The switch will not enable the ANYCAST RP by default.
Usage Guide: This command will globally enable ANYCAST RP protocol, but in order to make ANYCAST RP work, it is necessary to configure self-rp-address and other-rp-address set.
Example: Enable ANYCAST RP in global configuration mode.
Switch(config)#ipv6 pim anycast-rp

13.8.4.3 ipv6 pim anycast-rp

Command: ipv6 pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>
no ipv6 pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>
Function: Configure ANYCAST RP address（ARA）and the unicast addresses of other RP communicating with this router(as a RP). The no operation of this command will cancel the unicast address of another RP in accordance with the configured RP address.
Parameters: ***anycast-rp-addr*****:** RP address, the current absence of the candidate interface in accordance with the address is allowed.
other-rp-addr**:** The unicast address of other RP communicating with this router(as a RP).
Command Mode: Global Configuration Mode.
Default: There is no configuration by default.
Usage Guide:
1. The anycast-rp-addr configured on this router (as a RP) is actually the RP address configured on multiple RP in the network, in accordance with the address of RP candidate interface (or Loopback interface). The current absence of the candidate interface in accordance with the address is allowed when configuring.
2. Configure the other-rp-address of other RPs communicating with this router (as a RP). The unicast address identifies other RP, and is used to communicate with the local router.
3. Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RP in the network to notify all the RP in the network of the source (S.G) state. While forwarding, the router will change the destination address of the register message into other-rp-address.
4. Multiple other-rp-addresses can be configured in accordance with one anycast-rp-addr, once the register message from a DR is received, it should be forwarded to all of these other RP one by one.

Example: Configure other-rp-address in global configuration mode.
Switch(config)#ipv6 pim anycast-rp 2000::1 2004::2

13.8.4.4 ipv6 pim anycast-rp self-rp-address

Command: ipv6 pim anycast-rp self-rp-address <*self-rp-addr*>
no ipv6 pim anycast-rp self-rp-address
Function: Configure the self-rp-address of this router (as a RP). This address will be used to exclusively identify this router from other RP, and to communicate with other RP. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RP.
Parameters: *self-rp-addr*: The unicast address used by this router (as a RP) to communicate with other RP.
Command Mode: Global Configuration Mode.
Default: No self-rp-address is configured by default.
Usage Guide:
1. Once this router (as a RP) receives the register message from DR unicast, it needs to forward the register message to all the other RP in the network, notifying them of the state of source (S.G). While forwarding the register message, this router will change the source address of it into self-rp-address.
2. Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a register-stop message, whose destination address is the source address of the register message.
3. self-rp-address has to be the address of a three-layer interface on this router, but the configuration is allowed to be done with the absence of the interface.
Example: Configure the self-rp-address of this router in global configuration mode.
Switch(config)#ipv6 pim anycast-rp self-rp-address 2000::1

13.8.4.5 ipv6 pim rp-candidate

Command: ipv6 pim rp-candidate {vlan<*vlan-id*> |loopback<*index*> |<*ifname*>} [<*A:B::C:D*>] [<*priority*>]
no ipv6 pim rp-candidate
Function: Add a Loopback interface as a RP candidate interface based on the original PIM6-SM command; the no operation of this command is to cancel the Loopback interface as a RP candidate interface.
Parameters: *index*: Loopback interface index, whose range is <1-1024>.
***vlan-id*:** the Vlan ID.
***ifname*:** the specified name of the interface.
A:B::C:D/M: the ip prefix and mask.
***<priority>*:** the priority of RP election, ranging from 0 to 255, the default value is 192, the smaller the value is the higher the priority is.

Command Mode: Global Configuration Mode.
Default Setting: No RP interface is configured by default.
Usage Guide: In order to support ANYCAST RP function, new rule allows configuring a Loopback interface to be the RP candidate interface, the RP candidate interface should be currently unique, and the address of which should be added into the router to make sure that PIM router can find the nearest RP. The “no ipv6 pim rp-candidate” command can be used to cancel the RP candidate.
Example: Configure Loopback1 interface as the RP candidate interface in global configuration mode.
Switch(config)# ipv6 pim rp-candidate loopback1

13.8.4.6 show debugging ipv6 pim

Command: show debugging ipv6 pim
Command Mode: Admin and Configuration Mode.
Usage Guide: The current state of ANYCAST RP debug switch.
Example:
Switch(config)#show debugging ipv6 pim

Debugging status:
PIM anycast-rp debugging is on

13.8.4.7 show ipv6 pim anycast-rp first-hop

Command: show ipv6 pim anycast-rp first-hop
Command Mode: Admin and Configuration Mode.
Usage Guide: Display the state information of ANYCAST RP, and display the mrt node information generated in the first hop RP which is currently maintained by the protocol.
Example:
Switch(config)#show ipv6 pim anycast-rp first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0

INCLUDE (2000:1:111::2, ffle::1)
Local .l.....

Display	Explanation
Entries	The number of all kinds of entries.
INCLUDE	The mrt information created in the first hop RP.

13.8.4.8 show ipv6 pim anycast-rp non-first-hop

Command: show ipv6 pim anycast-rp non-first-hop
Command Mode: Admin and Configuration Mode.
Usage Guide: Display the state information of ANYCAST RP, and display the mrt node information generated in the non first hop RP which is currently maintained by the protocol, that is the mrt node information which is created after the first hop RP transfers the register message it received to this RP.
Example:
Switch(config)#show ip pim anycast-rp non-first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0

INCLUDE (2002:1:111::2, ffle::2)
Local .l.....

Display	Explanation
Entries	The number of all kinds of entries.
INCLUDE	The mrt information created in the first hop RP.

13.8.4.9 show ipv6 pim anycast-rp status

Command: show ipv6 pim anycast-rp status
Command Mode: Admin and Configuration Mode.
Usage Guide: Display the configuration information of ANYCAST RP, whether ANYCAST RP globally enables, whether the self-rp-address is configured and the list of currently configured ANYCAST RP set.
Example:
Switch(config)#show ipv6 pim anycast-rp status

Anycast RP status:
anycast-rp:Enabled!

self-rp-address:2004::2

anycast-rp address: 2000:1:111::2
other rp unicast rp address: 2002::1
other rp unicast rp address: 2005::1

anycast-rp address: 2003::1

other rp unicast rp address: 2002::2

Display	Explanation
anycast-rp:	Whether the ANYCAST RP switch is globally enabled.
self-rp-address:	The configured self-rp-address.
anycast-rp address:	The configured anycast-rp-address.
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address.
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address.
anycast-rp address:	The configured anycast-rp-address*.
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address.

13.8.5 PIM-SSM6

13.8.5.1 ipv6 pim ssm

Command: ipv6 pim ssm {default|range <*access-list-name* >}

no ipv6 pim ssm

Function: Configure the range of pim ssm multicast address. The "**no ipv6 pim ssm**" command deletes configured pim ssm multicast group.

Parameter: default: indicates the default range of pim ssm multicast group is ff3x::/32.

<access-list-number > is the name of applying access-list.

Default: Do not configure the range of pim ssm group address

Command Mode: Global Mode

Usage Guide:

1. Only this command is configured, pim ssm can be available.
2. Before configuring this command, make sure ipv6 pim multicasting succeed.
3. Access-list only can use the lists created by ipv6 access-list.
4. Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ipv6 pim ssm can release the bondage.
5. If ssm is needed, this command should be configured at the related edge route. For example, the local switch with igmp(must) and multicast source DR or RP(at least one of the two) configure this command, the middle switch need only enable PIM-SM.

Example: Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23.

Switch (config)#ipv6 pim ssm range 23

Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::/48

13.8.6 IPv6 DCSCM

13.8.6.1 ipv6 access-list(ipv6 multicast source control)

Command: ipv6 access-list <*8000-8099*> {deny|permit} {{<*source/M*> }|{host-source <*source-host-ip*>}|any-source} {{<*destination/M*> }|{host-destination <*destination-host-ip*>}|any-destination}

no ipv6 access-list <*8000-8099*> {deny|permit} {{<*source/M*>}|{host-source <*source-host-ip*>}|any-source} {{<*destination/M*> }|{host-destination <*destination-host-ip*>}|any-destination}

Function: Configure IPv6 source control multicast access list, the no operation of this command is used to delete the access list.

Parameters: *<8000-8099>*: The source control access list number.

{deny|permit}: Deny or permit.

***<source/M>*:** The multicast source address and the length of mask.

***<source-host-ip>*:** The multicast host address.

***<destination/M>*:** The multicast destination address and the length of mask.

***<destination-host-ip>*:** The multicast destination host addresses.

Default: None.

Command Mode: Global Configuration Mode.

Usage Guide: IPv6 multicast source control entries control the ACL it uses with ACL number 8000-8099, this command is used to configure such ACL. IPv6 multicast source control ACL only needs to configure the source IPv6 address and destination IPv6 address (that is the group IPv6 addresses)which are to be controlled, the configuration adopts a method similar to other ACLs, which can either be an address range configured by the length of mask, or a specified host address or all addresses. Pay attention to that: for group IPv6 addresses, the “all addresses” mentioned here is ff:/8.

Example:

Switch(config)#ipv6 access-list 8000 permit fe80::203:228a/64 ff1e::1/64

13.8.6.2 ipv6 access-list(multicast destination control)

Command: ipv6 access-list <*9000-10999*> {deny|permit} {{<*source/M*> }|{host-source <*source-host-ip*>}|any-source} {{<*destination/M*> }|{host-destination <*destination-host-ip*>}|any-destination}

no ipv6 access-list <*9000-10999*> {deny|permit} {{<*source/M*> }|{host-source <*source-host-ip*>}|any-source}

{{<*destination/M*> }|{host-destination <*destination-host-ip*>}|any-destination}

Function: Configure IPv6 destination control multicast access list, the no operation of this command is used to delete the access list.

Parameters: <9000-10999>: The source control access list number.

{deny|permit}: Deny or permit.

<source/M>: The multicast source address and the length of mask.

<source-host-ip>: Multicast source host address.

<destination/M>: Multicast destination address and the length of mask.

<destination-host-ip>: Multicast destination host address.

Default: None.

Command Mode: Global Configuration Mode.

Usage Guide: IPv6 multicast destination control entries control the ACL it uses with ACL number 9000-10999, this command is used to configure such ACL. IPv6 multicast source control ACL only needs to configure the source IPv6 address and destination IPv6 address (that is the group IPV6 addresses) , the configuration adopts a method similar to other ACLs, which can either be a address range configured by the length of mask, or a specified host address or all addresses Which are to be controlled. Pay attention to that, for group IPV6 addresses, the “all addresses” mentioned here is ff:/8.

Example:

Switch(config)#ipv6 access-list 9000 permit fe80::203:228a/64 ff1e::1/64

13.8.6.3 ipv6 multicast destination-control access-group

Command: ipv6 multicast destination-control access-group <*9000-10999*>

no ipv6 multicast destination-control access-group <*9000-10999*>

Function: Configure the IPv6 multicast destination control access list used by the port, the no operation of the command will delete this configuration.

Parameters: <*9000-10999*>: The destination control access list number.

Default: Not configured.

Command Mode: Port Configuration Mode.

Usage Guide: This command can only take effect when the IPv6 multicast destination control is globally enabled, after configuring this command, if the MLD-SNOOPING is enabled, when adding the port to the multicast group, it will be matched according to the configured access list. Only when the port is matched as permit, will it be added, or it can not be added.

Example:

switch(config)#inter ethernet 1/0/4

switch(Config-If-Ethernet1/0/4)#ipv6 multicast destination-control access-group 9000

switch(Config-If-Ethernet1/0/4)#

13.8.6.4 ipv6 multicast destination-control access-group (sip)

Command: ipv6 multicast destination-control <*IPADDRESS/M*> access-group <*9000-10999*>

no ipv6 multicast destination-control <*IPADDRESS/M*> access-group

<9000-10999>

Function: Configure multicast destination-control access-list used on specified net segment, the "**no ipv6 multicast destination-control <*IPADDRESS/M*> access-group <*9000-10999*>**" command deletes this configuration.

Parameter: <*IPADDRESS/M*>: IP address and mask length;

***<9000-10999>*:** Destination control access-list number.

Default: None.

Command Mode: Global Mode.

Usage Guide: The command is only working under global IPv6 multicast destination-control enabled, after configuring the command, if MLD-SPOOPING or MLD is enabled, for adding the members to multicast group. If configuring multicast destination-control on specified net segment of transmitted MLD-REPORT, and match configured access-list, such as matching permit, the interface can be added, otherwise do not be added. If relevant group or source in **show ipv6 mld groups detail** has been established before executing the command, it needs to execute **clear ipv6 mld group** command to clear relevant groups in admin mode.

Example:

Switch(config)#ipv6 multicast destination-control 2008::8/64 access-group 9000

13.8.6.5 ipv6 multicast destination-control access-group (vmac)

Command: ipv6 multicast destination-control *<1-4094>* *<macaddr>* access-group *<9000-10999>*

no ipv6 multicast destination-control *<1-4094>* *<macaddr>* access-group *<9000-10999>*

Function: Configure the IPv6 multicast destination access list used by the specified vlan-mac, the no operation of this command will delete this configuration.

Parameters: *<1-4094>*: VLAN-ID;

***<macaddr>*:** The source MAC address sending of the MLD-REPORT, the format of which is"xx-xx-xx-xx-xx-xx".

***<9000-10999>*:** Destination access list number.

Default: Not configured.

Command Mode: Global Configuration Mode.

Usage Guide: This command can only take effect when the IPv6 multicast destination control is globally enabled, after configuring this command, if the MLD-SNOOPING is enabled, when adding the port to the multicast group, it will be matched according to the configured access list. Only when the port is matched as permit, will it be added, or it can not be added.

Example:

switch(config)#ipv6 multicast destination-control 1 00-01-03-05-07-09 access-group 9000

13.8.6.6 ipv6 multicast policy

Command: ipv6 multicast policy *<IPADDRSRC/M>* *<IPADDRGRP/M>* cos *<priority>*

no ipv6 multicast policy <*IPADDRSRC/M*> <*IPADDRGRP/M*> cos

Function: Configure IPv6 policy multicast, the no operation of this command is to cancel the policy multicast of IPv6.

Parameters: <*IPADDRSRC/M*>: The source address and the length of the mask of IPv6 multicast.

<*IPADDRGRP/M*>: The multicast address of IPv6 and the length of mask of multicast address

<*priority*>: The specified priority, the range of which is <0-7>.

Default: Not configured.

Command Mode: Global Configuration Mode.

Usage Guide: Using this command to configure can change the priority of the multicast data which is confined by the act of matching of this switch to a specified value, and set the TOS to the same value simultaneously. Please pay attention to that, for the messages sent in UNTAG mode, their priority will not be changed.

Example:

Switch(config)**#**ipv6 multicast policy 2008::1/64 ff1e::3/64 cos 4

13.8.6.7 ipv6 multicast source-control

Command: ipv6 multicast source-control

no ipv6 multicast source-control

Function: Configure to globally enable IPv6 multicast source control, the no operation of this command is to recover and globally disable the IPv6 multicast source control.

Parameters: None.

Default: Disabled.

Command Mode: Global Configuration Mode.

Usage Guide: Only when the IPv6 multicast source control is enabled globally, the source control access list can be applied to ports. After configuring this command, the IPv6 multicast data received by all the ports will be dropped by the switch if there is no matched multicast source control entry, that it only the multicast data matched as PERMIT can be received and forwarded.

Example:

Switch(config)#ipv6 multicast source-control

13.8.6.8 ipv6 multicast source-control access-group

Command: ipv6 multicast source-control access-group <*8000-8099*>

no ipv6 multicast source-control access-group <*8000-8099*>

Function: Configure the multicast source control access list used by the port, the no operation of this command is used to delete the configuration.

Parameters: <*8000-8099*>: Source control access list number.

Default: Not configured.

Command Mode: Port Configuration Mode.

Usage Guide: This command can only be successfully configured when the IPv6 multicast source control is globally enabled, after configuring this command, all the IPv6 multicast messages

entering from the port will be matched according to the configured access list, only when the message is matched as permit, can it be received and forwarded, or it will be dropped.

Example:

switch(config)#inter ethernet 1/0/4

switch(Config-If-Ethernet1/0/4)#ipv6 multicast source-control access-group 8000

13.8.6.9 multicast destination-control

Command: multicast destination-control

no multicast destination-control

Function: Configure to globally enable IPv4 and IPv6 multicast destination control, after configuring this command, IPv4 and IPv6 multicast destination control will take effect at the same time. The no operation of this command is to recover and disable the IPv4 and IPv6 multicast destination control globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Configuration Mode.

Usage Guide: Only after globally enabling the multicast destination control, the other destination control configuration can take effect, the destination access list can be applied to ports, VLAN-MAC and SIP. After configuring this command, IGMP-SNOOPING, MLD-SNOOPING and IGMP, MLD will match according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT and MLD-REPORT.

Example:

switch(config)# multicast destination-control

13.8.6.10 show ipv6 multicast destination-control

Command: show ipv6 multicast destination-control [detail]

show ipv6 multicast destination-control interface <*Interfacename*> [detail]

show ipv6 multicast destination-control host-address <*ipv6addr*> [detail]

show ipv6 multicast destination-control <*vlan-id*> <*mac*> [detail]

Function: Display IPv6 multicast destination control configuration.

Parameters: detail: Whether to display detailed information.

***<Interfacename>*:** Interface name.

***<ipv6addr>*:** IPv6 address.

***<vlan-id>* :** VLAN ID.

***<mac>*:** MAC address.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Use this command to display the configured multicast destination control rules, if including the detail option, it will also display the details of the access-list in use.

Example:

switch(config)#show ipv6 multicast destination-control

ipv6 multicast destination-control is enabled
ipv6 multicast destination-control 2003::1/64 access-group 9003
ipv6 multicast destination-control 1 00-03-05-07-09-11 access-group 9001
multicast destination-control access-group 6000 used on interface Ethernet1/0/13
switch(config)#

13.8.6.11 show ipv6 multicast destination-control access-list

Command: show ip multicast destination-control access-list
show ip multicast destination-control access-list <*9000-10999*>
Function: Display the configured IPv6 destination control multicast access list.
Parameters: <*9000-10099*>: Access list number.
Default: None.
Command Mode: Admin Mode.
Usage Guide: Use this command to display the configured IPv6 destination control multicast access list.
Example:
switch# sh ipv6 multicast destination-control acc
ipv6 access-list 9000 permit 2003::2/64 ff1e::3/64
ipv6 access-list 9000 deny 2008::1/64 ff1e::1/64
ipv6 access-list 9000 permit any-source any-destination
ipv6 access-list 9001 deny any-source host-destination ff1a::1
ipv6 access-list 9001 permit any-source any-destination

13.8.6.12 show ipv6 multicast policy

Command: show ipv6 multicast policy
Function: Display the configured IPv6 multicast policy.
Parameters: None.
Default: None.
Command Mode: Admin Mode.
Usage Guide: Use this command to display the configured IPv6 multicast policy.
Example:
switch#show ipv6 multicast policy
ipv6 multicast-policy 2003::2/64 ff1e::3/64 cos 5

13.8.6.13 show ipv6 multicast source-control

Command: show ipv6 multicast source-control [detail]
show ipv6 multicast source-control interface <*Interfacename*> [detail]
Function: Display IPv6 multicast source control configuration.
Parameters: *detail*: whether to display detailed information.

***<Interfacename>*:** Port name.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Use this command to display the configured multicast source control rules, if including the detail option, it will also display the details of the access-list in use.

Example:

Switch#show ipv6 multicast source-control detail
Ipv6 multicast source-control is enabled
Interface Ethernet 1/0/1 use multicast source control access-list 8000
 ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64
 ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64
 ipv6 access-list 8000 permit any-source any-destination

13.8.6.14 show ipv6 multicast source-control access-list

Command: show ipv6 multicast source-control access-list

show ipv6 multicast source-control access-list *<8000-8099>*

Function: Display the configured IPv6 source control multicast access list.

Parameters: *<8000-8099>*: Access list number.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Use this command to display the configured source control multicast access list.

Example:

switch#sh ipv6 multicast source-control access-list
 ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64
 ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64

13.8.7 MLD

13.8.7.1 clear ipv6 mld group

Command: clear ipv6 mld group [X:X::X:X | IFNAME]

Function: Delete the group record of the specific group or interface.

Parameters: X:X::X:X the specific group address; IFNAME the specific interface address.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

Switch#clear ipv6 mld group

Relative Command: show ipv6 mld group

13.8.7.2 debug ipv6 mld events

Command: debug ipv6 mld events

no debug ipv6 mld events

Function: Enable the debug switch that displays MLD events. The **"no debug ipv6 mld events**" command disables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: This switch can be enabled to get MLD events information.

Example:

Switch# debug ipv6 mld events

Switch#1970/01/01 07:30:13 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3

1970/01/01 07:30:13 IMI: Processing Report comes from Vlan1, ifindex 2003

1970/01/01 07:30:13 IMI: MLD(Querier) ff1e::1:3 (Vlan1): No Listeners --> Listeners Present

13.8.7.3 debug ipv6 mld packet

Command: debug ipv6 mld packet

no debug ipv6 mld packet

Function: Enable the debug switch that displays MLD packets. The **"no debug ipv6 mld events**" command disables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: This switch can be enabled to get MLD packets information.

Example:

Switch# deb ipv6 mld packet

Switch#1970/01/01 07:33:12 IMI: Recv MLD packet

1970/01/01 07:33:12 IMI: Type: Listener Report (131)

1970/01/01 07:33:12 IMI: Code: 0

1970/01/01 07:33:12 IMI: Checksum: 3b7a

1970/01/01 07:33:12 IMI: Max Resp Delay: 0

1970/01/01 07:33:12 IMI: Reserved: 0

1970/01/01 07:33:12 IMI: Multicast Address: ff1e::1:3

1970/01/01 07:33:12 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3

1970/01/01 07:33:12 IMI: Processing Report comes from Vlan1, ifindex 2003

1970/01/01 07:33:12 IMI: MLD(Querier) ff1e::1:3 (Vlan1): Listeners Present --> Listeners Present

13.8.7.4 ipv6 mld access-group

Command: ipv6 mld access-group {<*acl_name*>}

no ipv6 mld access-group

Function: Configure the access control of the interface to MLD groups; the "**no ipv6 mld access-group**" command stops the access control.
Parameter: ***<acl-name>*** is the name of IPv6 access-list
Default: no filter condition
Command Mode: Interface Configuration Mode
Usage Guide: Configure the interface to filter MLD groups, allow or deny some group's join.
Example: Configure the interface vlan2 to accept group FF1E::1:0/112 and deny others
Switch(config)#ipv6 access-list extended aclv6
Switch(config-ipv6-ext-nacl-aclv6)#permit ff1e::1:0/112 any-destination
Switch(config-ipv6-ext-nacl-aclv6)#deny any-source any-destination
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)#ipv6 mld access-group aclv6

13.8.7.5 ipv6 mld immediate-leave

Command: ipv6 mld immediate-leave group-list {*<acl-name>*}
no ipv6 mld immediate-leave
Function: Configure MLD to work in the immediate leave mode, that's when the host sends a membership qualification report that equals to leave a group, the router doesn't send query and consider there is no this group's member in the subnet. The **"no ipv6 mld immediate-leave**" command cancels the immediate leave mode.
Parameter: ***<acl-name>*** is the name of IPv6 access-list
Default: Do not configure immediate-leave group
Command Mode: Interface Configuration Mode
Usage Guide: This command is used only when there is only one host in the subnet.
Example: Configure access-list"aclv6"as immediate leave mode.
Switch(Config-if-Vlan1)#ipv6 mld immediate-leave group-list aclv6

13.8.7.6 ipv6 mld join-group

Command: ipv6 mld join-group *<address>*
no ipv6 mld join-group <address>
Function: Configure the interface to join in certain multicast group; the "**no ipv6 mld join-group <address>**" command cancels joining certain multicast group.
Parameter: ***<address>*** is a valid IPv6 multicast address
Default: No multicast group joined by factory default
Command Mode: Interface Configuration Mode
Usage Guide: The address range of the IPv6 multicast is FFxy::/8, however the (FF02::/16) is permanent addresses which can not be joined in.
Example: Join the interface vlan2 in multicast group with multicast address of ff1e::1:3.
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3

13.8.7.7 ipv6 mld join-group mode source

Command: ipv6 mld join-group *<X:X::X:X>* mode *<include|exclude>* source *<.X:X::X:X>*

no ipv6 mld join-group <X:X::X:X> source <.X:X::X:X>

Function: Configure the sources of certain multicast group which the interface join in. Note: because of the client group has got only INLCUDE and EXCLUDE modes, if the source mode is not in accordance with current mode configured, the group mode will be changed and the original sources of the other modes configured will be cleared permanently; the "no" form of this command cancels joining certain group.

Parameter: ***<X:X::X:X>*** is a valid IPv6 multicast address

***<include|exclude>*:** joining mode

***<.X:X::X:X>*:** source list, configure several sources is allowed.

Default: No multicast group to be joined by factory default

Command Mode: Interface Configuration Mode

Usage Guide: The address range of the IPv6 multicast is FFxy::/8, however the (FF02::/16) is permanent addresses which can not be joined in. As for sources with mode same as the original one, the source will be added, while for those with different modes, the original sources will be cleared.

Example:

Join vlan2 in multicast group with multicast address of ff1e::1:3, with sources 2003::1 and 2003::2 in INCLUDE mode.

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3 mode include source 2003::1 2003::2

13.8.7.8 ipv6 mld last-member-query-interval

Command: ipv6 mld last-member-query-interval *<interval>*

no ipv6 mld last-member-query-interval

Function: Configure the interface's sending interval of querying specific group. The "**no ipv6 mld last-member-query-interval**" command cancels the manually configured value and restores the default value.

Parameter: ***<interval>*** is the interval of querying specific group, it ranges from 1000 to 25500ms. It's the integer times of 1000ms. If it's not the integer times of 1000ms, the system will convert it to the integer times of 1000ms.

Default: 1000ms.

Command Mode: Interface Configuration Mode

Example: Configure the interface vlan1's MLD last-member-query-interval as 2000.

Router(config)#int vlan 1

Router(Config-if-vlan1)#ipv6 mld last-member-query-interval 2000

13.8.7.9 ipv6 mld limit

Command:ipv6 mld limit <*state-count*>

no ipv6 mld limit

Function: Configure the MLD state count limit of the interface; the "**no ipv6 mld limit**" command restores the manually configured value to default value.

Parameter: <*state-count*>:max MLD state the interface maintains, the valid range is 1-5000.

Default: 400 by default

Command Mode: Interface Configuration Mode

Usage Guide: When max state-count is configured, the number of the state the interface saves will only upper to the state-count limit; and when the max state-count is reached, the later new member qualification report received will be ignored. If some MLD group state has already been saved before this command configured, the original states will be removed and the MLD general query will be sent to collect group member qualification reports no more than the max state-count.

Example: Set the MLD state-count limit of the interface vlan2 to 4000.

Switch(config)#interface vlan2

Switch(Config-if-Vlan2)#ipv6 mld limit 4000

13.8.7.10 ipv6 mld query-interval

Command: ipv6 mld query-interval <*time_val*>

no ipv6 mld query-interval

Function: Configure the interval of the periodically sent MLD host-query messages; the "**no ipv6 mld query-interval**" command restores the default value.

Parameter: <*time_val*> is the interval of the periodically sent MLD host-query messages; it ranges from 0 to 65535s

Default: Intrerval of periodically transmitted MLD query message is 125s.

Command Mode: Interface Configuration Mode

Usage Guide: When a interface enables a kind of multicast protocol, it will send MLD host-query messages periodically. This command is used to configure the query period.

Example: Configure the interval of the periodically sent MLD host-query messages to 10s.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 mld query-interval 10

13.8.7.11 ipv6 mld query-max-response-time

Command: ipv6 mld query-max-response-time <*time_val*>

no ipv6 mld query- max-response-time

Function: Configure the maximum of the response time of MLD queries; the "**no ipv6 mld query-max-response-time**" command restores the default value.

Parameter: <*time_val*> is the maximum of the response time of MLD queries, it ranges from 1 to 8000s.

Default: 10s.

Command Mode: Interface Configuration Mode

Usage Guide: When the switch receives a query message, the host will set a timer to each

multicast group. The timer's value is between 0 to the maximum response time. When any one of the timers decreases to 0, the host will group member announce messages. Configuring the maximum response time reasonablely, the host can swiftly response to the query messages and the router can also get the group members' existing states quickly.

Example: Configure the maximum response time of MLD queries to 20s.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 mld query- max-response-time 20

13.8.7.12 ipv6 mld query-timeout

Command: ipv6 mld query-timeout <*time_val*>

no ipv6 mld query-timeout

Function: Configure the interface's timeout of MLD queries; the "**no ipv6 mld query-timeout**" command restores the default value.

Parameter: <*time_val*> is the timeout of MLD queries, it ranges from 60 to 300s

Default: 255s

Command Mode: Interface Configuration Mode

Usage Guide: In the share network, when there are more switches that run MLD, one switch will be selected as the querying host and others set a timer to inspect the querying host's state. If no querying packet is received when the timeout is over, a switch will be reselected as the querying host.

Example: Configure the interface's timeout of MLD queries to 100s.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 mld query-timeout 100

13.8.7.13 ipv6 mld static-group

Command: ipv6 mld static-group <group_address> [source <source_address>]

no ipv6 mld static-group <group_address> [source <source_address>]

Function: Configure certain static group or static source on the interface. The "no" form of this command cancels certain previously configured static group or static source.

Parameter: <group_address> is a valid IPv6 multicast address;<source_address> is a valid IPv6 unicast address.

Default: No static group or static source is configured on the interface by factory default.

Command Mode: Interface Configuration Mode

Usage Guide: The valid range of the static group multicast address configured by the interface is the dynamic multicast address specified by the IPv6 protocol. Once the interface configures static group or static source for the multicast address, no matter whether there is membership qualification report of this group or source in the subnet, MLD protocol will consider that the group or source exist. Note: the configured static source is the source to be forwarded.

Example: Configure an MLD static-group ff1e::1:3 on interface vlan2.

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3

Configure a static source 2001::1 of the group ff1e::1:3 on interface vlan2
Switch(config)#int vlan2
Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3 source 2001::1

13.8.7.14 ipv6 mld version

Command: ipv6 mld version *<version_no>*
no ipv6 mld version
Function: Configure the version of the MLD protocol running on the interface; the "**no ipv6 mld version**" command restores the manually configured version to the default one.
Parameter: *<version_no>* is the version number of the MLD protocol, with a valid range of 1-2.
Default: 2 by default
Command Mode: Interface Configuration Mode
Usage Guide: While there is routers still not upgraded to version 2 of MLD protocol on the subnet connected, the interface should be configured to corresponding version.
Example: Configure the MLD version to 2.
Swith(config)#interface vlan 1
Swith(config-if-vlan1)#ipv6 mld version 2

13.8.7.15 show ipv6 mld groups

Command: show ipv6 mld groups [{*<ifname | group_addr>*}]
Function: Display the MLD group information.
Parameter: *<ifname>* is the name of the interface. Display the MLD group information. ***<group_addr>*** is the group address. Display the specified group information.
Default: Do not display
Command Mode: Admin Mode
Example:
Switch#sh ipv6 mld group
MLD Connected Group Membership

Group Address	Interface	Uptime	Expires
ff1e::1:3	Vlan1	00:00:16	00:03:14

Switch#

Displayed Information	Explanations
Group Address	Multicast group IP address
Interface	The interface of multicast group
Uptime	The existing time of the multicast group
Expires	The left time to overtime

13.8.7.16 show ipv6 mld interface

Command: show ipv6 mld interface [*<ifname>*]
Function: Display the relevant MLD information of an interface.

Parameter: ***<ifname>*** is the name of the interface. Display the MLD information of a specific interface.
Default: Do not display
Command Mode: Admin Mode
Example: Display the MLD information of the Ethernet Interface vlan1
Switch#show ipv6 mld interface Vlan1
Interface Vlan1(2003)
Index 2003
Internet address is fe80::203:fff:fe01:e4a
MLD querier
MLD query interval is 100 seconds
MLD querier timeout is 205 seconds
MLD max query response time is 10 seconds
Last member query response interval is 1000 ms
Group membership interval is 210 seconds
MLD is enabled on interface

13.8.7.17 show ipv6 mld join-group

Command: show ipv6 mld join-group
show ipv6 mld join-group interface {vlan *<vlan_id>*|*<ifname>*}
Function: Display the join-group messages on the interfaces.
Parameters: <ifname> is the name of the interface, which means to display MLD information on the specified interface.
Default: Do not display
Command Mode: Admin and Configuration Mode.
Example: Display the MLD information on Ethernet interfaces in vlan2.
Switch#show ipv6 mld join-groups vlan 2
Mld join group information:
INTERFACE: Vlan2
HOST VERSION: 2
MULTICAST ADDRESS: ff1e:: 1:3
GROUP STATE: EXCLUDE
SOURCE ADDRESS: 2003::1 mode: EXCLUDE
SOURCE ADDRESS: 2003::2 mode: EXCLUDE
SOURCE ADDRESS: 2003::6 mode: EXCLUDE
SOURCE ADDRESS: 2003::9 mode: EXCLUDE

13.8.8 MLD Snooping

13.8.8.1 clear ipv6 mld snooping vlan

Command: clear ipv6 mld snooping vlan <1-4094> groups [X:X::X:X]

Function: Delete the group record of the specific VLAN.

Parameters: <1-4094> the specific VLAN ID; X:X::X:X the specific group address.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

Switch#clear ipv6 mld snooping vlan 1 groups

Relative Command: show ipv6 mld snooping vlan <1-4094>

13.8.8.2 clear ipv6 mld snooping vlan <1-4094> mrouter-port

Command: clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet IFNAME|IFNAME]

Function: Delete the mrouter port of the specific VLAN.

Parameters: <1-4094> the specific VLAN ID; ethernet the Ethernet port name; IFNAME the port name.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete the mrouter port in vlan 1.

Switch# clear ipv6 mld snooping vlan 1 mrouter-port

Relative Command: show ipv6 mld snooping mrouter-port

13.8.8.3 debug mld snooping all/packet/event/timer/mfc

Command: debug mld snooping all/packet/event/timer/mfc

no debug mld snooping all/packet/event/timer/mfc

Function: Enable the debugging of the switch MLD Snooping; the "no" form of this command disables the debugging.

Command Mode: Admin Mode

Default: The MLD Snooping Debugging of the switch is disabled by default

Usage Guide: This command is used for enabling the switch MLD Snooping debugging, which displays the MLD data packet message processed by the switch——packet, event messages——event, timer messages——timer,messages of down streamed hardware entry——mfc,all debug messages——all.

13.8.8.4 ipv6 mld snooping

Command: ipv6 mld snooping

no ipv6 mld snooping

Function: Enable the MLD Snooping function on the switch; the "**no ipv6 mld snooping**"

command disables MLD Snooping.
Command Mode: Global Mode
Default: MLD Snooping disabled on the switch by default
Usage Guide: Enable global MLD Snooping on the switch, namely allow every VLAN to be configured with MLD Snooping; the "no" form of this command will disable MLD Snooping on all the VLANs as well as the global MLD snooping
Example: Enable MLD Snooping under global mode.
Switch (config)#ipv6 mld snooping

13.8.8.5 ipv6 mld snooping vlan

Command: ipv6 mld snooping vlan *<vlan-id>*
no ipv6 mld snooping vlan *<vlan-id>*
Function: Enable MLD Snooping on specified VLAN; the "no" form of this command disables MLD Snooping on specified VLAN.
Parameter: ***<vlan-id>*** is the id number of the VLAN, with a valid range of <1-4094>.
Command Mode: Global Mode
Default: MLD Snooping disabled on VLAN by default
Usage Guide: To configure MLD snooping on certain VLAN, the global MLD snooping should be first enabled. Disable MLD snooping on specified VLAN with the no ipv6 mld snooping vlan vid command
Example: Enable MLD snooping on VLAN 100 under global mode.
Switch (config)#ipv6 mld snooping vlan 100

13.8.8.6 ipv6 mld snooping vlan immediately-leave

Command: ipv6 mld snooping vlan *<vlan-id>* immediately-**leave**
no ipv6 mld snooping vlan *<vlan-id>* immediately-**leave**
Function: Enable immediate-leave function of the MLD protocol in specified VLAN; the "no" form of this command disables the immediate-leave function of the MLD protocol
Parameter: ***<vlan-id>*** is the id number of specified VLAN, with valid range of <1-4094>.
Command Mode: Global Mode
Default: Disabled by default
Usage Guide: Enabling the immediate-leave function of the MLD protocol will hasten the process the port leaves one multicast group, in which the specified group query of the group will not be sent and the port will be directly deleted.
Example: Enable the MLD immediate-leave function on VLAN 100.
Switch (config)#ipv6 mld snooping vlan 100 immediately-leave

13.8.8.7 ipv6 mld snooping vlan l2-general-querier

Command: ipv6 mld snooping vlan < *vlan-id* > l2-general-querier
no ipv6 mld snooping vlan < *vlan-id* > l2-general-querier

Function: Set the VLAN to Level 2 general querier.

Parameter: ***vlan-id***: is the id number of the VLAN, with a valid range of <1-4094>

Command Mode: Global Mode

Default: VLAN is not a MLD Snooping L2 general querier by default.

Usage Guide: It is recommended to configure an L2 general querier on a segment. If before configure with this command, MLD snooping is not enabled on this VLAN, this command will no be executed. When disabling the L2 general querier function, MLD snooping will not be disabled along with it. Main function of this command is sending general queries periodically to help the switches within this segment learn mrouter port.

Comment: There are three ways to learn mrouter port in MLD Snooping:

1. The port which receives MLD query messages
2. The port which receives multicast protocol packets and support PIM
3. The port statically configured.

Example: Set VLAN 100 to L2 general querier.

Switch (config)# ipv6 mld snooping vlan 100 l2-general-querier

13.8.8.8 ipv6 mld snooping vlan limit

Command: ipv6 mld snooping vlan < *vlan-id* > limit {group <*g_limit*> | source <*s_limit*>}

no ipv6 mld snooping vlan < *vlan-id* > limit

Function: Configure number of groups the MLD snooping can join and the maximum number of sources in each group.

Parameter: ***vlan-id*:** VLAN ID, the valid range is <1-4094>

g_limit: <1-65535>, max number of groups joined

s_limit: <1-65535>, max number of source entries in each group, consisting of include source and exclude source

Command Mode: Global Mode

Default: Maximum 50 groups by default, with each group capable with 40 source entries.

Usage Guide: When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, MLD snooping must be enabled on VLAN. The “no” form of this command restores the default other than set to “no limit”. For the safety considerations, this command will not be configured to “no limit”. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example: Switch(config)#ipv6 mld snooping vlan 2 limit group 300

13.8.8.9 ipv6 mld snooping vlan mrouter-port interface

Command: ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface [<*ethernet*>|<*port-channel*>] <*ifname*>

no ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface [<*ethernet*>|<*port-channel*>] <*ifname*>

Function: Set the static mrouter port of the VLAN; the “no” form of this command cancels the

configuration.

Parameter: *vlan-id*: VLAN id, the valid range is<1-4094>

***Ehternet*:** name of Ethernet port

***Ifname*:** Name of interface

***port-channel*:** port aggregate

Command Mode: Global Mode

Default: When a port is made static and dynamic mrouter port at the same time, it's the static mrouter properties is preferred. Deleting the static mrouter port can only be done with the "no" form of this command.

Example: Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/0/13

13.8.8.10 ipv6 mld snooping vlan mrouter-port learnpim6

Command: ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6

no ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6

Function: Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets), the no command will disable the function.

Parameter: <*vlan-id*>: The specified VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode

Default: Enable

Usage Guide: Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets). After a port received pimv6 packets, it will be set to mrouter port for implementing the automatic learning.

Example: Disable the function that vlan 100 learns mrouter-port (according to pimv6 packets).

Switch(config)#no ipv6 mld snooping vlan 100 mrouter-port learnpim6

13.8.8.11 ipv6 mld snooping vlan mrpt

Command: ipv6 mld snooping vlan <*vlan-id*> mrpt <*value*>

no ipv6 mld snooping vlan <*vlan-id*> mrpt

Function: Configure the keep-alive time of the mrouter port.

Parameter: *vlan-id*: VLAN ID, the valid range is <1-4094>

***value*:** mrouter port keep-alive time with a valid range of <1-65535> secs.

Command Mode: Global Mode

Default: 255s

Usage Guide: This configuration is applicable on dynamic mrouter port, but not on static mrouter port. To use this command, MLD snooping must be enabled on the VLAN.

Example: Switch(config)#ipv6 mld snooping vlan 2 mrpt 100

13.8.8.12 ipv6 mld snooping vlan query-interval

Command: ipv6 mld snooping vlan <*vlan-id*> query-interval <*value*>

no ipv6 mld snooping vlan <*vlan-id*> query-interval

Function: Configure the query interval.

Parameter: ***vlan-id*****:** VLAN ID, the valid range is <1-4094>

value**:** query interval, valid range: <1-65535>secs.

Command Mode: Global Mode

Default: 125s

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

Switch(config)#ipv6 mld snooping vlan 2 query-interval 130

13.8.8.13 ipv6 mld snooping vlan query-mrsp

Command: ipv6 mld snooping vlan <*vlan-id*> query-mrsp <*value*>

no ipv6 mld snooping vlan <*vlan-id*> query-mrsp

Function: Configure the maximum query response period. The "no" form of this command restores the default value.

Parameter: ***vlan-id*****:** VLAN ID, the valid range is<1-4094>

value**:** the valid range is <1-25> secs .

Command Mode: Global Mode

Default: 10s

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18

13.8.8.14 ipv6 mld snooping vlan query-robustness

Command: ipv6 mld snooping vlan <vlan-id> query-robustness <*value*>

no ipv6 mld snooping vlan <vlan-id> query-robustness

Function: Configure the query robustness; the "no" form of this command restores to the default value.

Parameter: ***vlan-id*****:** VLAN ID, the valid range is <1-4094>

value**:** the valid range is <2-10>.

Command Mode: Global Mode

Default: 2

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

Switch(config)#ipv6 mld snooping vlan 2 query- robustness 3

13.8.8.15 ipv6 mld snooping vlan static-group

Command: ipv6 mld snooping vlan<vlan-id> static-group <X:X::X:X> [source< X:X::X:X>]

interface [ethernet | port-channel] <IFNAME>

no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source< X:X::X:X>]

interface [ethernet | port-channel] <IFNAME>

Function: Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.

Parameter: ***vlan-id***: ranging between <1-4094>

X:X::X:X:The address of group or source.

ethernet: Name of Ethernet port

port-channel: Port aggregation

ifname: Name of interface

Command Mode: Global mode

Default: No configuration by default.

Usage Guide: When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.

Example:

Switch(config)#ip igmp snooping vlan 1 static-group ff1e::15 source 2000::1 interface ethernet 1/0/1

13.8.8.16 ipv6 mld snooping vlan suppression-query-time

Command: ipv6 mld snooping vlan <*vlan-id*> suppression-query-time <*value*>

no ipv6 mld snooping vlan <*vlan-id*> suppression-query-time

Function: Configure the suppression query time; the "no" form of this command restores the default value.

Parameter: ***vlan-id*****:** VLAN ID, valid range: <1-4094>

value**:** valid range: <1-65535>secs.

Command Mode: Global Mode

Default: 255s

Usage Guide: This command can only be configured on L2 general querier. The Suppression-query-time represents the period the suppression state maintains when general querier receives queries from layer 3 MLD within the segment. To use this command, the query-intervals in different switches within the same segment must be in accordance. It is recommended to use the default value.

Example:

Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270

13.8.8.17 show ipv6 mld snooping

Command: show ipv6 mld snooping [vlan <*vlan-id*>]

Parameter: <*vlan-id*> is the number of VLAN specified to display the MLD Snooping messages

Command Mode: Admin Mode

Usage Guide: If no VLAN number is specified, it will show whether the global MLD snooping is enabled and layer 3 multicast protocol is running, as well as on which VLAN the MLD Snooping is

enabled and configured l2-general-querier. If a VLAN number is specified, the detailed MLD Snooping messages of this VLAN will be displayed.

Example:

1. Summary of the switch MLD snooping

```
Switch(config)#show ipv6 mld snooping
Global mld snooping status:    Enabled
L3 multicasting:                running
Mld snooping is turned on for vlan 1(querier)
Mld snooping is turned on for vlan 2
--------------------------------
```

Displayed Information	Explanation
Global mld snooping status	Whether or not the global MLD Snooping is enabled on the switch
L3 multicasting	Whether or not the layer 3 multicast protocol is running on the switch.
Mld snooping is turned on for vlan 1(querier)	On which VLAN of the switch is enabled MLD Snooping, if the VLAN are l2-general-querier.

2. Display the detailed MLD Snooping information of vlan1

```
Switch#show ipv6 mld snooping vlan 1
Mld snooping information for vlan 1

Mld snooping L2 general querier                  :Yes(COULD_QUERY)
Mld snooping query-interval                      :125(s)
Mld snooping max reponse time                    :10(s)
Mld snooping robustness                          :2
Mld snooping mrouter port keep-alive time        :255(s)
Mld snooping query-suppression time              :255(s)

MLD Snooping Connect Group Membership
Note:*-All Source, (S)- Include Source, [S]-Exclude Source
Groups          Sources          Ports              Exptime    System Level
Ff1e::15        (2000::1)        Ethernet1/0/8      00:04:14   V2
                (2000::2)        Ethernet1/0/8      00:04:14   V2

Mld snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/0/2
```

Displayed information	Explanation
Mld snooping L2 general querier	whether or not l2-general-querier is enabled on VLAN, the querier display status is set to could-query or suppressed
Mld snooping query-interval	Query interval time of the VLAN

Mld snooping max reponse time	Max response time of this VLAN
Mld snooping robustness	Robustness configured on the VLAN
Mld snooping mrouter port keep-alive time	Keep-alive time of the dynamic mrouter on this VLAN
Mld snooping query-suppression time	timeout of the VLAN as l2-general-querier at suppressed status.
MLD Snooping Connect Group Membership	Group membership of the VLAN, namely the correspondence between the port and （S,G）.
Mld snooping vlan 1 mrouter port	Mrouter port of the VLAN, including both static and dynamic.

13.9 IPv6 Security RA

13.9.1 ipv6 security-ra enable

Command: ipv6 security-ra enable

no ipv6 security-ra enable

Function: Globally enable IPv6 security RA function, all the RA advertisement messages will not be forwarded through hardware, but only sent to CPU to handle. The no operation of this command will globally disable IPv6 security RA function.

Parameters: None.

Command Mode: Global Configuration Mode.

Default: The IPv6 security RA function is disabled by default.

Usage Guide: Only after enabling the global security RA function, the security RA on a port can be enabled. Globally disabling security RA will clear all the configured security RA ports. The global security RA function and the global IPv6 SAVI function are mutually exclusive, so they can not be enabled at the same time.

Example: Globally enable IPv6 security RA.

Switch(config)#ipv6 security-ra enable

13.9.2 ipv6 security-ra enable

Command: ipv6 security-ra enable

no ipv6 security-ra enable

Function: Enable IPv6 security RA on a port, causing this port not to forward the received RA message. The **no ipv6 security-ra enable** will disable the IPv6 security RA on a port.

Parameters: None.

Command Mode: Port Configuration Mode.
Default: IPv6 security RA function is disabled by default.
Usage Guide: Only after globally enabling the security RA function, can the security RA on a port be enabled. Globally disabling security RA will clear all the configured security RA ports.
Example: Enable IPv6 security RA on a port.
Switch(Config-If-Ethernet1/0/2)#ipv6 security-ra enable

13.9.3 show ipv6 security-ra

Command: show ipv6 security-ra [interface *<interface-list>*]
Function: Display all the interfaces with IPv6 RA function enabled.
Parameters: No parameter will display all distrust ports, entering a parameter will display the corresponding distrust port.
Command Mode: Admin and Configuration Mode.
Example:
Switch# show ipv6 security-ra
IPv6 security ra config and state information in the switch
Global IPv6 Security RA State: Enable
Ethernet1/0/1
IPv6 Security RA State: Yes
Ethernet1/0/3
IPv6 Security RA State: Yes

13.9.4 debug ipv6 security-ra

Command: debug ipv6 security-ra
no debug ipv6 security-ra
Function: Enable the debug information of IPv6 security RA; the no operation of this command will disable the debug information of IPv6 security RA.
Command Mode: Admin Mode.
Parameters: None.
Usage Guide: Users can check the proceeds of message handling of IPv6 security RA, which will help investigate the causes to problems if there is any.
Example: Enable the debug information of IPv6 security RA.
Switch#debug ipv security-ra

13.10 SAVI

13.10.1 Commands for SAVI

13.10.1.1 ipv6 cps prefix

Command: ipv6 cps prefix *<ipv6-address>* vlan *<vid>*

no ipv6 cps prefix*<ipv6-address>*

Function: Configure IPv6 address prefix of the link manually, no command deletes IPv6 address prefix.

Parameter: ipv6-address: the address prefix of link, like 2001::/64;

vid: vlan ID of the current link.

Command Mode: Global Mode.

Default: None.

Usage Guide: Users should configure local address prefix: fe80::/64 of the link before enable the function of matching address prefix of the link, it accepts the packets of which source addresses are the local addresses of the link.

Example: Configure the address prefix of the link to 2001::/64.

Switch(config)#ipv6 cps prefix 2001::/64 vlan 2

13.10.1.2 ipv6 cps prefix check enable

Command: ipv6 cps prefix check enable

no ipv6 cps prefix check enable

Function: Enable SAVI address prefix check function, no command will disable this function.

Parameter: None.

Command Mode: Global Mode.

Default: Disable SAVI address prefix check function.

Usage Guide: After enable the prefix check function, if the IPv6 address prefix of the packets does not accord with the link prefix, then do not establish the corresponding IPv6 address binding. If users enable the matched address prefix of the link, configure the local address prefix of fe80::/64 first to accept the packets with the source address as local link address. Disable address prefix check function by default.

Example: Enable SAVI address prefix check function.

Switch(config)#ipv6 cps prefix check enable

13.10.1.3 ipv6 dhcp snooping trust

Command: ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

Function: Configure the port as dhcpv6 trust port, it does not establish dynamic DHCPv6 binding again and allows all DHCPv6 protocol packets to pass; no command deletes the port trust function.

Parameter: None.

Command Mode: Port Mode.

Default: Disable.

Usage Guide: Set the port as dhcpv6 trust attribute, enable uplink port of the switch with SAVI

function for connecting dhcpv6 server or dhcpv6 relay generally.

Example: Set ethernet1/0/1 to be DHCP trust port.

Switch(config)#interface ethernet1/0/1

Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust

13.10.1.4 ipv6 nd snooping trust

Command: ipv6 nd snooping trust

no ipv6 nd snooping trust

Function: Configure the port as slaac trust and RA trust port, this port will not establish dynamic slaac binding any more and forwards RA packets. The no command deletes the port trust function.

Parameter: None.

Command Mode: Port Mode.

Default: Disable port trust function.

Usage Guide: If the port disables ipv6 nd snooping trust function, it is considered to untrust RA packets port and discards all RA packets. Setting the port as trust attribute, enable the uplink port of the switch with SAVI or the conjoint port between switches with SAVI generally.

Example: Set the port ethernet1/0/1 to be nd trust port.

Switch(config)#interface ethernet1/0/1

Switch(config-if-etherne1/0/1)#ipv6 nd snooping trust

13.10.1.5 savi check binding

Command: savi check binding <*simple | probe*> mode

no savi check binding mode

Function: Configure the check mode for conflict binding, the no command deletes the check mode.

Parameter: simple mode: only check the port state for conflict binding, if the state is up, keep the conflict binding and do not set new binding. If the state is down, delete the conflict binding to set a new one

probe mode: besides checking the port state for conflict binding, it will send NS packets to probe the usability of the corresponding user when the port state is up. If receiving the responded NA packets from users, it will keep the current conflict binding and does not set new binding, otherwise delete the conflict binding to set new one.

Command Mode: Global Mode.

Default: Disable the conflict binding check mode by default. It will adopt the mode that delete the conflict binding directly to set new one.

Usage Guide: It is recommended to configure probe mode to prevent the attack that the spurious address conflict binding deletes the legal user binding.

Example: Configure the conflict binding check mode to probe mode.

Switch(config)#savi check binding probe mode

13.10.1.6 savi enable

Command: savi enable

no savi enable

Function: Enable the global SAVI function, the no command disables this global function.

Parameter: None.

Command Mode: Global Mode.

Default: Disable the global SAVI function.

Usage Guide: Command configuration can be processed for SAVI function after enabling the global SAVI function. Because SAVI function has already contained security RA function, global SAVI function and security RA function are mutually exclusive in the global mode.

Example: Enable SAVI function.

Switch(config)#savi enable

13.10.1.7 savi ipv6 binding num

Command: savi ipv6 binding num <*limit-num*>

no savi ipv6 binding num

Function: Configure the number of the corresponding binding with the port, no command restores the default value.

Parameter: limit-num: set the range from 0 to 100, the default value of the port binding number is 100.

Command Mode: Port Mode.

Default: 100.

Usage Guide: The configured binding number only include the dynamic binding type of slaac, dhcp. If the binding sum exceeds the configured number, this port does not create new dynamic binding any more, if the configured number is 0, this port does not create any dynamic binding.

Example: Configure the binding number to be 100 for port ethernet1/0/1.

Switch(config)#interface ethernet1/0/1

Switch(config-if-ethernet1/0/1)# savi ipv6 binding num 100

13.10.1.8 savi ipv6 check source binding

Command: savi ipv6 check source binding ip <*ip-address*> mac <*mac-address*> interface <*if-name*> {type [slaac | dhcp] lifetime <*lifetime*> | type static}

no savi ipv6 check source binding ip <*ip-address*> interface <*if-name*>

Function: Configure the static or dynamic binding function manually; the no command deletes the configured binding.

Parameter: ip-address: is the unicast IPv6 address, including local link and global unicast address

mac-address: is the mac address of Ethernet

if-name: is the port name, like interface ethernet 1/0/1

slaac|dhcp: slaac means create the dynamic binding for slaac type, **dhcp** means

create the dynamic binding for dhcp type

lifetime: configure the lifetime period for the dynamic binding, the unit is second.

static: create the binding of the static type.

Command Mode: Global Mode.

Default: None.

Usage Guide: After the dynamic binding configured by handwork is overtime, the corresponding binding will be deleted but the configuration is still be kept, so the binding still be shown. If the binding needs to take effect again, it should delete it first and configure a new binding again.

When the binding type is static type, do not configure lifetime period, the lifetime period is infinite.

Example: Configure the dynamic binding of slaac type for SAVI manually.

Switch(config)#savi ipv6 check source binding ip 2001::10 mac 00-25-64-BB-8F-04 Interface ethernet1/0/1 type slaac lifetime 2010

Configure the static binding for SAVI manually.

Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-04
Interface ethernet1/0/1 type static

13.10.1.9 savi ipv6 check source ip-address mac-address

Command: savi ipv6 check source [ip-address mac-address | ip-address | mac-address]

no savi ipv6 check source

Function: Enable the control authentication function for the packets of the port, no command disables this function.

Parameter: None.

Command Mode: Port Mode.

Default: Disable the control filtering function of the port.

Usage Guide: The global SAVI function must be enabled before configuring this command.

Example: Enable the control filtering function of the packets on port ethernet1/0/1.

Switch(config)#interface ethernet1/0/1
Switch(config-if-ethernet1/0/1)# savi ipv6 check source ip-address mac-address

13.10.1.10 savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Command: savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

no savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Function: Enable SAVI application scene function, no command disables the function.

Parameter: dhcp-only: dhcp-only application scene

slaac-only: slaac-only application scene

dhcp-slaac: combination application scene of dhcp-only and slaac-only

Command Mode: Global Mode.

Default: Disable SAVI application scene.

Usage Guide: dhcp-only application scene only detects DHCPv6 packets and DAD NS packets of link-local ipv6 address to be IPv6 address with target field, it does not detect DAD NS packets of non-link-local address. slaac-only application scene detects DAD NS packets of all types. dhcp-slaac combination application scene detects all DHCPv6 and DAD NS packets. Disable all kinds of application scene detection function for SAVI by default.

Example: Enable the specified dhcp-only application scene for SAVI.

Switch(config)#savi ipv6 dhcp-only enable

13.10.1.11 savi ipv6 mac-binding-limit

Command: savi ipv6 mac-binding-limit <*limit-num*>

no savi ipv6 mac-binding-limit

Function: Configure the dynamic binding number of the same MAC address, no command restores the default value.

Parameter: limit-num: set the ranging from 1 to 10, the default dynamic binding number is 32 for the same MAC address.

Command Mode: Global Mode.

Default: 32.

Usage Guide: This command is used to prevent the exhaust attack of the dynamic binding entry for SAVI.

Example: Set the dynamic binding number to be 5 for the same MAC address.

Switch(config)#isavi ipv6 mac-binding-limit 5

13.10.1.12 savi max-dad-dalay

Command: savi max-dad-delay *<max-dad-delay>*

no savi max-dad-delay

Function: Configure the dynamic binding at DETECTION state and send lifetime period of DAD NS packet detection, no command restores the default value.

Parameter: max-dad-delay: set the ranging between 1 and 65535 seconds, its default value is 1 second.

Command Mode: Port Mode.

Default: 1 second.

Usage Guide: It is recommended to use the default value.

Example: Set the detection lifetime as 2 seconds.

Switch(config)#savi max-dad-delay 2

13.10.1.13 savi max-dad-prepare-delay

Command: savi max-dad-prepare-delay *<max-dad-prepare-delay>*

no savi max-dad-prepare-delay

Function: Configure lifetime period of redetection for the dynamic binding, no command restores

the default value.

Parameter: max-dad-prepare-delay: set the ranging between 1 and 65535 seconds, its default value is 1 second.

Command Mode: Global Mode.

Default: 1 second.

Usage Guide: It is recommended to user the default value.

Example: Set the redetection lifetime as 2 seconds.

Switch(config)#savi max-dad-prepare-delay 2

13.10.1.14 savi max-slaac-life

Command: savi max-slaac-life *<max-slaac-life>*

no savi max-slaac-life

Function: Configure lifetime period of slaac dynamic binding at BOUND state, no command restores the default value.

Parameter: max-slaac-life: set the ranging between 1 and 31536000 seconds, its default value is 4 hours.

Command Mode: Global Mode.

Default: 4 hours.

Usage Guide: None.

Example: Configure lifetime period of slaac binding type as 2010 seconds at BOUND state.

Switch(config)#savi max-slaac-life 2010

13.10.1.15 savi timeout bind-protect

Command: savi timeout bind-protect *<protect-time>*

no savi timeout bind-protect

Function: Configure the bind-protect lifetime period for a port after its state from up to down, no command restores the default value.

Parameter: protect-time: set the ranging between 1 and 300 seconds, its default value is 30 seconds.

Command Mode: Global Mode.

Default: 30 seconds.

Usage Guide: After the configured lifetime period is overtime, the port is still at down state, the binding of this port will be deleted. If the port state is changed from down to up state during the configured lifetime period, the binding of the port will reset it as lifetime period of BOUND state. If the configured parameter is 0 second, all binding of the port will be deleted immediately.

Example: Set bind-protect lifetime period to be 20 seconds.

Switch(config)#savi timeout bind-protect 20

13.10.2 Commands for Monitor and Debug

13.10.2.1 Monitor and Debugg

13.10.2.1.1 debug ipv6 dhcp snooping binding

Command: debug ipv6 dhcp snooping binding

no debug ipv6 dhcp snooping binding

Function: Enable binding debug of dhcp type for SAVI, no command disables the debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable this function, the relative binding of dhcp type or static type create the print information for misarranging. The no command disables this function.

Example: Enable the binding debug of dhcp type.

Switch#debug ipv6 dhcp snooping binding

13.10.2.1.2 debug ipv6 dhcp snooping event

Command: debug ipv6 dhcp snooping event

no debug ipv6 dhcp snooping event

Function: Enable event debug of dhcp type for SAVI, no command disables the debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable event debug, the relative event information of dhcp type will be print for misarranging. The no command disables this function.

Example: Enable binding event debug of dhcp type.

Switch#debug ipv6 dhcp snooping event

13.10.2.1.3 debug ipv6 dhcp snooping packet

Command: debug ipv6 dhcp snooping packet

no debug ipv6 dhcp snooping packet

Function: Enable the debug of DHCPv6 packets, no command disables the debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable packets debug, the relative DHCPv6 packtets will be print for misarranging. The no command disables this function.

Example: Enable the debug of DHCPv6 packets.

Switch#debug ipv6 dhcp snooping packet

13.10.2.1.4 debug ipv6 nd snooping binding

Command: debug ipv6 nd snooping binding

no debug ipv6 nd snooping binding

Function: Enable the binding debug of slaac type for SAVI, no command disables the binding debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable binding debug, the relative binding of slaac type will create the print information for misarranging. The no command disables this function.

Example: Enable binding debug of slaac type.

Switch#debug ipv6 nd snooping binding

13.10.2.1.5 debug ipv6 nd snooping event

Command: debug ipv6 nd snooping event

no debug ipv6 nd snooping event

Function: Enable the event debug of slaac type for SAVI, no command disables the event debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable event debug, the relative event information of slaac type will be print for misarranging. The no command disables this function.

Example: Enable the event debug of slaac type.

Switch#debug ipv6 nd snooping event

13.10.2.1.6 debug ipv6 nd snooping packet

Command: debug ipv6 nd snooping packet

no debug ipv6 nd snooping packet

Function: Enable ND packets debug, no command disables ND packets debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable packets debug, the relative ND packets will be print for misarranging. The no command disables this function.

Example: Enable ND packets debug.

Switch#debug ipv6 nd snooping packet

13.10.2.1.7 show savi ipv6 check source binding

Command: show savi ipv6 check source binding [interface<*if-name*>]

Function: Show the global SAVI binding entry list.

Parameter: if-name: port name such as interface ethernet 1/0/1.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Descriptions of each field are as below:

Field	Description
MAC	The bound MAC address
IP	The bound IP address
Vlan	The binding VLAN belongs to
Port	The binding port belongs to
Type	Binding type
State	Binding state
Expires	The bound lifetime period

Example: Show the global binding state of SAVI.

Switch(config)#show savi ipv6 check source binding

Static binding count: 0

Dynamic binding count: 3

Binding count: 3

MAC	IP	VLAN	Port	Type	State	Expires
00-25-64-bb-8f-04	fe80::225:64ff:febb:8f04	1	Ethernet1/0/5	slaac	BOUND	14370
00-25-64-bb-8f-04	2001::13	1	Ethernet1/0/5	slaac	BOUND	14370
00-25-64-bb-8f-04	2001::10	1	Ethernet1/0/5	slaac	BOUND	14370

13.11 IPv6 VRRPv3

13.11.1 advertisement-interval

Command: advertisement-interval <*adver_interval*>

Function: Configure the advertisement interval of VRRPv3.

Parameters: ***<adver_interval>*** is the interval of sending VRRPv3 advertisement messages, in centiseconds, ranging from 100 to 1000, and has to be a multiple of 100.

Command Mode: VRRPv3 Protocol Mode.

Default: <*adver_interval*> is 100 centiseconds (1 second) by default.

Usage Guide: The Master in a VRRPv3 backup group will send a VRRPv3 message to notify other routers (layer-three switches) in the group that it is working normally at intervals. This interval is ***adver_interval***. If the Backup hasn't received any VRRPv3 message from Master over a certain

period of time (the length of the time is ***master_down_interval***), it will assume that the master is not working normally and will change the state of itself to Master.

Uses can use this command to adjust the interval of VRRPv3 advertisement messages sent by Master. For the members in the same backup group, this attribute should have same value. For Backup, the value of its ***master_down_interval*** should be three times more than *adver_interval*. If the network flow is too big or different routers (or layer-three switches) have different timers, ***master_down_interval*** might has a time-out, which will cause a state change as a result. This kind of situation can be solved by prolonging ***adver_interval*** or setting a longer preempts delay time.

Example: Configure the VRRPv3 advertisement interval as 300 centiseconds.

Switch(config-router)# advertisement-interval 300

13.11.2 circuit-failover

Commands: circuit-failover {vlan<*ID*>| *IFNAME*} <*value_reduced*>

no circuit-failover

Function: Configures the VRRPv3 monitor interface.

Parameters: {vlan<*ID*>| *IFNAME*} is the name for the interface to be monitored.

<*value_reduced*> stands for the amount of priority decreased, the range value is from 1 to 253.

Command mode: VRRPv3 Protocol Configuration Mode.

Default: Not configured by default.

Usage Guide: The interface monitor function is a valuable extension to backup function, which not only enable VRRPV3 to provide backup function on router (or L3 Ethernet switch) fail, but also allow decreasing the priority of a router (or L3 Ethernet switch) to ensure smooth implementation of backup function when status of that network interface is **down**.

When this command is used, if the status of an interface monitored turns from **up** to **down**, then the priority of that very router (or L3 Ethernet switch) in its Standby cluster will decrease (If the priority of that value_reduced is higher than interface configuration, then the corresponding router is **down**, the priority of interface in Backup decrease until 0), lest Backup cannot changes its status due to lower priority than the Master when the Master fails. After the interface monitored turns up over again, the priority of corresponding router (or L3 Ethernet switch) will restore in Backup.

Example: Configuring VRRPv3 monitor interface to VLAN 2 and decreasing amount of priority to 10.

Switch(Config-router)# circuit-failover vlan 2 10

13.11.3 debug ipv6 vrrp

Command: debug ipv6 vrrp [all | events | packet [recv | send]]

no debug ipv6 vrrp [all | events | packet [recv | send]]

Function: Display the state change, message receiving and sending of a VRRPv3 backup group, the no operation of this command will disable the display of DEBUG.

Parameters: None.

Command Mode: Admin Mode.

Example:

Switch#debug ipv6 vrrp

Jan 01 01:03:13 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]

Jan 01 01:03:14 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]

Jan 01 01:03:15 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]

13.11.4 disable

Command: disable
Function: Disable VRRPv3 virtual router.
Parameters: None.
Command Mode: VRRPv3 Protocol Mode.
Default: There is no configuration by default.
Usage Guide: Disable the corresponding virtual router session. Only after disabling the virtual router, can the relative configuration parameters be changed.
Examples: Disable the VRRPv3 virtual router whose ID is 10.
Switch(config)#router ipv6 vrrp 10
Switch(config-router)#disable

13.11.5 enable

Command: enable
Function: Enable VRRPv3 virtual router.
Parameters: None.
Command Mode: VRRPv3 Protocol Mode.
Default: There is no configuration by default.
Usage Guide: Start the corresponding virtual router session. Only the interface of the enabled router (or the layer-three switch) can actually join the backup group. Before enabling the virtual router, the virtual IPv6 address and interface of VRRPv3 should be configured.
Example: Enable the VRRPv3 virtual router whose ID is 10.
Switch(config)#router ipv6 vrrp 10
Switch(config-router)#enable

13.11.6 preempt-mode

Command: preempt-mode {true | false}
Function: Configure the preempt mode of VRRPv3.
Parameters: None.
Command Mode: VRRPv3 Protocol Mode.
Default: It is preempt mode by default.

Usage Guide: If it is needed that a router (or a layer-three switch) with higher priority can the role of master router, the preempt mode needs to be configured.
Example: Configure VRRPv3 as non-preempt mode.
Switch(config-router)# preempt-mode false

13.11.7 priority

Command: priority <*value*>
Function: Configure the priority of VRRPv3.
Parameters: <*value*> is the priority, whose range is from 1 to 254.
Command Mode: VRRPv3 Protocol Mode.
Default: Backup routers (or layer-three switches) all have a priority of 100, the priority of IP address owners are all 255 in the backup group they belong to.
Usage Guide: Priority decides the state of a router (or a layer-three Ethernet switch) in a backup group. The higher the priority is, the more possible the router can be a Master. The configurable priority ranges from 1 to 254, while the priority of 255 is reserved to the IP address owner. The priority of 0 has special usage, which is when disabling a VRRP session, Master will send an advertisement message with a priority of 0. When Backup receives such advertisement message, it will start a new round of Master selection. When there are two or more routers (or layer-three switches) in one backup group have the same priority, the router with biggest local link IPv6 address has higher priority.
Example: Configure the priority of VRRPv3 as 150.
Switch(config-router)# priority 150

13.11.8 router ipv6 vrrp

Command: router ipv6 vrrp <*vrid*>
no router ipv6 vrrp <*vrid*>
Function: Create or delete a VRRPv3 virtual router.
Parameters: <*vrid*> is the ID of the virtual router, the valid range is 1 to 255.
Command Mode: Global Mode.
Default: There is no configuration by default.
Usage Guide: This command is used to create or delete a VRRPv3 virtual router. The virtual router is uniquely specified by the virtual router ID and the related virtual IPv6 address. Only after creating a virtual router, relative configuration can be set on it. Considering the stability, the number of configurable virtual routers should not be more than 64.
Example: Configure a virtual router whose ID is10.
Switch(config)# router ipv6 vrrp 10

13.11.9 show ipv6 vrrp

Command: show ipv6 vrrp [<*vrid*>]
Function: Display the state and configuration information of VRRPv3 backup group.

Parameters: ***<vrid>***is the ID of the virtual router, whose range is from 1 to 255, no parameter means to display the state and configuration infomation of all backup gorups.

Command Mode: Admin and Configuration Mode.

Example:

```
Switch# show ipv6 vrrp
VrId 1
  State is Master
  Virtual IPv6 is fe80::2 (Not IPv6 owner)
  Interface is Vlan1
  Configured priority is 150, Current priority is 150
  Advertisement interval is 100 centisec
  Preempt mode is TRUE
  Circuit failover interface Vlan1, Priority Delta 3, Status UP
VrId 10
  State is Initialize
  Virtual IPv6 is fe80::3 (Not IPv6 owner)
  Interface is Vlan2
  Priority is 100
  Advertisement interval is 300 centisec
  Preempt mode is TRUE
  Circuit failover interface Vlan2, Priority Delta 10, Status UP
```

Display	Explanation
State	State.
Virtual IPv6	Virtual IPv6 address.
Interface	Interface name.
Priority	Priority.
Advertisement interval	The interval of VRRPv3 advertisement messages.
Preempt	Preempt mode.
Circuit failover interface	Monitor interface information.

13.11.10 virtual-ipv6 interface

Command: virtual-ipv6 <*ipv6-address*> interface {Vlan <*ID*>| *IFNAM*E}

no virtual-ipv6 interface

Function: Configure the virtual IPv6 address and interface of VRRPv3.

Parameters: <*ipv6-address*>is the virtual IPv6 address, which has to be an IPv6 local link address.

{Vlan <*ID*>| *IFNAM*E} is the interface name.

Command Mode: VRRPv3 Protocol Mode.

Default: There is no configuration by default.

Usage Guide: This command is used to add an IPv6 address and interface to an existing backup group. The no operation of this command will delete the virtual IPv6 address and interface of the

specified backup group. The virtual IPv6 address is the link local unicast address. There can only be one virtual IPv6 address in a backup group. In order to avoid the fault of returning physical MAC address when Ping virtual IPv6 address, it is regulated that the virtual IPv6 address should not be the real IPv6 address of the interface. Thus, the interfaces of all VRRPv3 backup groups are Backup by default, and need to select a Master within the backup groups.

Example: Configure the virtual IPv6 address of the backup group as fe80::2, the interface is VLAN1.

Switch(config-router)# virtual-ipv6 fe80::2 interface vlan 1

Chapter 14 Commands for vpn

14.1 MPLS

14.1.1 mpls egress-ttl

Command: mpls egress-ttl <*0-255*>

no mpls egress-ttl

Function: Set the TTL value of IP messages through the egress LSR of LSP; the no operation will cancel the configured value.

Parameters: <*0-255*>: the TTL value.

Default: None.

Command Mode: Global Mode

Usage Guide: The egress-ttl configuration of the LSR will be the TTL of all IP messages forwarded through this egress LSR.

Example: Set the egress TTL as 45.

Switch#config terminal

Switch(config)#mpls egress-ttl 45

Related Commands: mpls ingress-ttl

14.1.2 mpls enable

Command: mpls enable

no mpls enable

Function: Enable mpls protocol; the no command will disable the protocol.

Parameters: None.

Default: The mpls protocol is disabled by default.

Command Mode: Global Mode.

Usage Guide: Implementing this command will enable the mpls protocol.

Example:

Switch(config)#mpls enable

14.1.3 mpls ingress-ttl

Command: mpls ingress-ttl <*0-255*>

no mpls ingress-ttl

Function: Set the TTL value of IP messages through the ingress LSR of LSP; the no operation will cancel the configured value.

Parameters: <*0-255*>: the TTL value.

Default: None.

Command Mode: Global Mode
Usage Guide: The ingress-ttl configuration of the ingress LSR will be the TTL value in the top label of all MPLS messages entering this LSP through the LSP ingress router.
Example: Set the ingress TTL as 45.
Switch#config terminal
Switch(config)#mpls ingress-ttl 45
Related Commands: mpls egress-ttl

14.1.4 mpls local-packet-handling

Command: mpls local-packet-handling
no mpls local-packet-handling
Function: Supporting mpls local transfer.
Parameters: None.
Default: No support of mpls local transfer.
Command Mode: Global mode.
Usage Guide: Supporting mpls local transfer after configure this command. It means the local sent flow will use mpls.
Example:
Switch(config)#mpls local-packet-handling

14.1.5 mpls mtu

Command: mpls mtu <64-2000>
no mpls mtu
Function: Configure the mpls mtu value.
Command Mode: Interface Configuration Mode.
Usage Guide: 1500.
Example: Configure the mpls mtu value as 1400.
Switch(config-if-vlan1)#mpls mtu 1400

14.1.6 show mpls

Command: show mpls
Function: Display all label data.
Parameters: None.
Default: None.
Command Mode: Admin and Config mode.
Usage Guide: Implementing this command will display all label data.
Example: Display all label data.
Switch#show mpls
Minimum label configured: 16

Maximum label configured: 1048575
Per label-space information:
Label-space 0 is using minimum label: 16 and maximum label: 1048575
Custom ingress TTL configured: none
Custom egress TTL configured: none

Display	Explanation
Minimum label configured	The configured minimum label
Maximum label configured	The configured maximum label
Per label-space information	The space information of each label
Label-space 0 is using minimum label	The minimum label can be used by label-space 0.
Label-space 0 is using maximum label	The maximum label can be used by label-space 0.
Custom ingress TTL configured	The ingress TTL configured by users
Custom egress TTL configured	The egress TTL configured by users

14.1.7 show mpls enable

Command: show mpls enable
Function: Display whether the mpls is enabled.
Parameters: None.
Default: None.
Command Mode: Admin and Config mode.
Usage Guide: Implementing this command will display whether the mpls is enabled.
Example: Display whether the mpls is enabled.
Switch#show mpls enable
Switch#MPLS enable has been on
Related Commands: mpls enable

14.1.8 show mpls forwarding-table

Command: show mpls forwarding-table
Function: Display the information of all LSP created by the switch as an ingress router, and FTN (FEC to Next-Hop-Label-Forwarding-Entry) marked as selected.
Parameters: None.
Default: None.
Command Mode: Admin and Config mode.
Usage Guide: Implementing this command will display the information of all LSP created by the switch as an ingress router, and FTN marked as selected.
Example: Display the information of all LSP created by the switch as an ingress router.
Switch#show mpls forwarding-table
Codes: > - selected FTN, B - BGP FTN, C - CR-LDP FTN, K - CLI FTN,
L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, U - unknownnnnn FTN
Code FEC FTN-ID Pri Nexthop Out-Label Out-Intf

L>	200.200.1.2/32	1	Yes	202.200.1.1	640	Vlan3
L>	202.200.1.0/24	2	Yes	0.0.0.0	3	Vlan3
L>	202.200.2.0/24	3	Yes	202.200.1.1	3	Vlan3

Display	Explanation
Code	Type
FEC	The FEC Address
FTN-ID	The FTN ID
Pri	The Primary lsp label
Nexthop	The next-hop address
Out-Label	The Out label
Out-Intf	The Out interface

14.1.9 show mpls ftn-table brief

Command: show mpls ftn-table brief

Function: Display brief information of public network FTN routers created by MPLS on the switch.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display brief information of public network FTN routers created by MPLS on the switch.

Example:

Switch#show mpls ftn-table brief

FTN Entry Brief Information

FEC	Out-Label	Out-intf	Next hop	Oper-code	Op-State	Vrf
100.1.1.0/24	3	Vlan10	0.0.0.0	Push	Up	0

14.1.10 show mpls ftn-table detail

Command: show mpls ftn-table detail

Function: Display detailed information of public network FTN router created by MPLS on the switch.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display detailed information of public network FTN routers created by MPLS on the switch.

Example:

Switch#show mpls ftn-table detail

FTN ID : 1

VrfIndex : 0

```
Fec                 :    100.1.1.0/24
Nexthop addr        :    0.0.0.0
Owner               :    LDP
Primary             :    Yes
Row Status          :    Active
Exp-bits            :    0X0
Incoming DSCP       :    none
Tunnel ID           :    0
Protected LSP id    :    0
QoS Resource id     :    0
In-Label            :    0
In-Interface        :    N/A
Out-Label           :    3
Out-Interface       :    Vlan10
Admin Status        :    Up
Oper Status         :    Up
Oper Code           :    Push
```

Display	Explanation
FTN ID	The FEC ID
VrfIndex	The Vrf Index
Fec	The Fec Address
Nexthop addr	The next-hop address
Owner	The protocol creating the cross-link table
Primary	Whether it is primary or not.
Row Status	The Row status
Exp-bits	The experiment bits
Incoming DSCP	Differentiated Services CodePoint.
Tunnel ID	The Tunnel ID
Protected LSP id	The id of protected LSP
QoS Resource id	The ID of Qos Resource
in label	The in label
In-Interface	The in interface
Out-Label	The out label
Out-Interface	The out interface
Admin Status	The administration status
Oper Status	The operation status
Oper Code	The operation code

14.1.11 show mpls ilm-table

Command: show mpls ilm-table

Function: Display the information of ILM routers created by MPLS on the switch.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display the information of ILM routers created by MPLS.

Example:

Switch#show mpls ilm-table

In-Label	Out-Label	In-Intf	Out-Intf	Nexthop	FEC
640	3	Vlan1	Vlan2	24.1.1.2	2.2.2.2/32
641	3	Vlan2	Vlan1	14.1.1.1	1.1.1.1/32

Display	Explanation
In-Label	The in label
Out-Label	The out label
In-Intf	The in interface
Out-Intf	The our interface
Nexthop	The next-hop address
FEC	The fec address

14.1.12 show mpls vrf-table

Command: show mpls vrf-table [vrf-name]

Function: Display the detailed information of all configured VRP ingresses.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display the detailed information of all configured VRP ingresses. If there is a specified VRF in the parameter, only details about this ingress will be displayed.

Example:

Switch#show mpls vrf-table

Output for VRF table with id: 1

FTN ID : 1
VrfIndex : 1
Fec : 10.1.1.0/24
Nexthop addr : 0.0.0.0
Owner : BGP
Primary : Yes
Row Status : Active
Exp-bits : 0X0

Incoming DSCP : none
Tunnel ID : 0
Protected LSP id : 0
QoS Resource id : 0
In-Label : 0
In-Interface : N/A
Out-Label : 0
Out-Interface : Vlan20
Admin Status : Up
Oper Status : Up
Oper Code : Deliver to IP

Display	Explanation
FTN ID	The FEC ID
VrfIndex	The Vrf Index
Fec	The Fec address
Nexthop addr	The next-hop address
Owner	The protocol creating the cross-link table
Primary	Whether it is primary or not
Row Status	The row status
Exp-bits	The experiment bits
Incoming DSCP	Differentiated Services CodePoint.
Tunnel ID	The tunnel ID
Protected LSP id	The ID of protected LSP
QoS Resource id	The ID of Qos resource
in label	The in label
In-Interface	The in interface
Out-Label	The out label
Out-Interface	The out interface
Admin Status	The administration status
Oper Status	The operation status
Oper Code	The operation code

14.2 LDP

14.2.1 advertisement-mode

Command: advertisement-mode {downstream-on-demand | downstream-unsolicited}
no advertisement-mode {downstream-on-demand | downstream-unsolicited}

Function: Configure the advertisement mode of labels; the no operation will cancel the configuration.
Parameters: None.
Default: Downstream-unsolicited mode
Command Mode: LDP Protocol Configuration Mode.
Usage Guide: The LDP label advertisement mode determines how the LDP protocol handles the label advertisement. The protocol supports two modes: the first one is downstream-on-demand, which means, only when the upstream propose a label request, will the switch advertise a label to it; the other one is downstream-unsolicited, which means, the switch will allocate labels for all upstreams no matter they need one or not. It is recommended to use this mode together with the label retention modes and label control modes: the downstream-unsolicited mode corresponds with the liberal retention mode and the liberal mode, while the downstream-on-demand mode with the conservative retention mode and the ordered mode. It is better not to configure other attributes separately. If the interface is in the label advertisement mode, this command will have no effect.
Example: Configure the label advertisement mode as downstream-unsolicited.
Switch(config)#router ldp
Switch(config-router)#advertisement-mode downstream-on-demand
Related Commands: ldp advertisement-mode, label-retention-mode, ldp label-retention-mode

14.2.2 clear ldp adjacency

Command: clear ldp adjacency {*<ip-addr>*|*}
Function: Cancel the LDP adjacency.
Parameters: ***<ip-addr>*** is the adjacent IP address, * means to clear all adjacencies.
Default: None.
Command Mode: Admin Mode.
Usage Guide: Implementing this command will clear the adjacency between the switch and its neighbor. With all configurations staying the same, the switch will recreate an adjacency with the neighbor through negotiation.
Example: Clear the adjacency with the neighbor 10.10.10.1.
Switch#clear ldp adjacency 10.10.10.1

14.2.3 clear ldp session

Command: clear ldp session {*<ip-addr>* | *}
Function: Clear LDP sessions.
Parameters: *<ip-addr>* is the IP address of the neighbor, * means to clear all sessions.
Default: None.
Command Mode: Admin Mode
Usage Guide: Implementing this command will clear session procedures. With all configurations staying the same, the switch will restart the session again. Please pay attention to the relationship between session and adjacency: multiple adjacencies may be created in one session.

Example:
Switch#clear ldp session *

14.2.4 clear ldp statistics

Command: clear ldp statistics
Function: Clear the LDP statistics.
Parameters: None.
Default: None.
Command Mode: Admin Mode.
Usage Guide: Implementing this command will clear all statistics.
Example:
Switch#clear ldp statistics

14.2.5 control-mode

Command: control-mode {ordered | independent}
no control-mode
Function: Configure the LSP control mode; the no operation will cancel the configuration.
Parameters: None.
Default: The default mode is “independent”.
Command Mode: LDP Protocol Configuration Mode
Usage Guide: LSP provides two different control modes: independent and ordered. The independent mode means that, there is no need to acquire a label map of the FEC from the downstream, which is required in the ordered mode when a LSR is advertising to the upstream a label map related with the specified FEC (unless this LSR is the egress router of this FEC). Hop-by-hop route applications usually work in the independent LSP control mode, and choose DU mode as the label advertisement mode. The ordered mode should be used along with the DoD mode.
Example: Configure the LSPcontrol mode to ordered.
Switch(config)#router ldp
Switch(config-router)#control-mode ordered
Related Commands: advertisement-mode, ldp advertisement-mode

14.2.6 debug ldp all

Command: debug ldp all
no debug ldp all
Function: Display all debug information related with LDP; when it is disabled, all debug switches will be disabled too.
Parameters: None.
Default: No display of debug information.
Command Mode: Admin Mode.

Example: Enable all debug switches.
Switch#debug ldp all
Switch#

14.2.7 debug ldp dsm

Command: debug ldp dsm
no debug ldp dsm
Function: Display debug information related with the LDP downstream state machine; the no operation will disable the debug information.
Parameters: None.
Default: No display of debug information.
Command Mode: Admin Mode.
Usage Guide: Implementing this command will display the debug information related with the LDP downstream state machine. With it is enabled, debug information will be displayed when any the LDP protocol change related with the downstream state machine happens.
Example: Enable the debug switch.
Switch#debug ldp dsm
Switch#

14.2.8 debug ldp error

Command: debug ldp error
no debug ldp error
Function: Display debug information of LDP errors; the no operation will disable the debug information.
Parameters: None.
Default: No display of debug information.
Command Mode: Admin Mode.
Usage Guide: When there is any LDP error, corresponding debug information will be displayed with this command enabled.
Example: Enable the debug switch.
Switch# debug ldp error
Switch#

14.2.9 debug ldp events

Command: debug ldp events
no debug ldp events
Function: Display debug information of LDP events; the no operation will disable the debug information.
Parameters: None.
Default: No display of debug information.

Command Mode: Admin Mode.
Usage Guide: With this command enabled, the corresponding debug information of LDP events will be displayed.
Example: Enable the debug switch.
Switch#debug ldp events
Switch#

14.2.10 debug ldp fsm

Command: debug ldp fsm
no debug ldp fsm
Function: Display debug information related with the LDP session finite state machine; the no operation will disable the debug information.
Parameters: None.
Default: No display of debug information.
Command Mode: Admin Mode.
Usage Guide: Enable (Disable) the debug information related with the LDP session finite state machine.
Example: Enable the debug switch.
Switch#debug ldp fsm
Switch#

14.2.11 debug ldp hexdump

Command: debug ldp hexdump
no debug ldp hexdump
Function: Display the debug information of LDP messages in hex; the no operation will disable the debug information.
Parameters: None.
Default: No display of debug information.
Command Mode: Admin Mode.
Usage Guide: Enable (Disable) the hex debug information of received and sent LDP message contents.
Example: Enable the debug switch
Switch#debug ldp hexdump
Switch#

14.2.12 debug ldp nsm

Command: debug ldp nsm
no debug ldp nsm
Function: Enable the debug information switch of the message communication between NSM and LDP; the no operation will disable the switch.

Parameters: None.
Default: No display of the debug information.
Command Mode: Admin Mode.
Usage Guide: Enable (Disable) the debug information of NSM, mainly including interface changes, route changes, entry distribution and etc.
Example: Enable the debug switch
Switch#debug ldp nsm

14.2.13 debug ldp packet

Command: debug ldp packet [receive|send|detail]
no debug ldp packet [receive|send|detail]
Function: Display the debug information of LDP messages; the no operation will disable the switch.
Parameters: None.
Default: No display of debug information.
Command Mode: Admin Mode.
Usage Guide: Enable (Disable) the debug information of LDP receiving and sending messages. All information about sending and receiving messages will be displayed with the switch enabled while no such information will be printed. receive|send|detail separately means information of receiving/sending and detailed information.
Example: Enable the debug switch.
Switch#debug ldp packet receive

14.2.14 debug ldp timer

Command: debug ldp timer
no debug ldp timer
Function: Display the debug information of the LDP timer; the no operation will disable the switch.
Parameters: None.
Default: No display of debug information.
Command Mode: Admin Mode.
Usage Guide: The debug information of the LDP timer will be displayed with this command enabled.
Example: Enable the debug switch.
Switch#debug ldp timer

14.2.15 debug ldp tsm

Command: debug ldp tsm
no debug ldp tsm
Function: Display the debug information of the LDP state machine.

Parameters: None.
Default: No display of debug information.
Command Mode: Admin Mode.
Usage Guide: Implementing this command will display the debug information of the LDP state machine.
Example: Enable the debug switch.
Switch#debug ldp tsm

14.2.16 debug ldp usm

Command: debug ldp usm
no debug ldp usm
Function: Display the debug information of the LDP upstream state machine.
Parameters: None.
Default: No display of debug information.
Command Mode: Admin Mode.
Usage Guide: Implementing this command will display the debug information of the LDP upstream state machine.
Example: Enable the debug switch.
Switch#debug ldp usm

14.2.17 ldp {enable|disable}

Command: ldp {enable|disable}
Function: Enable the LDP protocol on the interface.
Parameters: None.
Default: The LDP is disabled.
Command Mode: Interface Mode.
Usage Guide: The LDP protocol is a label switching protocol used when switching labels in the public network, which usually works in a BGP VPN environment. “router ldp” is used to globally enable the LDP protocol, however, in interfaces where the protocol is actually working, implementing “ldp enable” in the interface configuration mode is required, so does enabling Label-switching, which, in combination with this command, work as a whole to ensure the normal operation of the protocol.
Example:
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp enable
Related Commands: router ldp, label-Switching

14.2.18 global-merge-capability

Command: global-merge-capability {merge-capable|non-merge-capable }
no global-merge-capability {merge-capable|non-merge-capable }

Function: Enable or disable globally the LDP label merging capability; the no operation will restore the default value.

Parameters: None.

Default: Enable the label merging capability globally.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: The LSP map multiple in-labels to the same FEC, corresponding with the same out-label and out-interface, in which case, when packets with different labels enter the LSR, the output packets will bear the same label. This procedure is called label merging. If the label-merging capability on the interface changes, the switch will reboot.

Example:

Switch(config)#router ldp

Switch(config-router)#global-merge-capability non-merge-capable

14.2.19 hello-interval

Command: hello-interval <*hello-interval*>

no hello-interval

Function: Set the global time interval between hello messages; the no operation will restore the default value.

Parameters: <*hello-interval*> is the time interval between hello messages, ranging from 1 to 65535 seconds.

Default: 5s.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP discovers its neighbors and keeps the communication with them through multicast Hello. Implementing this command will set the time interval of sending hello messages. Please pay attention to the relationship between it and the hold-time. It is better to set a value no greater than 1/3 of the latter. When the interface is configured with Hello-interval, the global configuration will have no effect on it.

Example: Configure the hello-interval as 10:

Switch(config)#router ldp

Switch(config-router)#hello-interval 10

Related Commands: hold-time, ldp hello-interval, ldp hold-time

14.2.20 hold-time

Command: hold-time <*hold-time*>

no hold-time

Function: Configure the hold-time of LDP multicast peers, whose default value is 15 seconds; the no operation will restore the default value.

Parameters: <hold-time> is the hold-time of multicast peer, ranging from 3 to 65535 seconds

Default: 15s.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP discovers its neighbors and keeps in communication with them through

multicast Hello. Implementing this command will set the time interval of sending hello messages. Please pay attention to the relationship between it and the hello-interval. It is better to set a value at least three times as long as the latter. When the interface is configured with Hold-interval, the global configuration will have no effect on it.

Example: Configure the hold-time as 50:

Switch(config)#router ldp

Switch(config-router)#hold-time 50

Related Commands: hello-interval, ldp hold-time, ldp hello-interval

14.2.21 import-bgp-routes

Command: import-bgp-routes

no import-bgp-routes

Function: Configure to import BGP routes; the "no" operation will restore the default configuration.

Parameters: None.

Default: LDP doesn't import BGP routes by default.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: In common cased, LDP finds routes the route table of the system. But there are exceptions where it doesn't import default routes or BGP routes. Importing the default routes may cause disorder, so it is forbidden in any case. If the users can make sure the security, then they can import BGP routes through this command and allocate labels for them.

Example: Import BGP routes and set the import route labels.

Switch(config)#router ldp

Switch(config-router)#import-bgp-routes

14.2.22 keepalive-interval

Command: keepalive-interval <*interval*>

no keepalive-interval

Function: Configure the interval between LDP keep-alive messages, whose default value is 10 seconds; the no operation will restore the default value.

Parameters: <interval>is the interval between keep-alive messages, ranging from 1 to 65535 seconds.

Default: 10s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP will send keepalive messages to each other for keeping the communication, if there is no data after the creation of a TCP session. Implementing this command will set the interval of sending keepalive messages. Please make sure the value is big enough to prevent too many keepalive messages. When this value is configured on the interface, the global configuration command will lose effect.

Example: Configure the global keepalive-interval as 50s.

Switch(config)#router ldp

Switch(config-router)#keepalive-interval 50

Related Commands: keepalive-timeout, ldp keepalive-interval

14.2.23 keepalive-timeout

Command: keepalive-timeout <*time-val*>

no keepalive-timeout

Function: Configure the timeout value of LDP sessions, whose default value is 30 seconds; the no operation will restore the default value.

Parameters: <time-val>is the timeout value of LDP sessions, ranging from 15 to 65535 seconds.

Default: 30s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP will send keepalive messages to each other for keeping the communication, if there is no data after the creation of a TCP session. Without receiving a keepalive message within the timeout period set by this command, the connection will be treated as disconnected. Usually this value should be at least three times as long as the keepalive interval. When this value is configured on the interface, the global configuration command will lose effect.

Example: Configure the global timeout value.

Switch(config)#router ldp

Switch(config-router)#keepalive-timeout 50

Related Commands: keepalive-interval, ldp keepalive-timeout

14.2.24 label-retention-mode

Command: label-retention-mode {conservative|liberal}

no label-retention-mode {conservative|liberal}

Function: Set the label retention mode; the no operation will cancel the configuration.

Parameters: None.

Default: Liberal

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: The LDP label retention mode determines how the LDP protocol handles the label information. The protocol provides two modes: the first one is conservative, which means only allows the retention of label information useful for the switch and drops other information. The other one is liberal, which means to allow the retention of all label information. This mode works together with the label advertisement mode, with liberal working with the “downstream unsolicited” advertisement mode, and conservative with the “downstream-on-demand” mode. Please notice that the manually configured liberal mode and the default one are different. When the liberal mode is set manually, the conservative mode of the interface will be the same as the global one if there is no configuration; while in the default liberal mode, it will be adjusted according to the label advertisement mode of the interface. In common cases, it is not recommended to configure this attributes, for it is in accordance with the label advertisement mode, and will be changed automatically when the label advertisement mode changes. Configuring this attribute separately may cause unmatched attributes. If the label retention mode

changes when the label retention modes of all sessions on the interface are already configured, the session will be reconnected.

Example: Set the global label retention mode as liberal.

Switch(config)#router ldp

Switch(config-router)#label-retention-mode liberal

Related Commands: advertisement-mode, ldp advertisement-mode

14.2.25 label-switching

Command: label-switching

no label-switching

Function: Enable the label-switching function; the no operation will disable the function.

Parameters: None.

Command Mode: Interface Configuration Mode

Default: The label-switching function is disabled.

Usage Guide: Implementing this command to enable the label-switching function. This is a necessity to ensure the normal operation of the LDP protocol.

Example: Enable the label-switching function of the interface vlan1:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#label-switching

Related Commands: enable-ldp

14.2.26 ldp advertisement-mode

Command: ldp advertisement-mode {downstream-on-demand | downstream-unsolicited}

no ldp advertisement-mode {downstream-on-demand | downstream-unsolicited}

Function: Set the interface label advertisement mode; the no operation will cancel the configuration.

Command Mode: Interface Configuration Mode.

Usage Guide: Implementing this command will set the label advertisement mode as downstream-unsolicited or downstream-on-demand. Parameters different with the global configuration can be used when configuring the interface. By default, the value is the global default or the global configuration, unless the interface has its own settings. This mode works together with two other modes, and any change of it will affect the other two at the same time. If the parameter is downstream-unsolicited, the label retention mode will be Liberal and the LSP control mode will be Independent, if it is downstream-on-demand, the label retention mode will be Conservative and the LSP control mode will be Ordered. Parameters different with the global configuration can be used when configuring the interface with this command.

Example: Configure the label advertisement mode as downstream-unsolicited in the interface mode.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp advertisement-mode downstream-unsolicited

Related Commands: label-retention-mode, ldp label-retention-mode, advertisement-mode

14.2.27 ldp hello-interval

Commands: ldp hello-interval <*hello-interval*>

no ldp hello-interval

Function: Set the hello-interval of the interface; the no operation will cancel the configuration.

Parameters: <*hello-interval*> is the interval between multicast Hello messages, ranging from 1 to 65535 seconds.

Default: Using the global configuration.

Command Mode: Interface Configuration Mode

Usage Guide: Implementing this command will set the interval between multicast Hello messages. Parameters different with the global configuration can be used when configuring the interface with this command.

Example: Set the hello interval of the interface as 25s.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp hello-interval 25

Related Commands: ldp hold-time, hold-time

14.2.28 ldp hold-time

Command: ldp hold-time <*hold-time*>

no ldp hold-time

Function: Set the neighbor hold-time of the interface; the no operation will restore the default value.

Parameters: <hold-time>is the neighbor hold time, ranging from 3 to 65535 seconds.

Default: Use the global configuration.

Command Mode: Interface Configuration Mode.

Usage Guide: LDP discovers its neighbors and keeps the communication with them through multicast Hello. Implementing this command will set neighbor hold-time when configuring the multicast. Please pay attention to the relationship between it and the hello-time, that is, it is better to set a value at least three times as long as the hello-time. When the interface is configured with Hold-interval, the global configuration will have no effect on it.

Example: Set the neighbor hold-time as 220s:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp hold-time 220

Related Commands: ldp hello-interval, hello-interval

14.2.29 ldp keepalive-interval

Command: ldp keepalive-interval <*interval-time*>

no ldp keepalive-interval

Function: Configure the interval between keep-alive messages; the no operation will restore the default value.

Parameters: ***<interval-time>*** is the interval between keep-alive messages, ranging from 1 to 65535 seconds.

Default: Use the global configuration.

Command Mode: Interface Configuration Mode

Usage Guide: LDP will send keepalive messages to each other for keeping the communication, if there is no data after the creation of a TCP session. Implementing this command will set the interval of sending keepalive messages. Please make sure the value is big enough to prevent too many keepalive messages. Parameters different with the global configuration can be used when configuring the interface.

Example: Configure the keepalive-interval of the interface as 33s.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp keepalive-interval 33

Related Commands: ldp keepalive-timeout, keepalive-timeout

14.2.30 ldp keepalive-timeout

Command: ldp keepalive-timeout <*time-val*>

no ldp keepalive-timeout

Function: Configure the session timeout value of the interface; the no operation will restore the default value.

Parameters: ***<time-val>*** is the timeout value of sessions, ranging from 15 to 65535 seconds.

Default: 30s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP will send keepalive messages to each other for keeping the communication, if there is no data after the creation of a TCP session. Without receiving a keepalive message within the timeout period set by this command, the connection will be treated as disconnected. Usually this value should be at least three times as long as the keepalive interval. Parameters different with the label configuration can be used when configuring the interface.

Example: Configure the keepalive-interval of the interface as 200s.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp keepalive-timeout 200

Related Commands: ldp keepalive-interval, keepalive-interval

14.2.31 ldp label-retention-mode

Command: ldp label-retention-mode {conservative | liberal}

no ldp label-retention-mode {conservative | liberal}

Function: Set the label retention mode; the no operation will restore the default value.

Parameters: None.

Default: Liberal

Command Mode: Interface Configuration Mode.

Usage Guide: Set the label retention mode as conservative or liberal. When the label retention mode is changed, all the sessions on the interface will be created. If the configuration of the interface is different with the global one, the latter will be ignored. Parameters different with the global configuration can be used when configuring the interface with this command.

Example: Set the label retention mode of the interface as conservative.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp label-retention-mode conservative

Related Commands: advertisement-mode, ldp advertisement-mode

14.2.32 ldp multicast-hellos

Command: ldp multicast-hellos

no ldp multicast-hellos

Function: Configure the interface to discover LDP neighbors with multicast Hello messages; the no operation will cancel the configuration.

Parameters: None.

Default: Use the global configuration.

Command Mode: Interface Configuration Mode

Usage Guide: LDP can discover its neighbors through multicast Hello messages or specify one via the “targeted-peer” command. Implementing this command will enable the multicast hello based neighbor discovery. Implementing the no operation will stop receiving and sending multicast Hello messages, so that the only way to discover neighbors is “targeted-peer”. Parameters different with the global configuration can be used when configuring the interface with this command.

Example:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp multicast-hellos

Related Commands: multicast-hellos

14.2.33 ldp targeted-peer-hello-interval

Command: ldp targeted-peer-hello-interval <*hello-interval*>

no ldp targeted-peer-hello-interval

Function: Set the interval of Hello to the specified target, the no operation will cancel the configuration and restore to the global one.

Parameters: ***<hello-interval>*** is the interval of Hello to the specified target, ranging from 1 to 65535 seconds.

Default: Use the global configuration

Command Mode: Interface Configuration Mode.

Usage Guide: LDP discovers its neighbors and keeps the communication with them by sending Hello to specified targets. Implementing this command will configure the interval of Hello to the specified target. Please pay attention to the relationship between it and the targeted-peer-hold-time. It is recommended to set a value no greater than 1/3 of the

targeted-peer-hold-time. Parameters different with the global configuration can be used when configuring the interface with this command.

Example: Set the interval of Hello to the specified target as 225s.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp targeted-peer-hello-interval 255

Related Commands: ldp targeted-peer-hold-time, targeted-peer-hold-time

14.2.34 ldp targeted-peer-hold-time

Command: ldp targeted-peer-hold-time <*hold-time*>

no ldp targeted-peer-hold-time

Function: Set the peer-hold-time of specified destination for the interface; the no operation will cancel the configuration can restore to the global one.

Parameters: ***<hold-time>*** is the peer-hold-time of the specified target, ranging from 3 to 65535 seconds.

Default: Use the global configuration.

Command Mode: Interface Configuration Mode.

Usage Guide: LDP keeps the communication with neighbors by sending Hello to specified targets. Implementing this command will configure the peer-hold-time of specified destination. Please pay attention to the relationship between it and the targeted-peer-hello-time. It is recommended to set a value at least 3 times as long as the targeted-peer-hello-time. Parameters different with the global configuration can be used when configuring the interface with this command.

Example:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp targeted-peer-hold-time 50

Related Commands: ldp targeted-peer-hello-interval, targeted-peer-hello-interval

14.2.35 loop-detection

Command: loop-detection

no loop-detection

Function: Enable the LDP loop detection; the no operation will cancel the configuration.

Parameters: None.

Default: The loop detection is disabled by default.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP can be configured to enable the loop detection or not. If it is enabled, LDP provides two methods: the first is to check whether the HOP-COUNT exceeds the upper limit; the other is to check whether there is any repeated LSR-ID on the path vector.

Example:

Switch(config)#router ldp

Switch(config-router)#loop-detection

14.2.36 loop-detection-count

Command: loop-detection-count <*count*>

Function: Set the max number of hops allowed in the LDP loop detection; the no operation will restore to the default value.

Parameters: ***<count>*** is the allowed hop number, ranging from 1 to 255.

Default: 255.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP can be configured to enable the loop detection or not. If it is enabled, implementing this command will set the allowed hop number. The configuration will only take effect with loop-detection enabled. The no operation will restore to the default value.

Example: Set the allowed hop number in the LDP loop detection as 200:

Switch(config)#router ldp

Switch(config-router)#loop-detection-count 200

Related Commands: loop-detection

14.2.37 multicast-hellos

Command: multicast-hellos

no multicast-hellos

Function: Configure the interface to discover LDP neighbors with multicast Hello messages or not; the no operation will stop receiving and sending multicast hellos.

Parameters: None.

Default: Enable the receiving and sending of multicast Hellos on the LDP interface.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP can discover its neighbors through multicast Hello messages or specify one via the “targeted-peer” command. Implementing this command will enable the multicast hello based neighbor discovery. Implementing the no operation will stop sending multicast Hello messages, so that the only way to discover neighbors is “targeted-peer”. Configure to sending and receiving multicast hello messages globally, and enumerate all interfaces. If this attribute is already configured on the interface, the global configuration will be ignored, otherwise, the global one will take effect.

Example:

Switch(config)#router ldp

Switch(config-router)#multicast-hellos

14.2.38 propagate-release

Command: propagate-release

no propagate-release

Function: Configure to propagate the label release to neighbors; the no operation will do the opposite.

Parameters: None.

Default: Disabled.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: If the label is expired, the switch won't send it to the upstream, unless this command is enabled.

Example:

Switch(config)#router ldp

Switch(config-router)#propagate-release

14.2.39 request-retry

Command: request-retry

no request-retry

Function: Set LDP to retry 5 times after the request for a label is rejected; the no operation will cancel the configuration.

Parameters: None.

Default Settings: Don't retry.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: When LDP send a label request to the downstream, if the latter rejects it for some reasons, LDP will retry for 5 times with this attribute is configured, at an interval of request-retry-timeout.

Example:

Switch(config)#router ldp

Switch(config-router)#request-retry

Related Commands: request-retry-timeout

14.2.40 request-retry-timeout

Command: request-retry-timeout <*time-val*>

no request-retry-timeout

Function: Set the retry timeout interval after LDP's request for a label is rejected; the no operation will restore the default value.

Parameters: *<time-val>* is the timeout interval, ranging from 1 to 65535 seconds.

Default: 5s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: When LDP send a label request to the downstream, if the latter rejects it for some reasons, LDP will retry for 5 times with this attribute is configured, at an interval of request-retry-timeout.

Example: Set the retry timeout interval as 10 seconds.

Switch(config)#router ldp

Switch(config-router)#request-retry-timeout 10

Related Commands: request-retry

14.2.41 router ldp

Command: router ldp

no router ldp

Function: Enable the LDP protocol; the no operation will disable it.

Parameters: None.

Default: LDP is disabled.

Command Mode: Global Mode.

Usage Guide: The LDP protocol is a label advertising protocol used when switching labels in the public network, which usually works in a BGP VPN environment. Implementing this command will globally enable the LDP protocol, however, in interfaces where the protocol is actually working, implementing "enable-ldp" in the interface configuration mode is required, so does enabling Label-switching, which, in combination with this command, work as a whole to ensure the normal operation of the protocol.

Example:

Switch(config)#router ldp

Switch(config-router)#

14.2.42 router-id

Command: router-id <*ip-addr*>

no router-id

Function: Set the router ID used by LDP; the no operation will cancel the configuration.

Parameters: ***<ip-addr>*** is the router ID, in dotted decimal format.

Default: The ID will be automatically obtained.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: The router ID exclusively identifies a LDP device in the network. Router-id is the value of router-id in Hello messages.

Example:

Switch(config)#router ldp

Switch(config-router)#router-id 10.10.10.10

14.2.43 show ldp

Command: show ldp

Function: Display some basic LDP attributes of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display the current configuration information of LDP.

Example:

Switch#show ldp

Router ID : 10.10.0.11

LDP Version : 1

Global Merge Capability : N/A

Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode : Liberal
Label Control Mode : Independent
Loop Detection : Off
Loop Detection Count : 0
Request Retry : Off
Propagate Release : Disabled
Hello Interval : 5
Targeted Hello Interval : 15
Hold time : 15
Targeted Hold time : 45
Keepalive Interval : 10
Keepalive Timeout : 30
Request retry Timeout : 5
Multicast Hello : Enabled
Targeted Hello Accept : Disabled
Transport Interface : N/A
Import BGP routes : No

Display	Explanation
Router ID : 10.10.0.11	Router id is 10.10.0.11
LDP Version : 1	The LDP version is 1
Global Merge Capability : N/A	The global label merging capability is disabled
Label Advertisement Mode : Downstream Unsolicited	The label advertisement mode is downstream unsolicited
Label Retention Mode : Liberal	The label retention mode is Liberal
Label Control Mode : Independent	The label control mode is Independent
Loop Detection : Off	The loop detection is disabled
Loop Detection Count : 0	The loop detection count is 0
Request Retry : Off	The switch won’t retry after a rejected label request.
Propagate Release : Disabled	The switch won’t propagate the label release messages
Hello Interval : 5	The interval between Hello messages is 5s
Targeted Hello Interval : 15	The interval between Hello messages to a specified target is 15s
Hold time : 15	The hold time of adjacency is 15s
Targeted Hold time : 45	The hold time of adjacency with specified targets is 45s
Keepalive Interval : 10	The intervals between keepalive messages sent by the interface is 10s
Keepalive Timeout : 30	The keepalive timeout period is 30s
Request retry Timeout : 5	The retry timeout after the label request being

	rejected is 5s.
Multicast Hello : Enabled	Discover neighbors via multicast Hello messages
Targeted Hello Accept : Disabled	The switch won't accept Hello from specified targets.
Transport Interface : N/A	No transport interface
Import BGP routes : No	The switch won't import BGP routes

14.2.44 show ldp adjacency

Command: show ldp adjacency

Function: Display all adjacency information of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display LDP adjacency information, for diagnosing and troubleshooting.

Example:

Switch#show ldp adjacency

IP Address	Interface Name	Holdtime	LDP ID
192.168.3.5	vlan1	15	10.10.0.18:0
192.168.4.5	vlan2	15	10.10.0.18:0

Display	Explanation
IP Address	The IP address of the neighbor
Interface Name	The interface name of the connection with the neighbor
Holdtime	The holdtime of the adjacency
LDP ID	（LSR-ID : Label Space）The LDP ID

14.2.45 show ldp downstream

Command: show ldp downstream

Function: Display all downstream information of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode

Usage Guide: Implementing this command will display the information of downstreams maintained by the current protocol.

Example:

Switch#show ldp downstream

Session peer 192.168.11.50:

Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:

Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:

Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:
Downstream state: Established Label: 20 RequestID: 0 Peer: 192.168.11.50 Attr

14.2.46 show ldp fec

Command: show ldp fec
Function: Display information about all FECs (Forwarding Equivalence Class) of this LSR.
Parameters: None.
Default: None.
Command Mode: Admin and Config mode.
Usage Guide: Display information about all FECs (Forwarding Equivalence Class) of this LSR.
Example:
Switch#show ldp fec
LSR codes : E/N - LSR is egress/non-egress for this FEC,
L - LSR received a label for this FEC,
> - LSR will use this route for the FEC

Code	FEC	Session	Out Label	Nexthop Addr
E >	3.3.3.1/32	Non-Existent	None	Connected
E >	4.4.4.1/32	Non-Existent	None	80.80.90.2
E >	80.80.90.0/24	Non-Existent	None	Connected
E >	80.90.70.0/24	Non-Existent	None	80.80.90.2
E >	80.90.70.10/32	Non-Existent	None	Connected
E >	80.90.70.78/32	Non-Existent	None	Connected

14.2.47 show ldp interface

Command: show ldp interface [vlan <*1-4094*> | IFNAME]
Function: Display LDP information about all or specified interfaces of this LSR.
Parameters: <*1-4094*> VLAN ID;
IFNAME: the interface name.
Default: None.
Command Mode: Admin and Config mode.
Usage Guide: Display the LDP information of the interface; user-provided parameters can specify some particular interfaces; no parameter means to display information of all interfaces.
Examples:
Switch#show ldp interface

Interface	LDP Identifier	Label-switching	Merge Capability
vlan0	10.10.0.11:0	Disabled	N/A
vlan1	10.10.0.11:0	Enabled	Merge capable
vlan2	10.10.0.11:0	Enabled	Merge capable

14.2.48 show ldp lsp

Command: show ldp lsp

Function: Display the label switching path of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display the label switching path of the switch.

Example:

```
 Switch#show ldp lsp
FEC IPV4:10.1.1.0/24 -> 0.0.0.0
   Downstream state: Established Label: none RequestID: 0 Peer: EGRESS Attr: None
      Upstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70 Attr: None
      Upstream state: Established Label: impl-null RequestID: 0 Peer: 20.1.1.1 Attr: None
   Downstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70 Attr: None
FEC IPV4:11.1.1.0/24 -> 0.0.0.0
   Downstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70 Attr: None
   Downstream state: Established Label: none RequestID: 0 Peer: EGRESS Attr: None
      Upstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70 Attr: None
   Downstream state: Established Label: impl-null RequestID: 0 Peer: 20.1.1.1 Attr: Hop Count: 1
```

14.2.49 show ldp session

Command: show ldp session [<*ip-addr*>]

Function: Display information about specified or all LDP sessions of this LSR.

Parameters: <*ip-addr*>: the IP address of the neighbor to display, in dotted decimal format.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information about current LDP sessions of this switch.

Example:

```
Switch#show ldp session
Peer IP Address IF Name        My Role      State              KeepAlive
192.168.11.50   vlan1            Passive      OPERATIONAL 30
192.168.13.60   vlan2            Passive      OPERATIONAL 30
```

14.2.50 show ldp statistics

Command: show ldp statistics

Function: Display the LDP statistics of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display the current LDP statistics of this switch.

Example:

Switch#show ldp statistics

PacketType	Sent	Received
Notification	18	22
Hello	102589	103935
Initialization	37	37
Keepalive	45216	45224
Address	44	40
Address Withdraw	3	1
Label Mapping	97	152
Label Request	0	0
Label Withdraw	3	38
Label Release	42	3
Request About	0	0

Display		Explanation
PacketType		The packet types will be listed as below:
Total	Sent	The total number of this type of packets that have been sent.
	Received	The total number of this type of packets that have been received.

14.2.51 show ldp targeted-peers

Command: show ldp targeted-peers

Function: Display the information of LDP targeted peers in the configuration of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display the currently configured LDP neighbor information.

Example:

Switch#show ldp targeted-peers

IP Address	Interface
10.1.1.66	Vlan2

14.2.52 show ldp upstream

Command: show ldp upstream

Function: Display information of all upstreams of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of all LDP upstreams maintained by the switch.

Example:

Switch#show ldp upstream

Session peer 192.168.11.50:

Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:

Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:

14.2.53 show mpls ldp discovery

Command: show mpls ldp discovery [vlan <*1-4094*> | IFNAME]

Function: Display all interfaces and label-switching information of this LSR.

Parameters: <*1-4094*>: VLAN ID.

IFNAME: The interface name

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display all or specified interfaces and label-switching information.

Example:

Switch#show mpls ldp discovery

Interface	LDP Identifier	Label-switching	Merge Capability
Vlan1	10.10.0.11:0	Enabled	Merge capable
Vlan2	10.10.0.11:0	Enabled	Merge capable
Loopback1	0.0.0.0:0	Disabled	N/A

14.2.54 show mpls ldp fec

Command: show mpls ldp fec

Function: Display information about all FECs of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information about currently maintained FECs.

Example:

Switch#show mpls ldp fec

LSR codes : E/N - LSR is egress/non-egress for this FEC,

L - LSR received a label for this FEC,

> - LSR will use this route for the FEC

Code	FEC	Session	Out Label	Nexthop Addr
E >	10.1.1.0/24	non-existent	none	15.1.1.68
NL	10.1.1.0/24	10.1.1.66	impl-null	15.1.1.68
E >	11.1.1.0/24	non-existent	none	15.1.1.68

E >	15.1.1.0/24	non-existent	none	connected
NL>	15.1.1.0/24	10.1.1.66	impl-null	connected
E >	20.1.1.0/24	non-existent	none	15.1.1.68
NL	30.1.1.0/24	10.1.1.66	impl-null	invalid
E >	100.1.1.0/24	non-existent	none	connected
NL	100.1.1.0/24	10.1.1.66	impl-null	connected

14.2.55 show mpls ldp neighbor

Command: show mpls ldp neighbor

Function: Display information about all neighbors of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of LDP neighbors, which is useful for troubleshooting.

Example:

Switch#show mpls ldp neighbor

IP Address	Interface Name	Holdtime	LDP ID
192.168.3.5	vlan1	15	10.10.0.18:0
192.168.4.5	vlan2	15	10.10.0.18:0

14.2.56 show mpls ldp parameter

Command: show mpls ldp parameter

Function: Display basic LDP attributes of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of current LDP configurations.

Example:

Switch#show mpls ldp parameter

Router ID : 10.10.0.11

LDP Version : 1

Global Merge Capability : N/A

Label Advertisement Mode : Downstream Unsolicited

Label Retention Mode : Liberal

Label Control Mode : Independent

Loop Detection : Off

Loop Detection Count : 0

Request Retry : Off

Propagate Release : Disabled

Hello Interval : 5

Targeted Hello Interval : 15

Hold time : 15
Targeted Hold time : 45
Keepalive Interval : 10
Keepalive Timeout : 30
Request retry Timeout : 5
Targeted Hello Receipt : Disabled
Transport Address : N/A
Transport Interface : N/A
Import BGP routes : No

Display	Explanation
Router ID : 10.10.0.11	Router id 为 10.10.0.11 Router ID is 10.10.0.11
LDP Version : 1	The LDP version is 1
Global Merge Capability : N/A	The global label merging capability is disabled
Label Advertisement Mode : Downstream Unsolicited	The label advertisement mode is Downstream Unsolicited
Label Retention Mode : Liberal	The label retention mode is Liberal
Label Control Mode : Independent	The label control mode is Independent
Loop Detection : Off	The loop detection is disabled
Loop Detection Count : 0	The loop detection count is 0.
Request Retry : Off	Don't retry when the request is rejected
Propagate Release : Disabled	Don't propagate the label release message
Hello Interval : 5	The interval between Hello messages is 5s
Targeted Hello Interval : 15	The interval between Hello messages to the specified target is 15s
Hold time : 15	The adjacency hold time is 15s
Targeted Hold time : 45	The hold time of adjacency with the specified target is 45s
Keepalive Interval : 10	The interval between keepalive messages is 10s
Keepalive Timeout : 30	The keepalive timeout of is 30s
Request retry Timeout : 5	The retry timeout after the request is rejected is 5s.
Targeted Hello Receipt : Disabled	Forbidden the receipt of Hello messages from the specified target.
Transport Address : N/A	No configuration of the Transport address
Transport Interface : N/A	No configuration of the Transport Interface
Import BGP routes : No	Don't import BGP routes.

14.2.57 show mpls ldp session

Command: show mpls ldp session [<*ip-addr*>]

Function: Display all or specified LDP sessions of this LSR.

Parameters: <ip-addr> is the IP address of the neighbors to be displayed, in dotted decimal

format.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information about current LDP sessions of this switch.

Example:

Switch#show mpls ldp session

Peer IP Address	IF Name	My Role	State	KeepAlive
192.168.11.50	vlan1	Passive	OPERATIONAL	30
192.168.13.60	vlan2	Passive	OPERATIONAL	30

14.2.58 targeted-hello-accept

Command: targeted-hello-accept [filter <*1-99*>]

no targeted-hello-accept

Function: Configure the LDP to receive Hello messages from the specified target, applied in the extended mode.

Parameters: <*1-99*>: the access list ID that will be used.

Default: Don't accept target-Hello messages.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: By implementing this command, users can specify targets, from which the LDP will accept Hello messages, via access list commands.

Example:

Switch(config)#router ldp

Switch(config-router)#targeted-hello-accept filter 1

14.2.59 targeted-peer

Command: targeted-peer <*ip-addr*>

no targeted-peer <*ip-addr*>

Function: Configure the LDP neighbor of the specified target; the no operation will delete the configuration.

Parameters: <ip-adddr> is the IP address of the neighbor, in dotted decimal format.

Default: No targeted-peer.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP can discover a neighbor via multicast Hello messages or manual configurations. This command enables the latter method by adding a targeted-peer and establishing the adjacency with it. The no operation will delete the configuration. Configuring a targeted-peer neighbor means to establish an extended session.

Example: Configure the LDP neighbor of the specified target is 10.10.10.10

Switch(config)#router ldp

Switch(config-router)#targeted-peer 10.10.10.10

14.2.60 targeted-peer-hello-interval

Command: targeted-peer-hello-interval <*hello-interva*>

no targeted-peer-hello-interval

Function: Configure the global interval between Hello messages to the specified target; the no operation will restore the default value.

Parameters: <*hello-interval*> is the interval between Hello messages to the specified target, ranging from 1 to 65535 seconds.

Default: 15s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP discovers a neighbor and stays in communication with it via sending Hello messages to the specified target. Implementing this command will configure the interval between those Hello messages. Please pay attention to the relationship between it and the targeted-peer-hold-time. It is recommended to configure a value no greater than 1/3 of the latter. When a specified interface has its own configuration, this command will lose effect on it.

Example: Configure the Hello interval as 50s.

Switch(config)#router ldp

Switch(config-router)#targeted-peer-hello-interval 50

Related Commands: targeted-peer-hold-time, ldp targeted-peer-hold-time, ldp targeted-peer-hello-Interval

14.2.61 targeted-peer-hold-time

Command: targeted-peer-hold-time <*hold-time*>

no targeted-peer-hold-time

Function: Configure the global hold-time of the specified target; the no operation will restore the default value.

Parameters: *<hold-time>* is the hold-time of the specified target, ranging from 3 to 65535 seconds.

Default: 45s.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP discovers a neighbor and stays in communication with it via sending Hello messages to the specified target. Implementing this command will configure the hold-time of neighbors discovered by the specified target. Please pay attention to the relationship between it and the targeted-peer-hello-interval. It is recommended to configure a value at least three times as long as the latter. When a specified interface has its own configuration, this command will lose effect on it.

Example: Configure the neighbor hold-time as 50s.

Switch(config)#router ldp

Switch(config-router)#targeted-peer-hold-time 50

Related Commands: targeted-peer-hello-interval, ldp targeted-peer-hold-time, ldp targeted-peer-hello-interval

14.2.62 transport-address

Command: transport-address <*ip-addr*>

no transport-address

Function: Configure the IP address used by LDP to establish TCP connections; the no operation will cancel the configuration.

Parameters: <*ip-addr*> is the IP address, in dotted decimal format. This address should be one of a loopback interface.

Default: The address is automatically obtained.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: After the discovery of a neighbor via multicast or targeted Hello messages, LDP doesn't use the interface address sending the messages as the source address when establishing TCP connections, instead it uses the transport-address in the Hello messages to guarantee the uniqueness of the connection. Usually, LDP chooses an interface address as transport-address. Implementing this command will configure this address. The no operation will cancel the configuration, and regain an interface address as transport-address automatically.

Example: Configure 10.10.10.10 as the source address of TCP connections.

Switch(config)#router ldp

Switch(config-router)#transport-address 10.10.10.10

14.3 MPLS VPN

14.3.1 address-family ipv4

Command: address-family ipv4 [unicast | vrf <*vrf-name*>| multicast]

no address-family ipv4 vrf <*vrf-name*>

Function: Configure the BGP VPN address family; the no operation will cancel the configuration. Before entering the BGP-VPN view, this VRF should be created and configured with rd.

Parameters: unicast: unicast address family factor

***<vrf-name>* :** the VPN route/forwarding instance name

Default: No BGP VPN address family.

Command Mode: BGP Route Configuration Mode.

Example:

Switch(config)#router bgp 100

Switch(config-router)#address-family ipv4 vrf VRF-A

Switch(config-router-af)#

14.3.2 address-family vpnv4

Command: address-family vpnv4 [unicast]

Function: Configure the BGP VPNv4 address family in non-default mode.

Parameters: unicast: the unicast address family factor.
Default: No BGP VPNv4 address family.
Command Mode: BGP Route Configuration Mode.
Example:
Switch(config)#router bgp 100
Switch(config-router)#address-family vpnv4 unicast
Switch(config-router-af)#

14.3.3 aggregate-address

Command: aggregate-address <*ip-address/M*> [summary-only] [as-set]
no aggregate-address <*ip-address/M*> [summary-only] [as-set]
Function: By aggregating addresses, users can decrease the route message propagation; the no operation will cancel the configuration.
Parameters: <*ip-address/M*>: IP address, MASK length
[summary-only]: Only send the summary and ignore the route.
[as-set]: Display each AS of the path once in the list form.
Default: No aggregate configuration.
Command Mode: BGP Route Configuration Mode, VRF Address Family Configuration Mode.
Usage Guide: By aggregating addresses, users can decrease the route message propagation. The summary-only option means only to send the summary and ignore the route, and the as-set option will display the AS of every route covered by the aggregate for once without repetition.
Example:
Switch(config-router)#aggregate-address 100.1.0.0/16 summary-only
Switch(config-router)#aggregate-address 100.2.0.0/16 summary-only as-set
Switch(config-router)#aggregate-address 100.3.0.0/16 as-set
Related Commands: bgp aggregate-nexthop-check, no bgp aggregate-nexthop-check

14.3.4 clear ip bgp

Command: clear ip bgp * [vrf <*vrf-name*>] [in | out | soft [in | out]]
Function: Reboot the corresponding bgp process of vrf-name, and the connections between all peers of the process.
Parameters: <*vrf-name*>: the configured VPN instance name, whose length ranges from 1 to 64 characters.
in: soft reboot and configure the inbound update;
out: soft reboot and configure the outbound update;
soft: soft reboot
Default: No configuration.
Command Mode: Admin Mode
Usage Guide: Implementing the “clear ip bgp *” command will restart the BGP process; configuring the “in” parameter will send route request message to neighbors; configuring the “out” parameter will send its route to neighbors; configuring the “soft” parameter won’t restart

the BGP process.

Example:

Switch#clear ip bgp * vrf VRF-A

Switch#

14.3.5 debug bgp mpls

Command: debug bgp mpls

no debug bgp mpls

Function: Display the information about processing VRF FTN, the global FTN, and global ILM entries while the bgp vpn is running; the no operation will disable the display.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: Enable the debug information to check the information about processing VRF FTN, the global FTN, and global ILM entries while the bgp vpn is running.

Example:

Switch#debug bgp mpls

Switch#

14.3.6 debug bgp update

Command: debug bgp update

no debug bgp update

Function: Display the route update information received by bgp vpn while it is running; the no command will disable the information.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Example:

Switch#debug bgp update

Switch#

14.3.7 description

Command: description <*text*>

no description

Function: Configure the description of VRF to record information like the relationship between the VNP instance and a VPN; the no operation will disable the description.

Parameters: <*text*>: the descriptive text, whose length ranges from 1 to 256 characters.

Default: No configuration.

Command Mode: VRF Configuration Mode.

Usage Guide: Following “description” is user’s description of VRF, which will be displayed below

the corresponding VRF to provide instructions.

Example: Configure the VRF description as "associate with VRF-B VRF-C**".**

Switch(config)#ip vrf VRF-A

Switch(config-vrf)#description associate with VRF-B VRF-C

14.3.8 import map

Command: import map <*route-map-name*>

no import map

Function: Apply import-route-map policy to the specified VPN instance.

Parameters: <*route-map-name*>: the route-map policy name.

Default: No configuration.

Command Mode: VRF Configuration Mode.

Usage Guide: When a more accurate method of importing VPN instance routes than the extended-community attribute is required, the import-route policy is an option. By default, the imported routes will be filtered according to their VPN-target extended-community attribute. The import-route policy may decline the routes chosen from the communities in the import list.

Example: Apply the map-a route-map to the VRF instance VRF-A.

Switch(config)#ip vrf VRF-A

Switch(config-vrf)#import map map-a

Switch(config-vrf)#

14.3.9 ip route vrf

Command: ip route vrf <*vrf-name*>{<*ip-prefix*> <*mask*>|<*ip-prefix/prefix-length*>}
{<*gateway-address*>|null0} [<*1-255*>]

no ip route vrf <*vrf-name*>{<*ip-prefix*> <*mask*>|<*ip-prefix/prefix-length*>}
{<*gateway-address*>|null0} [<*1-255*>]

Function: Specify static routes for the specified VRF. Before doing this, a successful VPN forwarding instance is required. The no operation will delete the configured static routes.

Parameters: <*vrf-name*>: The specified VRF name

<*ip-prefix*>: the destination IP address

<*mask*>: mask, in dotted decimal format

<*prefix-length*>: the length of the prefix

<*gateway-address*>: the next-hop address

null0: the black hole route;

<1-255>: Administrative distance.

Example:

Switch(config)#ip route vrf VRF-A 10.1.1.10 255.255.255.0 10.1.1.1

Switch(config)#

14.3.10 ip vrf

Command: ip vrf <*vrf-name*>

no ip vrf <*vrf-name*>

Function: Configure a VPN instance with the specified name; the no operation will cancel the instance.

Parameters: ***<vrf-name>*** the configured VPN instance name, whose length is 1 to 64.

Default: No configuration.

Command Mode: Global Mode.

Usage Guide: Configure a VPN instance with the specified name. There is no default VPN instance on PE, which allows multiple VPN instances. The VPN instance name is case sensitive. Please notice that only after configuring RD will the VPN instance take effect.

Example:

Switch(config)#ip vrf VRF-A

Switch(config-vrf)#

14.3.11 ip vrf forwarding vrfName

Command: ip vrf forwarding <vrfName>

no ip vrf forwarding <*vrfName*>

Function: Bind interfaces to the specified VRF.

Parameters: ***<vrfName>*** is the VRF name, a string shorter than 32 characters.

Command Mode: Interface Configuration Mode.

Usage Guide: Implementing the command if the interface needs to access the Internet. Each interface can only be bound to one VRF, while the latter can be bounded with multiple interfaces. The IGP supporting VPN will record the binding relationship between interfaces and VRF by adding a route received from the bound interface to the route table of the bound VRF. By default, the interface is bound to no VRF, and is a public network interface.

Example:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ip vrf forwarding vpn1

14.3.12 neighbor remote-as

Command: neighbor *<ip-address>* remote-as *<as-num>*

no neighbor <*ip-address*> remote-as <*as-num*>

Function: Add a new BGP neighbor; the no operation will delete it.

Parameters: ***<ip-address>*****:** specify the BGP neighbor address. BGP neighbor address should be Loopback port IP for neighbor switch.

<as-num>**:** specify the AS number of the BGP neighbor.

Default: No BGP neighbor.

Command Mode: VRF Address Family Configuration Mode.

Usage Guide: Implementing this command will add a new neighbor for the switch.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf VRF-A
Switch(config-router-af)#neighbor 3.0.0.1 remote-as 65001
Switch(config-router-af)#
```

14.3.13 neighbor as-override

Command: neighbor {*<ip-address>* | *<TAG>*} as-override

no neighbor {*<ip-address>* | *<TAG>*} as-override

Function: Override the AS path (the previous AS number). Before implementing this command, users should create a neighbor first. The no operation will delete the configuration.

Parameters: *<ip-address>*: specify the BGP neighbor address;

***<TAG>*:** Specify the BGP neighbor group number.

Default: Not configured.

Command Mode: VRF Address Family Configuration Mode.

Usage Guide: After this command being implemented, the route from the neighbor will override the existing AS number.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf VRF-A
Switch(config-router-af)#neighbor 3.0.0.1 remote-as 65001
Switch(config-router-af)#neighbor 3.0.0.1 as-override
Switch(config-router-af)#
```

14.3.14 neighbor soo

Command: neighbor *<ip-addr>* soo *<soo-val>*

no neighbor *<ip-addr>* soo *<soo-val>*

Function: Configure the site-of-origin from the neighbor route; the no operation will delete the configuration.

Parameters: *<ip-addr>* the neighbor's ip address, in dotted-decimal format.

<soo-val> is the site-of-origin, in the same form as RD.

Default: Not configured.

Command Mode: VRF Address Family Configuration Mode.

Usage Guide: If the customer AS is connected with multiple ISP devices, configuring this attribute can prevent the customer route from returning to the customer after passing the P area. This configuration will propagate once set. The route with the SOO attribute won't propagate to the neighbor already configured with this attribute.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf test
Switch(config-router-af)#neighbor 11.1.1.64 remote 200
Switch(config-router-af)#neighbor 11.1.1.64 soo 100:10
```

After configuring this attribute, the switch won't propagate the remote route with the 100:10 rt attribute to 11.1.1.64. (To be clear, the soo attribute will be checked together with other rt attributes, that is to say, the neighbor will be treated as the original neighbor no matter it is or not, once the rt is configured with the same attributes. In fact, soo is usually configured separately with a value different with rt/rd, and is unique in the reachable area to describe the origin accurately).

14.3.15 rd

Command: rd <*ASN:nn_or_IP-address:nn*>

Function: Configure the RD (Route Distinguish) of VRF.

Parameters: ASN:nn_or_IP-address:nn：The IP address format of the switch ID. ASN is AS ID, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100); IP-address is IP address that the length is 4 bytes; nn is arbitrary number that the length is 2 bytes.

Default: Not configured.

Command Mode: VRF Configuration Mode.

Usage Guide: RD can uniquely identify the VPN route. VPN instances realize address space independence via RD, and thus realize the address overlap between different VPNs. Usually the configuration includes the AS number and an arbitrary number. RD can't be deleted directly.

Example:

Switch(config)#ip vrf VRF-A
Switch(config-vrf)#rd 300:3
Switch(config-vrf)#

14.3.16 route-target

Command: route-target {import | export | both} <*rt-value*>
no route-target {import | export | both} <*rt-value*>

Function: Configure the Route-Target of the specified VRF Route-Target; The no operation will delete the configuration.

Parameters: import: Means to filter the import route, which means to judge whether the VPN route can be added into the VRF;

export: Means to use the route of this VRF as the Route-Target that will be added to when the VPNv4 route sends out messages, in order to filter the interface import;

both: Means the import and the export use the same Route-Target;

<*rt-value*>: Is the the route target value, the format is ASN:nn_or_IP-address:nn. ASN is AS ID, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100); IP-address is IP address that the length is 4 bytes; nn is arbitrary number that the length is 2 bytes.

Default: Not configured.

Command Mode: VRF Configuration Mode.

Usage Guide: A RT is a BGP extended community, for filtering the VPN routes and controlling the

VNP membership of directly connected site and route policies. For the configured import rule, enumerate all routes received by the bgp process and add routes matching the condition (the export route-target overlaps with the import route-target of this VRF) to the bgp process of this VRF and advertise the route update messages to the bgp private network neighbors of this VRF. For the configured export rule, enumerate all bgp routes stored in the bgp process related with this VRF, add an export-target to these routes and advertise the route update messages to the bgp public network neighbors. If there is an import route-target of some other VRF matches the export route- target, copy the routes to the matching VRF and advertise the route update messages to the bgp private network neighbors of it.

Example:

Switch(config)#ip vrf VRF-A
Switch(config-vrf)#route-target both 100:1
Switch(config-vrf)#

14.3.17 show ip bgp vpnv4

Command: show ip bgp vpnv4 {all|rd <*rd-val*>|vrf <*vrf-name*>}

Function: Implementing this command will display all VRF of this switch or route information of the specified VRF.

Parameters: all: all VPNv4 peers.

rd-val: the route distinguisher, usually in a format of numbers (AS number of IP address), such as 100:10.

<vrf-name> the configured VPN instance name, whose length is 1 to 64.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of a specified RD or VRF.

Example:

Switch#show ip bgp vpn4 all
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24 11.1.1.64 0 0 200 ?
*> 20.1.1.0/24 11.1.1.64 0 0 200 ?

14.3.18 show ip route vrf

Command: show ip route vrf <*vrf-name*> [bgp|datebase]

Function: Display information of the specified route protocol.

Parameters: <*vrf-name*>: the VRF name created with the “if vrf<vrf-name>” command.

bgp: the route imported via bgp;

database: the IP route table database.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of the specified route protocol.

Example:

```
 Switch#show ip route vrf vrf-a bgp
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24 11.1.1.64 0 0 200 ?
*> 20.1.1.0/24 11.1.1.64 0 0 200 ?
```

14.3.19 show ip vrf

Command: show ip vrf [<*vrf-name*>]

Function: Implementing this command will display the RIP instance information related with this VPN route/forwarding instance and the fallback global option of the interfaces bound with the VRF.

Parameters: ***<vrf-name>*** specifies the name of the VPN route/forwarding instance.

Default: No display by default.

Command Mode: Admin and Config mode.

Usage Guide: This command also exists in other route protocols. Implementing this command will also display the information of other related route protocol processes.

Example: Display the information of the RIP instances related with the IPI vrf route/forwarding instance.

```
Switch#show ip vrf IPI
  VRF IPI, FIB ID 1
  Router ID: 11.1.1.1 (automatic)
  Interfaces:
  Vlan1
  !
  VRF IPI; (id=1); RIP enabled Interfaces:
   Ethernet1/0/8

  Name                Interfaces
  IPI                  Vlan1

  Name                        Default RD          Interfaces
  IPI                                              Vlan1
```

14.4 VPLS&VPWS

14.4.1 clear mac-address-table

Command: clear mac-addresse-table [vfi <vfi-name>]

Function: Clear MAC address table of forwarding in VPLS instances, if there is parameter input, clear the specified MAC address table, or clear all MAC address tables.

Parameter: vfi <vfi-name>：It is the name of VPLS instance, it is a character string with the length from 1 to 32.

Default: None

Command Mode: Admin mode

Usage Guide: Use this command to clear all MAC (clear all MAC addresses including VFI and non-VFI addresses when no VFI is specified), or clear MAC in the specified VFI.

Example:

Switch#clear mac-address-table vfi v1

14.4.2 debug vpls packet

Command: debug vpls packet [send | receive | detial]

no debug vpls packet

Function: Enable the debugging of receiving and sending packets for VPLS, no command disables the debugging.

Parameter: send：send packet's information

receive：receive packet's information

detail：detail information for receiving and sending packets

Default: Do not display the debugging.

Command Mode: Admin mode

Usage Guide: Use this command to check the relevant packets of VPLS forwarded by software platform, including the packets of VPWS and VPLS and layer 2, layer 3 packets processed by VPLS and VPWS.

Example:

Switch#debug vpls packet send

14.4.3 description

Command: description <text>

no description

Function: Add descriptive information for VPLS instance, no command deletes the information.

Parameter: <text>：Descriptive information for VFI, it is a character string with the length from 1 to 128, do not distinguish capital letter and small letter.

Default: No descriptive information

Command Mode: VFI configuration mode

Usage Guide: Configure this command to add descriptive information for VPLS instance in VFI.
Example:
Switch(config)#vfi v1 100
Switch(config-vfi)#description vpn1

14.4.4 encapsulation

Command: encapsulation {ethernet | vlan}
Function: Set encapsulation type for VPLS instance. By default, it is in VLAN mode, and in Tagged mode for PW. As long as there is VFI, this command can be used to specify and modify encapsulation type as long as VFI exists.
Parameter: ethernet：Specify encapsulation type for VPLS instance to be in Ethernet mode and in Raw mode for PW.
vlan：Specify encapsulation type for VPLS instance to be in VLAN mode and in Tagged mode for PW.
Default: Encapsulation type for VPLS instance to be in VLAN, while in Tagged mode for PW.
Command Mode: VFI configuration mode
Usage Guide: Use this command to modify VFI encapsulation mode. Notice: it can not be modified after PW is established.
Example:
Switch(config)#vfi v1 100
Switch(config-vfi)#encapsulation ethernet

14.4.5 l2-vc

Command: l2-vc <ip-address> pw-id <pw-id> [group <group-id>] [pw-class <class-name>]
no l2-vc <ip-address> pw-id <pw-id>
Function: Configure peer PE for VPWS, no command deletes it.
Parameter: <ip-address>： Specify neighbor address of the peer PE in VPWS, the address usually is the router-id of the peer PE or an address of loopback interface.
<pw-id>：Specify PW ID of the peer PE, range from 1 to 4294967295. A PW of two PEs must be same.
<group-id>：Group ID of neighbor in VPWS, range from 1 to 4294967295.
<class-name>：Specify PE template name used by VPWS neighbor, it is a character string with the length from 1 to 32, do not distinguish capital letter and small letter.
Default: group_id is 0 by default. Do not specify PW-class, the default trans_mode is in tag mode.
Command Mode: Global mode
Usage Guide: Create a VPWS with this command, it needs to specify the address of the peer and the relevant pw-id.
Example:
Switch(config)#l2-vc 192.168.0.1 pw-id 1 pw-class c1

14.4.6 mac-address-table limit

Command: mac-address-table vfi <*vfi-name*> limit <*num*>

no mac-address-table vfi <*vfi-name*> limit

Function: Specify the total limit of MAC addresses in VPLS instance. If it exceeds the threshold, the system will not learn MAC addresses, it will broadcast packets among VPLS instance. No command restores the default value.

Parameter: <num>: the number threshold of MAC addresses.

Default: Do not limit the MAC address number in VPLS instances.

Command Mode: System mode

Usage Guide: Use this command to limit the total of MAC address in VFI. If it exceeds the threshold, the system will not learn MAC addresses and the new MAC will not be forwarded.

Example:

Switch(config)#mac-address-table vfi v1 limit 100

Switch(config)#no mac-address-table vfi v1 limit

14.4.7 mac-address-table static address

Command: mac-address-table static address <FF-FF-FF-FF-FF-FF> vfi <vfi-name> {interface [ethernet | port-channel] <IFNAME> [svid <1-4094>] | peer <peer-address>}

no mac-address-table {static | dynamic} [address <FF-FF-FF-FF-FF-FF>] vfi <vfi-name> [interface [ethernet | port-channel] <IFNAME> | peer <peer-address>]

Function: Configure static MAC addresses in VPLS instance. We can set them to local MAC addresses or remote MAC addresses. No command deletes them.

Parameter: static：specify static MAC addresses, It allows users to configure static VFI MAC addresses so far

<FF-FF-FF-FF-FF-FF>：static MAC addresses

vfi：specify VPLS instance

<vfi-name>：specify name of VPLS, it is a character string with the length from 1 to 32

<IFNAME>：specify interfaces of static MAC addresses, it is a character string with the length from 1 to 32

peer：specify remote station of static MAC

<peer-address>：specify IP address of remote station corresponded with static MAC

Default: No static MAC address.

Command Mode: VFI configuration mode

Usage Guide: Use this command to add/delete static MAC on VFI, the method for processing MAC is same as non-VFI.

Example: Configure static MAC addresse for local station.

Switch(config)#mac-address-table static address 00-00-00-00-00-01 vfi v1 interface Ethernet1/0/1 svid 200

14.4.8 mtu

Command: mtu <mtu>

no mtu

Function: Specify MTU (maximum transmission unit) in VPLS instance, no command restores the default values.

Parameter: <mtu>：Specify MTU (maximum transmission unit) in VPLS instance. Its range from 576 to 10218.

Default: The default value is 1500.

Command Mode: VFI configuration mode

Usage Guide: Set MTU value forwarded by VPLS, the defaut value is 1500, its value is related with the actual application. Usually, MTU is not modified, only the small packets can pass, but the big packets can not pass, it will be modified.

Example:

Switch(config)#vfi v1 100

Switch(config-vfi)#mtu 1600

14.4.9 peer

Command: peer <ip-address> [pw-id <pw-id>] [no-split-horizon] [pw-class <class-name>]

no peer <ip-address>

Function: Configure the peer PE included in VPLS instance. By default, enable level division. A neighbor without the ability of the level division is considered to correspond with spoke-vc, else correspond with mesh-vc. No command deletes a specified neighbor.

Parameter: <ip-address>：Specify neighbor address of the peer PE in VPLS, usually it is the address of t router-id of the peer PE or an address of loopback interface.

pw-id <pw-id>：Specify PW ID of the peer PE, its range from 1 to 4294967295. A PW of two PEs must be same.

no-split-horizon：disable level division. For mesh neighbor, it must enable level division.

pw-class <class-name>：Specify PW template name used by VPLS neighbor, it is a character string with the length from 1 to 32, do not distinguish capital letter and small letter

Default: No PW-class is specified, pw-id is vpls-id, and level division is enabled. Please note that it must enable level division to avoid loopback for the neighbor of mesh.

Command Mode: VFI configuration mode

Example:

Switch(config)#vfi v1 100

Switch(config-vfi)#peer 192.168.0.1 pw-class pw1

14.4.10 pw-class

Command: pw-class <class-name>

no pw-class <class-name>

Function: pw-class is used to create a PW template and enter template view. No command deletes an existing PW template.

Parameter: <pw-class-name>：PW template name, it is a character string with the length from 1 to 32, do not distinguish capital letter and small letter

Default: No PE template.

Command Mode: Global mode
Usage Guide: Use this command to create PW template, it can set PW encapsulation mode.
Example:
Switch(config)#pw-class pw1
Switch(config-class)#

14.4.11 show mpls l2-vc

Command: show mpls l2-vc [<vc-id>]
Function: Display summary information of VC.
Parameter: <vc-id>： ID for virtual circuit, its range form 1 to 4294967295
Default: None.
Command Mode: Any modes
Usage Guide: Display the relevant information for VPWS.
Example:
Switch#show mpls l2-vc

VC ID	State	Type	In Label	Out Label	Endpoint
10	UP	VLAN	645	650	2.2.2.2
14	UP	VLAN	645	650	2.2.2.2

14.4.12 show pw-class

Command: show pw-class [<class-name>]
Function: Display PW class.
Parameter: <class-name>： name of PW class, it is a character string with the length from 1 to 32.
Default: None
Command Mode: Any modes
Usage Guide: Display pw-class information.
Example:
Switch#show pw-class
PW-Class Name：class1，encapsulated mode：VLAN

14.4.13 show vpls

Command: show vpls [<vfi-name> | detail]
Function: Show VPLS instance. If there is no specified vfi-name, it will show all information for VPLS instances. If there is a detail parameter, it will show the detail information for VPLS instance, or it will show summary information for VPLS instance.
Parameter: <vfi-name>： name of VPLS instance, it is a character string with the length from 1 to 32.
detail: show the detail information.
Default: None.

Command Mode: Any modes

Usage Guide: Show VPLS information.

Example:

Switch#show vpls

Name	VPLS-ID	Type	MTU	Peers	State
govern	100	Ethernet	1500	2	Active

14.4.14 show vpls fib

Command: show vpls fib [<vfi-name>]

Function: Show forwarding table of VPLS instance.

Parameter: <vfi-name>： name of VPLS instance, it is a character string with the length from 1 to 32.

Default: None.

Command Mode: Any modes

Usage Guide: Show VPLS forwarding instances.

Example:

<Sysname> show vpls fib vfi vpna

VfiName PwId Inlabel OutLabel NextHop

vpna 1 103 102 6.1.1.1

Table 4-1 information description table

Display	Description
VfiName	Name of VPLS instance
PwId	ID in PW of VPLS instance
Inlabel	Inlabel value of VPLS instance
OutLabel	OutLabel value of VPLS instance
NextHop	Nexthop address of VPLS instance

14.4.15 show vfi mac-address-table

Command: show vfi mac-addresses-table [vfi <vfi-name>]

Function: Display MAC address table in VPLS instance. If there is parameter input, it will display the specified MAC address table, or it will display all MAC address tables.

Parameter: vfi： specify VPLS instance

<vfi-name>： name of VPLS instance, it is a character string with the length from 1 to 32.

Default: None.

Command Mode: Any modes

Usage Guide: Display MAC address learnt from VPLS.

Example:

switch# show vfi mac-address-table vfi aaa

Vfi	MAC Address	Type	Creator	Ports
----	----------	----------	---------	----------

aaa 00-01-02-03-04-05 Dynamic ethernet1/0/1

Table 4-2 description information

Vfi	Name of VPLS instance
MAC Address	MAC address
Type	Type of MAC address, Static or Dynamic
Creator	Creator of MAC address
Ports	Port name, it will be N/A if it is null.

14.4.16 show vfi mac-address-table count

Command: show vfi mac-addresses-table count [vfi <vfi-name>]

Function: Display total of MAC address table in VPLS instance. If there is parameter input, it will display total of MAC address table in VPLS instance, or it will display all MAC address tables.

Parameter: vfi： specify VPLS instance

<vfi-name>： name of VPLS instance, it is a character string with the length from 1 to 32.

Default: None.

Command Mode: Any modes

Usage Guide: Display the statistic MAC addresses learnt from VFI.

Example:

```
switch# show vfi mac-address-table count
Vfi        MAC count
------     ---------------
vpna       100
vpnb       90
```

14.4.17 show vpls peer

Command: show vpls peer [<vfi-name>] {mesh | spoke}

Function: Display PW summary in VPLS instance. If there is no vfi-name parameter input, it will display all information of mesh or spoke neighbor in VPLS instance.

Parameter: <vfi-name>： name of VPLS instance, it is a character string with the length from 1 to 32.

mesh: display mesh neighbor

spoke： display spoke neighbor

Default: None.

Command Mode: Any modes

Usage Guide: Display the relevant peer of the specified type for VPLS.

Example:

```
switch#show vpls peer aaa mesh
PW-ID      Peer Addr   In-Intf     In-Label    Out-Intf    Out-Label   Lkps/St
---------  -----------  ---------  -----------  ---------  -----------  ----------
100         2.2.2.2 N/A          650          N/A         651          1/UP
```

Table 4-3 description information

PW-ID	ID of PW
Peer Addr	Address of peer
In-Intf	Name of InInterface, if it is null, display N/A
In-Label	ID of In-Label, if it is null, display none
Out-Intf	Name of Out-Intface, if it is null, display N/A
Out-Label	ID of Out-Label, if it is null, display none
Lkps	Values are 0, 1, 2; 1 stands for PUSH_FOR_VC, 2 stands for PUSH_AND_LOOKUP_FOR_VC
St	State of PW, UP or DOWN

14.4.18 transport-mode

Command: transport-mode {ethernet | vlan}

no transport-mode

Function: Configure packet encapsulation mode of PW template, no command restores the default value.

Parameter: ethernet： packets in PW is in ethernet mode without vlan tag.

vlan： packets in PW is in VLAN-tagged mode, drop non-VLAN-tagged packets/

Default: PW transmission mode is VLAN.

Command Mode: PW template configuration mode

Usage Guide: Use this command to create PW template which can set PW encapsulation mode currently. When it conflicts with encapsulation mode of VFI, PW encapsulation mode is preferential.

Example:

Switch(config)#pw-class pw1

Switch(config-class)#transport-mode vlan

14.4.19 ptag

Command: ptag <vlan_id>

no ptag

Function: Configure the inner vlanID encapsulated when sending end-to-end PW messages.

Parameter: <vlan_id>The expected inner tag carried by the PW message on the opposite end, with a value range of<1-4094>.

Default: The inner vlanID encapsulated during the sending of the end-to-end PW message is 0.

Command Mode: PW template configuration mode

Usage Guide: Using this command on PE can create a PW template, which can currently set the expected inner vlan carried by the peer PW. After configuration, in tagged mode, the inner tag of the message sent by the peer PW side is the configured ptag.

Example:

Switch(config)#pw-class pw1

Switch(config-class)#ptag 10

14.4.20 Vfi

Command: vfi <vfi-name> <vfi-id>

no vfi <vfi-name> <vfi-id>

Function: Create a VPLS instance, at the same time, it must specify the global and unique VFI-NAME and VFI-ID. vfi-name and vfi-id should be one-to-one correspondence. A vfi-name or vfi-id can uniquely identify a VPLS instance. No command deletes the VPLS instance.

Parameter: <vfi-name>： name of VFI, it is unique in global mode, it is a character string with the length from 1 to 32.

<vfi-id>： VFI ID, its range from 1 to 4294967295.

Default: No VPLS instance.

Command Mode: Global mode

Usage Guide: Use this command to create a VFI and enter VFI view to configure the relevant VFI command.

Example:

Switch(config)#vfi v1 1

Switch(config-vfi)#

14.4.21 vfi vfi-name

Command: vfi <vfi-name>

Function: Enter VFI mode. When the relevant VPLS instance exists, enter VFI mode.

Parameter: <vfi-name>： name of VFI, it is unique in global mode, it is a character string with the length from 1 to 32.

Default: No VPLS instance.

Command Mode: Global mode

Usage Guide: Use this command to enter the relevant VFI view.

Example:

Switch(config)#vfi v1

Switch(config-vfi)#

14.4.22 xconnect l2-vc

Command: xconnect l2-vc pw-id <pw-id> [mode {ethernet | vlan [svid <svid>]}]

no xconnect l2-vc pw-id <pw-id>

Function: Bind port and the specified PW and configure access mode of AC. If access mode is VLAN, it specifies svid additionally. This command binds port and PW directly to establish point-to-point connection, it is used to support VPWS. No command deletes the binding.

Parameter: ethernet： access mode is ethernet

vlan： access mode is VLAN-tagged

<pw-id>: PW ID, its range from 1 to 4294967295

<svid>：service-vlan-id, its range from 1 to 4094

Default: Do not bind port to any PW, access mode is VLAN.

Command Mode: Global mode

Usage Guide: Use this command to bind port to the specified PW, it is used in VPWS.

Example:

Switch(config)#interface Ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#xconnect l2-vc pw-id 1 mode vlan svid 200

14.4.23 xconnect vfi

Command: xconnect vfi <vfi-id> [mode {ethernet | vlan [svid <svid>]}]

no xconnect vfi <vfi-id>

Function: Bind a port to a VPLS instance and configure AC access mode, no command deletes the binding.

Parameter: <vfi-id>: ID for VPLS instance, its range from 1 to 4294967295

svid: service-vlan-id is outer label, it is used to specify outer VLAN matched with packets

ethernet：access mode is ethernet

vlan：access mode is VLAN-tagged

<svid>：service-vlan-id, its range from 1 to 4094

Default: Do not bind port to any VFI, access mode is VLAN and the default Svid is 0.

Command Mode: Port mode

Usage Guide: Use this command to bind port to the specified VFI, it is used in VPLS.

Example:

Switch(config)#interface Ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#xconnect vfi 100 mode vlan svid 200