PIXE L3 8T 4X-R

Industrial Layer 3

10 Gbps Ethernet Switch

CLI Manual

This Page Left Blank Intentionally

1 System Management Configuration 1
1.1 System Security Configuration 1
1.1.1 Multi-user management control 1
1.1.2 Enable Password Control 2

2 CLI Command Line Introduction 1
2.1 Introduction to CLI Mode 1
2.1.1 What CLI mode does 1
2.1.2 Identification of CLI mode 1
2.1.3 Classification of CLI modes 2
2.2 Command Syntax Introduction 3
2.2.1 Command composition 3
2.2.2 Parameter type 3
2.2.3 Command Syntax Rule 3
2.2.4 Command Abbreviation 4
2.2.5 Syntax Help 5
2.2.6 Command line error message 5
2.3 Command Line Shortcut 6
2.3.1 Line Editing Shortcut 6
2.3.2 Show Command Shortcut 6
2.4 History Command 7
2.4.1 TELNET Service Control 7
2.4.2 SNMP Service Control 7
2.4.3 HTTP Service Control 8
2.4.4 HTTPS Service control 8
2.4.5 SSH Service control 8
2.5 System maintenance and commissioning 9
2.5.1 Configure the system's clock 9
2.5.2 Configure Terminal Timeout Properties 10
2.5.3 System Reset 10
2.5.4 View system information 10
2.5.5 Network connectivity debugging 11
2.5.6 Traceroute Debug 11
2.5.7 Telnet client 11
2.5.8 ssh Client 11
2.6 Profile Management 12
2.6.1 View configuration information 12
2.6.2 Save Configuration 12
2.6.3 Delete Profile 13
2.6.4 Configuration file upload and download 13
2.7 Software version upgrade 15
2.7.1 Commands for software version upgrade 15
2.7.2 Software upgrade process 16

3 Configure Port 18
3.3 Configure STORM-CONTROL 20
3.4 Configure STORM-CONSTRAIN 21
3.5 Configure flow-control 23
3.6 Configure port bandwidth 23
3.7 Configure TRUNK 24
3.7.1 LACP protocol configuration 25
3.7.2 Configuration of the trunk group 25
3.7.3 TRUNK Member Port Configuration 25
3.7.4 TRUNK Load Balancing Policy Configuration 26

3.7.5 Display of TRUNK 26
3.8 Configure Jumbo Frame 26
3.8.1 Introduction to Jumbo Frame 26
3.8.2 Jumbo Frame Configuration 26
3.9 Configuring Redundant Port 27
3.9.2 Display of Redundant Port 28
3.10 UDLD Configuration 28
3.11 Configure LLDP 29

4 Configuring Port-Based Security 31
4.1 Introduction 31
4.2 MAC Binding Configuration 31
4.3 MAC filtering configuration 32
4.4 Port Learning Limit Configuration 33
4.5 Protection port configuration 33
4.5.1 Introduction to Protection Port 33
4.5.2 Protection port configuration 34

5 Configure port IP and MAC bindings 35
5.1 Introduction 35
5.2 IP and MAC binding configuration 36
5.3 Configuration examples 36
5.4 Configuration Troubleshooting 37

6 Port Loop Detection 38
6.1 Introduction 38
6.2 Protocol principle 38
6.2.1 Detection Process 38
6.2.2 Recovery Mode 38
6.2.3 Protocol Security 38
6.3 Configuration Introduction 39
6.3.1 Global Configuration 39
6.3.2 Display Configuration 40

7 Configuring VLAN 41
7.1 Introduction to VLAN 41
7.1.1 Benefits of VLAN 41
7.1.2 VLAN ID 42
7.1.3 VLAN Port Membership Type 42
7.1.4 Default VLAN for the port 43
7.1.5 VLAN mode of the port 43
7.1.6 VLAN Trunk 43
7.1.7 Forwarding of traffic within a VLAN 44
7.2 VLAN Configuration 45
7.2.1 Create and delete VLAN 45
7.2.2 Configure the VLAN mode of the port 45
7.2.3 VLAN Configuration in ACCESS Mode 46
7.2.4 VLAN Configuration in TRUNK Mode 46
7.2.5 VLAN Configuration in HYBRID Mode 47
7.2.6 Viewing VLAN Information 47
7.3 Example VLAN configuration 48
7.3.1 PORT-based VLAN 48
7.3.2 802.1Q-based VLAN 49

7.4 MAC, IP subnet, protocol VLAN 50
7.4.1 Introduction to MAC, IP Subnet and Protocol VLAN 50
7.4.2 MAC, IP Subnet, Protocol VLAN Configuration 51
7.5 Voice VLAN 52
7.5.1 Introduction to Voice VLAN 52
7.5.2 Voice VLAN Configuration 52
7.5.3 Voice VLAN Configuration Example 53
7.6 VLAN mapping 54
7.6.1 Introduction to VLAN Mapping 54
7.6.2 VLAN mapping configuration 54
7.7 Q-in-Q 54
7.7.1 Introduction to QinQ 54
7.7.2 Q in Q configuration on page 56
7.7.3 QinQ configuration examples 56

8 Configuring QoS 58
8.1.1 QoS based on COS 59
8.1.2 **DSCP based QoS** 59
8.1.3 MAC-based QoS 59
8.1.4 Policy-based QOS 59
8.2 QoS Configuration 60
8.2.1 QoS Configuration 60
8.2.2 Configure the scheduling method 60
8.2.3 Configure queue weight 61
8.2.4 Configure the mapping relationship between DSCP and QosProfile 61
8.2.5 Configuring Port DSCP Based QoS 61
8.2.6 Configure port user priority (COS value) 61
8.3 QoS Configuration Example 61
8.3.1 Policy QoS Configuration Example 62

9 Configuring MSTP 63
9.1.1 Overview 63
9.1.2 Multiple spanning tree domain 63
9.1.3 IST, CIST, and CST 63
9.1.4 Intra-domain operation 64
9.1.5 Interdomain operation 64
9.1.6 Count of hop 64
9.1.7 Boundary Port 65
9.1.8 Interoperability of MSTP and 802.1d STP 65
9.1.9 Port Role 65
9.1.10 Introduction to 802.1D Spanning Tree 67
9.2 MSTP Configuration 68
9.2.1 Default configuration 68
9.2.2 General configuration 68
9.2.3 Domain Configuration 70
9.2.4 Instance Configuration 71
9.2.5 Port configuration 71
9.2.6 PORTFAST related configuration 73
9.2.7 Root Guard related configuration 74
9.3 MSTP Configuration Example 75

10 Configuring EAPS 76
10.1 EAPS introduction 76
10.2 EAPS Basic concepts 76
10.3 EAPS Protocol introduction 76
10.3.1 Link-Down Give an alarm 77
10.3.2 Loop check 77
10.3.3 Ring recovery 77
10.3.4 EAPS compatible with extreme 78
10.3.5 More EAPS Domain 78
10.4 EAPS configuration 78
10.5 Restrictions 78
10.6 EAPS Brief introduction of command 78
10.6.1 EAPS Configuration command 79
10.7 Single ring configuration example 80
10.8 Cross ring data forwarding configuration example 83

11 Configuring ERPS 86
11.1 ERPS Overview 86
11.2 Introduction to ERPS Technology 86
11.2.1 ERPS ring 86
11.2.2 ERPS Node 86
11.2.3 Link and channel 87
11.2.4 ERPS VLAN 87
11.3 ERPS operating principle 87
11.3.1 Normal State 87
11.3.2 Link failure 88
11.3.3 Link Recovery 88
11.4 Technical features of ERPS 89
11.4.1 ERPS Load Balancing 89
11.4.2 Good safety 89
11.4.3 Support multi-loop intersection tangency 90
11.5 ERPS protocol command 91
11.6 ERPS Typical Application 92
11.6.1 Single Ring Example 92
11.6.2 Multi-loop examples 95
11.6.3 Multi-Instance Load Balancing Example 99

12 Configure AAA 106
12.1 802.1x Introduction 106
12.1.1 802.1x device composition 107
12.1.2 Introduction to Protocol Package 108
12.1.3 Protocol flow interaction 109
12.1.4 802.1x Port Status 110
12.2 RADIUS Introduction 111
12.2.1 Introduction to Protocol Package 111
12.2.2 Protocol flow interaction 112
12.2.3 User authentication method 113
12.3 Configuring 802.1x 114
12.3.1 802.1x Default Configuration 114
12.3.2 Turning 802.1x On and Off 114
12.3.3 Configure 802.1x port state 114
12.3.4 Configure the recertification mechanism 115
12.3.5 Configure the maximum number of hosts connected to the port 115

12.3.6 Configure the interval time and number of retransmission 115
12.3.7 Configure the port as a transmit port 116
12.3.8 Configure 802.1x client version number 116
12.3.9 Configure whether to check client version number 116
12.3.10 Configure authentication method 116
12.3.11 Configure whether to check the timing packet of the client 117
12.3.12 Displaying 802.1x information 117
12.4 Configure RADIUS 117
12.4.1 RADIUS Default Configuration 117
12.4.2 Configure the address of the authentication server 118
12.4.3 Configure Shared Secret 118
12.4.4 Start and stop billing 118
12.4.5 Configure RADIUS port and attribute information 118
12.4.6 Configure RADIUS roaming 119
12.4.7 Display RADIUS information 119
12.5 Configuration examples 119
12.6 TACACS+ Introduction 119

13 Configuring GMRP 121
13.1 Introduction to GMRP 121
13.2 Configure GMRP 121
13.2.1 Turn on GMRP settings 121
13.2.2 Viewing GMRP Information 122
13.3 GMRP Typical Configuration Example 122

14 Configuring IGMP SNOOPING 123
14.1 IGMP SNOOPING Introduction 123
14.1.1 IGMP SNOOPING process 123
14.1.2 Layer-2 dynamic multicast 124
14.1.3 Join a group 124
14.1.4 Leave a group 125
14.1.5 IGMP Querier 126
14.1.6 IGMP snooping multicast filtering 126
14.2 IGMP SNOOPING Configuration 126
14.2.1 IGMP SNOOPING Default Configuration 126
14.2.2 Turn IGMP SNOOPING ON and OFF 127
14.2.3 Configuration Lifetime 127
14.2.4 Configuring fast-leave 127
14.2.5 Configure MROUTER 127
14.2.6 Configure IGMP snooping query port function 128
14.2.7 Configuring the IGMP snooping query feature 128
14.2.8 Configure IGMP snooping multicast filtering 128
14.2.9 Display Information 128
14.3 IGMP SNOOPING Configuration Example 129
14.3.1 Configuration 129

15 MVR Configuration 130
15.1 Introduction to MVR 132
15.2 Configure MVR 132
15.3 MVR Configuration Example 133

16 Configuring DHCP Snooping 135
16.1 Introduction to DHCP SNOOPING 135
16.1.1 DHCP SNOOPING Handling Procedure 133
16.1.2 DHCP SNOOPING Binding Table 133
16.1.3 DHCP SNOOPING Specifies the physical port of the linked server 134
16.2 DHCP SNOOPING Configuration 134
16.2.1 DHCP SNOOPING Default Configuration 134
16.2.2 Turning DHCP SNOOPING on and off globally 134
16.2.3 Interface DHCP SNOOPING ON and OFF 135
16.2.4 Interface DHCP SNOOPING OPTION8 ON and OFF 135
16.2.5 Display Information 135
16.3 DHCP SNOOPING Configuration Example 136
16.3.1 Configuration 136
16.4 DHCP SNOOPING Configuration Troubleshooting 137

17 DHCP CLIENT Configuration 138
17.1 Introduction to DHCP CLIENT 138
17.2 DHCP CLIENT Configuration 138

18 DHCP RELAY 139
18.1 Introduction to DHCP RELAY 139
18.2 DHCP RELAY Configuration 140
18.2.1 Start the DHCP-relay function of the interface 140
18.2.2 Display Information 140
18.3 DHCP RELAY Configuration Example 140

19 DHCP CLIENT Configuration 141
19.1 Introduction to DHCP CLIENT 141
19.2 DHCP SERVER Configuration 143
19.2.1 Start the global DHCP server function 143
19.2.2 Start the interface to receive the DHCP server message 143
19.2.3 Configure address pool 143
19.2.4 Configure address pool ran 143
19.2.5 Configure address pool subnet mask 144
19.2.6 Configure address pool lease 144
19.2.7 Configure the address pool default gateway 144
19.2.8 Configure address pool DNS server 144
19.2.9 Configure manual exclusion addresses in address pool 144
19.2.10 Configure OPTION82 145
19.2.11 Clear Allocated Address Table Entry 145
19.2.12 Clear address entry with conflict detected 145
19.3 DHCP SERVER Configuration Example 145

20 Configuring ACL 148
20.1 ACL Resource Library Introduction 148
20.2 ACL Filtering Introduction 149
20.2 ACL Filtering Introduction 149
20.3 ACL Resource Pool Configuration 151
20.4 ACLTime-based ACL 153
20.5 ACL filtering configuration 154
20.6 ACL Configuration Example 154
20.7 ACL Configuration Troubleshooting 155

21 Basic TCP/IP Configuration 156
21.1 Configure VLAN interface 156
21.2 Configure ARP 157
21.2.1 Configure static ARP 157
21.2.2 View ARP information 158
21.3 Configure Static Routine 158
21.4 TCP/IP Basic Configuration Example 160
21.4.1 Layer Three interface 160
21.4.2 Static Route 160
21.4.3 ARP 161

22 Configuring SNMP 162
22.1 Introduction to SNMP 162
22.2 SNMP Configuration 163
22.3 SNMP Configuration Example 164
22.3.1 Configuration 164

23 RMON Configuration 165
23.1 RMON Introduction 165
23.2 RMON Configuration Example 166

24 Cluster Configuration 168
24.1 Introduction to Cluster Management 168
24.1.1 Cluster Definition 168
24.1.2 Cluster Role 169
24.1.3 NDP Introduction 169
24.1.4 NTDP Introduction 170
24.1.5 Cluster management and maintenance 170
24.1.6 Management VLAN 173
24.2 Introduction to Cluster Configuration 174
24.3 Configuration management device 174
24.3.1 Enables NDP functionality for the system and port 174
24.3.2 Configure NDP parameter 175
24.3.3 Enable NTDP functionality for system and interface 175
24.3.4 Configuring NTDP Parameters 176
24.3.5 Configure manual collection of NTDP information 176
24.3.6 Enable cluster function 176
24.3.7 Set up a cluster 176
24.3.8 Configure intra-cluster member interaction 178
24.3.9 Configure cluster member management 179
24.4 Configure Member Device 179
24.4.1 Enables NDP functionality for the system and port 179
24.4.2 Enables NTDP functionality for the system and port 179
24.4.3 Configure manual collection of NTDP information 179
24.4.4 Enable cluster function 179
24.5 Configure access to cluster member 179
24.6 Cluster Management Display and Maintenance 180
24.7 Typical Configuration Example of Cluster Management 180

25 SNTP Configuration 183
25.1 Introduction to SNTP 183
25.2 Configuring SNTP 183
25.2.1 Default SNTP settings 183
25.2.2 Configure SNTP Server Address 183

25.2.3 Configure the interval of SNTP synchronization clock 184
25.2.4 Configure the local time zone 184
25.3 Information display of SNTP 184

26 Configuring PTP 185
25.26.1 Introducing PTP 185
25.26.2 Configuring PTP 185
25.27.25.26.2.1 PTP
Settings 185
25.27.25.26.2.2
Configure the protocol version of the interface 186
25.26.3 IGMP configuration 186

27 Configuring IGMP 187
25.27.1 IGMP introduction 187
25.27.2 IGMP configuration 188
27.2.1 Start IGMP function of interface 188
27.2.2 Configure the group filter access control list for the interface 188
27.2.3 Configure the access control list filtered by the interface leaving the group 188
27.2.4 Number of specific group queries for the configuration interface 189
27.2.5 Configure the specific group query interval of the interface 189
27.2.6 Configure the non querier timer time of the interface 189
27.2.7 Configure the query timer interval of the interface 190
27.2.8 Configure the maximum response time of the interface 190
27.2.9 Configure interface parameters 190

28 Configuring PIM-SM 191
25.28.1 PIM-SM introduction 191
25.28.2 PIM-SM configuration 192
28.2.1 Start multicast routing function 193
28.2.2 Configure multicast routing table capacity 193
28.2.3 Configure TTL value of multicast interface 193
28.2.4 Start interface PIM SM function 194
28.2.5 Configure passive mode of interface 194
28.2.6 Configure interface priority 194
28.2.7 The configuration interface Hello message does not contain genid information 194
28.2.8 Configure interface Hello timer interval 195
28.2.9 Configure the holding time of neighbours on the interface 195
28.2.10 Configure neighbour list filtering of the interface 195
28.2.11 Configure the source address of unicast registration message 196
28.2.12 Configure the number limit of registered message 196
28.2.13 Check RP when configuring registration 196
28.2.14 Configure registration inhibit timer time value 196
28.2.15 Configure and register Kat timer time value 197
28.2.16 Registration address configuration 197
28.2.17 Configure the checksum of the registered message in Cisco mode 197
28.2.18 Configure static RP address 198
28.2.19 Configure candidate RP 198
28.2.20 Configure ignore RP set priority 198
28.2.21 Configure c-rp-adv message in Cisco mode 198
28.2.22 Configure candidate BSR 199
28.2.23 Configure JP timer interval 199
28.2.24 Configure SPT switching 199
28.2.25 Configure SSM 200

28.2.26 Configure multicast security 200
28.3 PIM-SM Configuration example 200

29 Configuring RIP 203
29.1 RIP Introduction 203
29.2 RIP Configuration 204
29.2.1 Start RIP and enter RIP configuration model 204
29.2.2 Enable RIP interface 204
29.2.3 Configure unicast message transmission 205
29.2.4 Configure the working status of the interface 205
29.2.5 Configure the default route weight 205
29.2.6 Configuration management distance 206
29.2.7 Configure the timer 206
29.2.8 Configuration version 206
29.2.9 Introducing external routing 207
29.2.10 Configure route filtering 207
29.2.11 Configure additional routing metric 207
29.2.12 Configure the RIP version of the interface 208
29.2.13 Configure the receiving and sending status of the interface 209
29.2.14 Configure split horizon 209
29.2.15 Message authentication 209
29.2.16 Configure interface weight 210
29.2.17 Display Information 210
29.3 Sample RIP configuration 211

30 Configuring RIPng 212
30.1 RIPng introduction 212
30.2 RIPng configuration 212
30.2.1 Start RIPng and enter RIPng configuration mod 213
30.2.2 Enable RIPng interface 213
30.2.3 Configure specific neighbours to send updates 213
30.2.4 Configure the working state of the interface 213
30.2.5 Configure default routing weights 214
30.2.6 Introducing external routing 214
30.2.7 Configure routing filtering 215
30.2.8 Configure additional routing weight 215
30.2.9 Configure horizontal segmentation 215
30.2.10 Configure interface weights 216
30.2.11 Display information 216
30.3 RIPng configuration example 217

31 Configuring OSPF 218
31.1 OSPF Introduction 218
31.2 OSPF configuration 219
31.2.1 Start OSPF and enter OSPF model 220
31.2.2 Enable interface 220
31.2.3 Specified host 220
31.2.4 Configure the router ID 221
31.2.5 Configuration of Adjacent Points 221
31.2.6 Prohibit the interface from sending messages 222
31.2.7 Configure SPF compute times 222
31.2.8 Configuration management distance 223
31.2.9 Introducing external routing 223
31.2.10 Configure the network type of the interface 224

31.2.11 Configure the time interval for sending the hello message 224
31.2.12 Configure that failure time of the neighbour router 225
31.2.13 Configure retransmission times 225
31.2.14 Configure interface delay 225
31.2.15 Configure the priority of interfaces in DR election 226
31.2.16 Configure the cost of sending messages on the interface 226
31.2.17 Configure whether to fill MTU value in DD messages sent by interface 226
31.2.18 Configure interface message authentication 227
31.2.19 Configure area virtual link 227
31.2.20 Configure regional route aggregation 228
31.2.21 Configure regional message authentication 229
31.2.22 Configure the nssa area 229
31.2.23 Configure external route aggregation 230
31.2.24 Configure the default metric of the external route 230
31.2.25 Display Information 230
31.3 Sample OSPF configuration 231

32 Configuring OSPFv3 233
32.1 OSPFv3 introduction 233
32.2 OSPFv3 configuration 234
32.2.1 Start OSPFv3 and enter OSPFv3 configuration mode 234
32.2.2 Configure router ID 235
32.2.3 Prohibit the interface from sending messages 235
32.2.4 Configure SPF calculation time 236
32.2.5 Configure management distance 236
32.2.6 Introducing external routing 236
32.2.7 Configure the network type of the interface 237
32.2.8 Configure Hello message sending interval 238
32.2.9 Configure neighbour router expiration time 238
32.2.10 Configure retransmission time 238
32.2.11 Configure interface delay 239
32.2.12 Configure the priority of interface in Dr election 239
32.2.13 Configure the cost of sending messages on the interface 240
32.2.14 Whether to fill in MTU domain for DD message sent by configuration interface 240
32.2.15 Configure regional virtual link 240
32.2.16 Configure regional routing aggregation 241
32.2.17 Configure stub area 241
32.2.18 Configure default weights for external routes 242
32.2.19 Display information 242
32.3 OSPFv3 Configuration example 243

33 Configuring BGP 244
33.1 BGP introduction 244
33.2 BGP configuration 246
33.2.1 Start BGP and enter BGP configuration mode 246
33.2.2 Inject routing information into BGP protocol 246
33.2.3 Configure BGP timer 246
33.2.4 Configure BGP and IGP synchronization 246
33.2.5 Configure the interaction between BGP and IGP 247
33.2.6 Selection of BGP optimal path 247
33.2.7 Configure BGP routing aggregation 248
33.2.8 Configure BGP routing reflector 248
33.2.9 Configure BGP's as Federation 249
33.2.10 Configure BGP management distance 249

33.2.11 Configure BGP routing update mechanism 249
33.2.12 Configure BGP local AS 250
33.3 BGP Configuration example 250

34 Configuring VRRP 252
34.1 VRRP Introduction 252
34.1.1 VRRP Overview 252
34.1.2 VRRP Terminology 254
34.1.3 VRRP protocol interaction 255
34.1.4 Election of virtual master router 256
34.1.5 Status of the virtual router 257
34.1.6 VRRP tracing 258
34.2 VRRP configuration 259
34.2.1 Create and delete virtual router 259
34.2.2 Configure the virtual IP address of the virtual router 260
34.2.3 Configure parameters for the virtual router 260
34.2.4 Configuring VRRP Tracing 261
34.2.5 Starting and shutting down the virtual router 262
34.2.6 View VRRP Information 262
34.3 VRRP Configuration Example 263

35 Configuring VLLP 264
35.1 Introduction to VLLP 264
35.2 VLLP configuration 267
35.2.1 Create a vllp device on a Layer 3 interface 267
35.2.2 Enable the vllp device 267
35.2.3 Create a vllp port on the Layer 2 interface 267
35.2.4 Configure vllp device priority 267
35.2.5 Configure the vllp device query timer interval 268
35.2.6 Configure an affiliated VLAN 268
35.2.7 Configure vllp port priority 268
35.2.8 Display Information 268
35.3 VLLP Configuration Example 269

36 Configuring Policy Routing 271
36.1 Introduction to Policy Routing 271
36.2 Policy routing configuration 271
36.2.1 Create a new policy route 271
36.2.2 Insert a policy route 271
36.2.3 Delete a policy route 272
36.2.4 Move a policy route 272
36.2.5 View policy routing information 272
36.3 Policy Routing Configuration Example 272

37 Configuring the System Log 273
37.1 System Log Introduction 273
37.1.2 Log storage 274
37.1.3 Log display 275
37.1.4 Debugging tool 275
37.2 Syslog Configuration 275
37.2.1 Configure terminal real-time display switch 275
37.2.2 Set Log Level 276
37.2.3 View log information 276
37.2.4 Configure debugging switch 276

37.2.5 View debugging information 277
37.3 Configuring SYSLOG 278
37.3.1 Introduction to SYSLOG 278
37.3.2 SYSLOG configuration 278
37.3.3 SYSLOG Configuration Example 279

38 IPv6 Basic Configuration 280
38.1 Introduction to IPv6 280
38.1.1 IPv6 Protocol Features 280
38.1.2 IPv6 Address Introduction 281
38.1.3 Introduction of IPv6 Neighbour Discovery Protocol 284
38.1.4 IPv6 PMTU discovery 287
38.1.5 Protocol Specification 288
38.2 Introduction to basic IPv6 configuration tasks 288
38.3 Configure basic functions of IPv6 288
38.3.1 Configure IPv6 unicast address 288
38.4 Configure IPv6 Neighbour Discovery Protocol 289
38.4.1 Configure relevant parameters of RA message 289
38.4.2 The number of times a Neighbour Solicition message is sent when duplicate address detection is configured 291
38.5 IPv6 Static Route Configuration 292
38.6 IPv6 display and maintenance 292

39 MLD SNOOPING Configuration 293
39.1 Introduction to MLD SNOOPING 293
39.1.1 MLD SNOOPING process 293
39.1.2 Layer-2 dynamic multicast 294
39.1.3 Join a group 294
39.1.4 Leave a group 296
39.2 MLD SNOOPING configuration 296
39.2.1 MLD SNOOPING default configuration 296
39.2.2 Opening and closing MLD SNOOPING 296
39.2.3 Configuration Lifetime 297
39.2.4 Configuring fast-leave 297
39.2.5 Configure MROUTER 297
39.2.6 Configure the startup VLAN querier 297
39.2.7 Display Information 298
39.3 MLD SNOOPING Configuration Example 298

40 PoE Configuration 299
40.1 Introduction to POE 299
40.2 Configure POE 299
40.2.1 Manual POE configuration 299
40.2.2 POE policy configuration 300
40.2.3 PD query configuration 301

41 GVRP Configuration 302
41.1 Introduction to GVRP 302
41.2 Configure GVRP 302
41.2.1 Enable GVRP settings 303
41.2.2 View GVRP information 303

1. System Management Configuration

Before learning the relevant function configuration of the switch, the user needs to master the basic configuration of the system management and maintenance of the switch. This chapter describes the basic configuration of the system management and maintenance, mainly including the following contents:

- System Security Configuration
- System maintenance and commissioning
- System Monitoring
- Profile Management
- Software version upgrade

1.1. System Security Configuration

In order to prevent illegal users from invading the switch, the system provides several security measures for system management, mainly including:

- Multi-user management control
- Enable Password Control
- TELNET Service Control
- SNMP Service Control
- HTTP Service Control

1.1.1. Multi-user management control

Multi-user management not only ensures the security of the switch system, but also provides the ability for multiple users to manage and maintain the switch at the same time. Multi-user management ensures system security by giving each user a user name, password and permission. Users need to verify the user name and password first when accessing the switch. Only when the user name and password are correct and consistent can they pass the verification. The user can access the switch after passing the authentication, but the user's authority limits the scope of user access to the switch.

Multi-user management divides the user's authority into two levels: ordinary user and privileged user. The normal user can only stay in the normal mode of the CLI command line interface and can only use the display command to query the information of the switch. Privileged users have access to all modes of the CLI command line interface and can use all commands provided by the CLI to query the switch for information and to maintain and manage the switch.

The multi-user management feature applies only to Telnet terminals and does not control Console terminals. Username and password authentication is not required to access the switch using the Console terminal, and the user can access the CLI directly. The user name and password need to be verified when accessing the switch through the Telnet terminal, and the CLI can be accessed only after the user name and password are verified.

The default user name and password of the switch are admin. The admin user must be an administrator, that is, a privileged user. It cannot be configured as an ordinary user, and the admin user cannot be deleted.

Commands related to multi-user management are shown in the following table:

Command	Describe	CLI Mode
username <user-name> password <key> {normal | privilege}	Add a user. If the specified user already exists, modify the password and permission of the user. The first parameter is the user name, the second parameter is the password, the optional represe nts the permission, the normal represents the nor mal user, and the privilege represents the privile ged user.	Global Configuration Mode
no username [user-name]	Deletes a user with the specified user name.	Global Configuration Mode
show running-config	View the current configuration of the system to view the configuration of multi-user management.	Privileged Mode

1.1.2. Enable Password Control

The enable password is used to control the switch from normal mode to privileged mode. Before the enable password is verified, the user can only view the information of the switch. After the enable password is verified, the user can configure and maintain the switch.

The enable password is not dependent on the user. Any user who logs in to the Console terminal or Telnet terminal must verify the enable password if he wants to enter the privileged mode. If the verification fails, he can only stay in the normal mode.

Enter the enable command in the normal mode, and the terminal will prompt the user to enter the password. At this time, the user can enter the enable password. If the password is verified successfully, the terminal enters the privileged mode. Otherwise, the terminal stays in the normal mode. For ordinary users, no matter whether the password is verified successfully, they cannot enter the privileged mode.

The enable password is empty by default. In this case, after the enable command is entered in the normal mode, the terminal directly enters the privileged mode without prompting for the password.

The commands related to enable password are shown in the following table:

Command	Describe	CLI Mode
enable password <key>	Set the enable password for the system.	Global Configuration Mod e
no enable password	Clear the enable password of the system. The enable password is blank.	Global Configuration Mod e
show running-config	View the current configuration of the system t o view the configuration of the enable passwor d.	Privileged Mode
enable	Interactive command to verify the enable pass word of the system. After successful verificati on, the terminal enters the privileged mode.	Normal Mode

Note: For system security, the administrator needs to set the enable password of the system.

2. CLI Command Line Introduction

This chapter describes the CLI command line interface in detail, mainly including the following contents:

- Accessing the CLI of the switch
- Introduction to CLI Mode
- Command Syntax Introduction
- Command Line Shortcut
- History Command

2.1 Introduction to CLI Mode

2.1.1 What CLI mode does

The CLI mode provides the two main functions:
It is convenient to classify users and prevent unauthorized users from using CLI illegally. Users can be divided into two levels, that is, two categories: normal users and privileged users.

- Ordinary users can only view some of the operating status of the switch and can only use the display command.
- In addition to viewing the operational status of the switch, privileged users can also maintain and configure the switch and change the behaviour of the switch.

- **It is convenient for the user to configure the switch.**

There are many configurations in the switch. If all the configurations are put in one mode, it is very inconvenient for users to use. To this end, multiple modes are established on the CLI, and similar commands are placed in one mode, which is convenient for users to understand and use. Uch as placing VLAN-related commands in VLAN configuration mode and interface-related commands in interface configuration mode.

2.1.2 Identification of CLI mode

The CLI prompt is the identification of the CLI mode. When using the CLI, the user can know the current CLI mode by looking at the CLI prompt.

The CLI prompt consists of two parts, one identifying the host and the other identifying the mode. The host part in the CLI prompt uses the host name of the system. The host name of the system is configurable, and the default is Switch. Therefore, the CLI prompt starts with Switch by default, and the CLI descriptor mentioned later generally uses the default host name.

The mode section in the CLI prompt is not configurable. Each mode has its own corresponding mode string. Some mode strings are fixed and some are variable. For example, the mode string of the VLAN configuration mode is fixed, and the mode string of the interface configuration mode is variable.

For example：

The CLI prompt **Switch # identifies** the privileged mode, Switch identifies the host, and # identifies the mode.
The CLI prompt Switch **(config-ge1/1) #** identifies the interface configuration mode, and the ge1/1 port is configured. Switch identifies the host, and (config-gel/1) # identifies the mode.

The CLI prompt **switch (config-vlan2) #** identifies the interface configuration mode, and the vlan2 interface is configured. Switch identifies the host, and (config-vlan2) # identifies the mode

2.1.3 Classification of CLI modes

CLI modes are divided into four categories: normal mode, privileged mode, global configuration mode and configuration sub-mode. The configuration sub-mode is composed of many CLI modes.

Normal users have access only to normal mode, and privileged users have access to all CLI modes.

The following table lists the main CLI modes for the switch:

Pattern	Describe	Prompt	Command to enter mode	Command to exit mode
Normal Mode	Provides the display command to view status information for the switch	**Switch>**	The mode that the terminal enters first.	There is no exit mode command on the Console terminal. Use the exit or quit command on the Telnet terminal to exit the Telnet terminal
Privileged Mode	In addition to providing display commands to view the status information of the switch, it also provides commands such as debugging, version upgrade, and configuration maintenance.	**Switch#**	Enter the enable command in normal mode.	Use the disable command to return to normal mode. Use the exit or quit command on the Console terminal to exit to normal mode and the exit or quit command
Global Configuration Mode	Provides generic commands that cannot be implemented within the configuration submode, such as the configure static route command.	**Switch(config)#**	Enter configure in privileged model The terminal command.	Use the exit, quit, or end command to exit to privileged mode
Interface Configuration Mode	Provides commands for configuring ports and VLAN interfaces.	**Port：Switch (configge1/1)# VLANInterface：Switch (config-vlan1)#**	Enter the interface < if-name > command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.
VLAN Configuration Mode	Commands to configure VLANs are provided. Such as commands to create and delete VLANs.	**Switch(config-vlan)#**	Enter the VLAN database command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.
MSTP Configuration Mode	Commands to configure MSTP are provided. such as the commands to create and delete an MSTP instance.	**Switch(config-mst)#**	Enter the spanning-tree mst configuration command in global configuration mode	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.
Terminal Configuration Mode	Commands are provided to configure Console and Telnet terminals, such as a timeout for the terminal.	**Switch(config-line)#**	Enter the line vty command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode

Console and Telnet terminals first enter the normal mode, enter the enable command in the normal mode, and enter the privileged mode after successfully verifying the password. On a Telnet terminal, a normal user can only stay in normal mode and cannot enter privileged mode. Enter configure terminal in privileged mode to enter CLI mode into global configuration mode. Each configuration submode can be entered by entering the relevant command in the global configuration mode.

Normal users have access only to normal mode, and privileged users have access to all CLI modes.

Console and Telnet terminals first enter the normal mode, enter the enable command in the normal mode, and enter the privileged mode after successfully verifying the password. On a Telnet terminal, a normal user can only stay in normal mode and cannot enter privileged mode. Enter configure terminal in privileged mode to enter CLI mode into global configuration mode. Each configuration submode can be entered by entering the relevant command in the global configuration mode

2.2 Command Syntax Introduction

2.2.1 Command composition

A CLI command consists of two parts: a keyword and a parameter. The first word must be a keyword, and the following words can be keywords or parameters. Keywords and parameters can appear alternately. A command must have a keyword, but it can have no parameters. For example, the command write has one keyword and no arguments; the command show version has two keywords and no arguments; the command VLAN < vlan-id > has one keyword and one argument; The command instance < instance-id > VLAN < vlan-id > has two keywords and two arguments, and the keywords and arguments alternate.

2.2.2 Parameter type

There are two types of parameters for CLI commands: required and optional.

Required parameters must be entered when entering a command, while optional parameters may or may not be entered.

If the parameter in the command VLAN < vlan-id > is a required parameter, it must be entered when entering the command; while the parameter in the command **show interface [if-name]** is an optional parameter, it may or may not be entered when entering the command.

2.2.3 Command Syntax Rule

1) The following rules must be met when describing commands with text:

Keywords are expressed directly in words.

Such as the command show version.

2) Parameters must be enclosed in < >. Such as the command VLAN < vlan-id >

3) If it is an optional parameter, the parameter must be enclosed in a].

Such as the command show VLAN < vlan-id >]

In this case, the < > of the parameter can be omitted and changed to:

Command show VLAN VLAN-ID]

Command show VLAN VLAN-ID]

If it is a required parameter, the parameter cannot have].

4) If one of multiple keywords or parameters must be selected, enclose multiple keywords or parameters with { }, separate multiple keywords or parameters with |, and require a space before and after |.

For example, a command with more than one keyword required:

spanning-tree mst link-type {point-to-point | shared}

You must choose between point-to-point and shared.

Commands with multiple required parameters:

no arp {<ip-address> | <ip-prefix>}

Keywords and parameters are mandatory commands:

Show spanning-tree mst {none|instance <0-15>}ng

5) If more than one keyword or parameter can be selected, use "to enclose more than one keyword or parameter, separate more than one keywords or parameters with, and need a space before and after.

The command is as follows:

debug ip tcp [recv | send] The keywords recv and send may or may not be selected.

show ip route [<ip-address> | <ip-prefix>]

show interface [<if-name> | switchport]

6) If there is a keyword or parameter or a group of keywords or parameters that can be repeatedly selected and input, add the symbol "*" after the keyword or parameter (group).

For example, ping:

ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*

-j <count> <ip-address>* --- Multiple IP addresses can be entered repeatedly

-k <count> <ip-address>* --- Multiple IP addresses can be entered repeatedly

The entire option can also be entered repeatedly.

7) The parameter is represented by a descriptor of one or more words. If there are multiple words, separate each word with the symbol "-". Each word is lowercase.

Correct argument notation: < vlan-id >, < if-name >, < router-id >, < count >, etc.

Incorrect parameter notation: < 1-255 >, < A. B. C. D >, < WORD >, < IFNAME >, etc.

2.2.4 Command Abbreviation

When a user enters a command on the CLI interface, the keyword for the command can be abbreviated. The CLI supports the prefix matching function of the command. As long as the input word is uniquely matched with the keyword prefix, the CLI will parse the input word into the matching keyword. This is very convenient for the user when using the CLI, and the user can type very few characters to complete a command, for example, the show version command can only type shver.

2.2.5 Syntax Help

Syntax help is set in the CLI command line interface to support the help function of each level of commands and parameters, which are described as follows:

1) Enter directly in one of the CLI modes? The first keyword and its description of all commands in this mode are listed on the terminal. For example Switch (config).

2) Enter the first part of a command, followed by a space and then? On the terminal, all the keywords or parameters of the next level and their descriptions are listed. For example Switch # show?.

3) Enter an incomplete keyword and then enter it directly? All keywords that match this input prefix and their descriptions are listed on the terminal. For example, Switch # show ver?.

4) Enter the first part of a command UNK1, then enter a space and then enter the Tab key. All keywords of the next level will be listed on the terminal. If the next level is a parameter, it will not be listed.

5) UNK1 input an incomplete keyword and then directly input the Tab key. If there is only one keyword matching with the input prefix, it will be completed directly. If there are multiple keywords matching with the input prefix, all matching keywords will be listed on the terminal.

2.2.6 Command line error message

If a command entered by the user fails the syntax check, an error message will be displayed on the terminal. Common error messages are shown in the following table.

Error Message Error Cause

Invalid input or

Unrecognized commandNo matching keywords were found.

Incorrect parameter input.

Too many keywords or parameters have been entered.

Incomplete command Command entry is incomplete, and there are keywords or parameters not entered.

Ambiguous command Keyword input is incomplete. More than one keyword matches the input prefix.

Error Message	Error Cause
Invalid input or Unrecognized command	No matching keywords were found. Incorrect parameter input. Too many keywords or parameters have been entered.
Incomplete command	Command entry is incomplete, and there are keywords or parameters not entered.
Ambiguous command	Keyword input is incomplete. More than one keyword matches the input prefix.

2.3 Command Line Shortcut

2.3.1 Line Editing Shortcut

The CLI command line interface supports the function of line editing shortcut keys, which can facilitate the input and editing of CLI commands. When users enter or edit commands, they can use the line editing shortcut keys to speed up the entry of commands. The following table lists all the line editing shortcuts and the functions they implement:

Shortcut key	function
Ctrl+p or ↑	Previous command
Ctrl+n or ↓	Next Command
Ctrl+u	Delete entire row
Ctrl+a	Cursor returns to the beginning of the line
Ctrl+f or →	Move the cursor one space to the right
Ctrl+b or ←	Move the cursor one space to the left
Ctrl+d	Delete the character where the cursor is located
Ctrl+h	Delete the character before the cursor
Ctrl+k	Delete all characters at and after the cursor
Ctrl+w	Delete all characters before the cursor
Ctrl+e	The cursor moves to the end of the links
Ctrl+c	Interrupt without executing the command line. If the CLI is in global configuration mode o r configuration submode, the CLI exits to privileged mode; if the CLI is in normal mode or privileged mode, the CLI mode remains the same, but the CLI starts a new line.
Ctrl+z	Same as Ctrl + C.
Tab	Use this key after entering an incomplete keyword. If one keyword matches the prefix ente red, complete the keyword. If more than one keyword matches the prefix entered, list all m atching keywords. If none of the keywords match, the key is invalid.

Note: The ↑, ↓, →, ← keys are not available on some Console terminals

2.3.2 Show Command Shortcut

Commands beginning with the show keyword are all display commands. Some display commands cannot be displayed in one screen because they display a lot of content. The terminal provides the function of split-screen display. After displaying a screen, the terminal waits for user input to determine subsequent processing. The following table lists the display command shortcut keys and their functions.

Shortcut key	**function**
Space	Show next screen
Enter	Show next line
Ctrl+c	Interrupt command execution and exit to CLI model
Other key	Same as Ctrl + C.

2.4 History Command

The CLI command line interface supports the command history function, which can remember the last 20 historical commands used by the user and save the last commands typed by the user.

You can use show history to display the commands that have been entered.

You can also use Ctrl + p, Ctrl + n, or the ↑ and ↓ keys to select the history commands. The history command function makes it easy for the user to enter commands.

2.4.1 TELNET Service Control

In some cases, the administrator does not need to remotely manage the switch, but only needs to manage the switch locally through the Console terminal. At this time, in order to improve the security of the system and prevent illegal users from remotely logging in the Telnet terminal, the administrator can turn off the Telnet service. The Telnet service is on by default.

Commands related to Telnet service control are shown in the following table:

Command	Description	CLI Mode
security-manage telnet enalbe	Turn on the Telnet service.	Global Configuration Mode
security-manage telnet disable	Turn off the Telnet service.	Global Configuration Mode
security-manage telnet number <1-100>	The number parameter can range from 1 to 100. The default is 5.	Global Configuration Mode
security-manage telnet access-group <1-99> (Note: subject to the actual product)	Specify an ACL group to turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address is not controlled.	Global Configuration Mode
no security-manage telnet access-group	Turn off source IP address control.	Global Configuration Mode
show security-manage	You can view the configuration of the service control.	Privileged Mode

2.4.2 SNMP Service Control

The SNMP service control turns the SNMP service on/off and also controls the IP addresses that access the switch through ACLs.

The commands related to SNMP service control are shown in the following table:

Command	describe	CLI Mode
security-manage snmp enalbe	Turn on the SNMP service.	Global Configuration Mode
security-manage snmp disable	Turn off the SNMP service.	Global Configuration Mode
Security-manage snmp access-group <1-99> (Note: subject to the actual product)	Specify an ACL group to turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address is not controlled.	Global Configuration Mode
no security-manage snmp access-group	Turn off source IP address control.	Global Configuration Mode
show security-manage	You can view the configuration of the service control.	Privileged Mode

2.4.3 HTTP Service Control

The HTTP service control can turn on/off the HTTP service and also control the access to the IP address of the switch through ACL.

Commands related to HTTP service control are shown in the following table:

Command	Description	CLI Mode
security-manage http enable	Turn on the HTTP service.	Global Configuration Mode
security-manage http disable	Turn off the HTTP service.	Global Configuration Mode
security-manage http access-group <1-99> (Note: subject to the actual product)	Specify an ACL group to turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address is not controlled.	Global Configuration Mode
no security-manage http access-group	Turn off source IP address control.	Global Configuration Mode
show security-manage	You can view the configuration of the service control.	Privileged Mode

2.4.4 HTTPS Service control

HTTPS service control can turn on / off HTTPS service and control the IP address of access switch through ACL。

The relevant commands of HTTPS service control are shown in the table below ：

Command	Description	CLI mode
security-manage https enalbe	Open HTTP service。	Global configuration mode
security-manage https disable	Close HTTP service。	Global configuration mode
security-manage https access-group <1-99> (Note: subject to the actual product)	Specify an ACL group and turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address will not be controlled.	Global configuration mode
no security-manage https access-group	Turn off source IP address control.	Global configuration mode
show security-manage	You can view the configuration of service control.	Privileged mode

2.4.5 SSH Service control

Traditional network service programs, such as FTP, pop and Telnet, are inherently insecure, because they transmit passwords and data in plaintext on the network. People with ulterior motives can easily intercept these passwords and data. Moreover, the security verification methods of these service programs also have their weaknesses, that is, they are vulnerable to the attack of "man-in-the middle".

The so called "middleman" attack means that the "middleman" pretends to be a real server to receive the data you send to the server, and then pretends to be you to send the data to the real server. After the data transmission between the server and you is tampered with by the "middleman", there will be serious problems.

By Using SSH, you can encrypt all the transmitted data, so that the "man in the middle" attack can not be realized, and it can also prevent DNS spoofing and IP spoofing. Another additional advantage of

Using SSH is that the transmitted data is compressed, so it can speed up the transmission speed. SSH has many functions. It can not only replace Telnet, but also provide a safe "channel" for FTP, pop and even PPP。

The commands related to SSH are shown in the following table

Command	Description	CLI mode
security-manage ssh enalbe	Open ssh service。	Global configuration mode
security-manage ssh disable	Close ssh service。	Global configuration mode
security-manage ssh access-group <1-99>	Specify an ACL group and turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address will not be controlled.	Global configuration mode
no security-manage ssh access-group	SSH turns off source IP address control.	Global configuration mode
ip sshd auth-retries < times>	Set the maximum number of verifications that the client can attempt	Global configuration mode
ip sshd silence-period < seconds>	Set the waiting time after the client exceeds the maximum number of verifications	Global configuration mode
show ip sshd	View the configuration information of sshd	Privileged mode
show security-manage	You can view the configuration of service control.	Privileged mode

2.5 System maintenance and commissioning

The basic system maintenance and commissioning functions mainly include the following:

- Configure the system's clock
- Configure Terminal Timeout Properties
- System Reset
- View system information
- Network connectivity debugging
- Traceroute Debug

2.5.1 Configure the system's clock

The switch provides the function of real-
time clock. The current clock can be set or viewed through the command. The clock of the system is p owered internally to ensure the continuous operation of the real-
time clock when the system is powered off, and the clock does not need to be reset after the system is started.

The clock has been set when the switch leaves the factory, and the user does not need to set it again. If the user finds that the time is not on time, the user can reset the clock.

The commands related to the system clock are shown in the following table

Command	Description	CLI Mode
set date-time <year> <month> <day> <hour> <minute> <second>	To set the current clock of the system , you need to enter the parameters of year, month, day, hour, minute and se cond.	Privileged Mode
show date-time	Displays the current clock of the syst em.	Normal mode, privileged mode

2.5.2 Configure Terminal Timeout Properties

For the security of the terminal, when there is no key input on the terminal, the terminal will exit after a certain time. Console terminal and Telnet terminal exit processing is different. For Console terminal, when the terminal times out, the CLI mode exits to the normal mode. For Telnet terminal, when the t erminal times out, the Telnet connection is interrupted and the Telnet terminal exits.

The default timeout time of the terminal is 10 minutes, and the user can also set the terminal to never t imeout.

Commands related to terminal timeout are shown in the following table

Command	Description	CLI Mode
exec-timeout <minutes> [seconds]	Set the timeout time of the terminal. If the paramete rs are all 0, it means that the terminal will never tim eout.	Terminal Configuration Mode
no exec-timeout	Set the terminal timeout back to the default, which i s 10 minutes.	Terminal Configuration Mode
show running-config	View the current configuration of the system to vie w the configuration of the terminal timeout.	Privileged Mode

2.5.3 System Reset

The system provides a reset method:

Reset the switch

Commands related to system reset are shown in the following table:

Command	Description	CLI Mode
reset	Reset the switch.	Privileged Mode

2.5.4 View system information

The system provides a variety of display commands to view the operating status and information of the system. Here are only a few commonly used display commands for system maintenance, as shown in the following table:

Command	Description	CLI Mode
show version	Displays the version number of the system and the ti me at which the file was compiled and linked.	Normal mode, privile ged mode
show snmp system information	Displays basic information about the system, includi ng how long the system has been running since it wa s started.	Normal mode, privile ged mode
show history	Displays a list of the most recently entered command s on the CLI command line.	Normal mode, privile ged mode

2.5.5 Network connectivity debugging

In order to debug the connectivity between the switch and another device in the network, it is necessary to implement the ping command on the switch and ping the IP address of the other party on the switch. If the switch receives the ping response from the other party, it indicates that the two ends are connected. Otherwise, it indicates that the two ends cannot communicate.

The switch not only implements the ping command, but also supports many options on the ping command that users can use for more precise and complex debugging.

The ping command is shown in the following table:

Command	Description	CLI Mode
ping <ip-address> [-n <count> | -l <size> | -w <timeout>]*	It can be used without any options, or with one or more options. Without any options, it is the simplest ping command. Command execution can be interrupted by typing Ctrl + C when the command is executed.	Privileged Mode

2.5.6 Traceroute Debug

The trace-route command needs to be implemented on the switch in order to debug which intermediate devices the switch passes through when communicating with another device on the network. When using the trace-route command on the switch, the IP address of the other party is specified, and all the paths in the middle are displayed during the execution of the command.

The switch not only implements the trace-route command, but also supports a number of options on the trace-route command that users can use for more precise and complex debugging.

The trace-route command is shown in the following table:

Command	Description	CLI Mode
trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]*	It can be used without any options, or with one or more options. Without any options, this is the simplest trace-route command. Command execution can be interrupted by typing Ctrl + C when the command is executed.	Privileged Mode

2.5.7 Telnet client

The switch provides a Telnet client function, through which the user can remotely access other devices.

Command	Description	CLI Mode
telnet <ip-address>	Parameter is the IP address of the target device	Privileged Mode

2.5.8 ssh Client

Series switches provide SSH client function, and users can remotely access other devices through SSH client.

Command	Description	CLI mode
ssh <ip-address> [user-name]	SSH client can access other devices remotely	Privileged mode

2.6 Profile Management

The configuration is divided into the current configuration and the initial configuration. The current configuration refers to the configuration when the system is running, which is stored in the memory of the system, while the initial configuration is the configuration used when the system is started, which is stored in the FLASH of the system, that is, the configuration file. When the user executes the relevant command, the current configuration of the system is modified. Only after the save command is executed, the current configuration is written into the initial configuration for the next startup of the system. After the system is started, the current configuration information of the system is the same as the initial configuration information when the user does not make any configuration.

The current configuration and the initial configuration use the same format, which is the format of command line text, which is very intuitive and easy for users to read. The format of the configuration file has the following characteristics:

- The configuration file is a text file.
- All saved are commands.
- Only the non-default configuration is saved, and the default configuration is not saved.
- Commands are organized according to the CLI mode. Commands in the same CLI mode are organized together to form a segment, and the segments are separated by "!". For the commands in the global configuration mode, the commands with the same function or similar functions are organized into a segment and separated by "!".
- Commands in configuration submode are preceded by a space, while commands in global configuration mode are not required to be preceded by a space.
- End the configuration with "end".

Configuration file management mainly includes the following contents:

- View configuration information
- Save Configuration
- Delete Profile
- Configuration file upload and download

2.6.1 View configuration information

Viewing configuration information includes viewing the current and initial configuration of the system. The initial configuration is actually the configuration file in FLASH. When the configuration file does not exist in FLASH, the default configuration is used when the system is started. At this time, if you view the initial configuration of the system, the system will prompt that the configuration file does not exist.

Commands for viewing configuration information are shown in the following table

Command	Description	CLI Mode
show running-config	View the current configuration of the system.	Privileged Mode
show startup-config	Review the initial configuration of the system.	Privileged Mode

2.6.2 Save Configuration

When the user modifies the current configuration of the system, these configurations need to be saved to the configuration file, so that these configurations will still exist after the next startup, otherwise, these configuration information will be lost after the restart. To save a configuration is to save the current configuration to the initial configuration.

The commands to save the configuration are shown in the following table:

Command	**Description**	CLI Mode
write	Save the current configuration.	Privileged Mode

Note: Users need to use this command to save the configuration after configuring the switch, otherwise the configuration will be lost after the system is restarted.

2.6.3 Delete Profile

When the user wants the initial configuration of the system to return to the default configuration, the configuration file can be deleted. Deleting the configuration file has no effect on the current configuration. If the user wants the current configuration of the system to return to the default configuration, the switch needs to be restarted. Users must be careful when deleting configuration files, otherwise the configuration will be lost.

The command to delete the configuration file is shown in the following table

Command	**Description**	**CLI Mode**
delete startup-config	Deletes the system's profile.	Privileged Mode

2.6.4 Configuration file upload and download

For the security of the configuration file, the user can use the command to upload the configuration file to the PC for backup. When the system configuration is abnormally lost or modified and the user wants to return to the original configuration, the user can download the original configuration file from the PC to the switch. The downloaded configuration file has no effect on the current configuration of the system, and the configuration will take effect after the switch is restarted. Configuration files can also be uploaded and downloaded through WEB. For specific operations, please refer to the WEB Operation Manual.

The commands downloaded from the configuration file are as follows:

Command	**Description**	**CLI Mode**
upload configure <ip-address> <file-name>	The configuration file is uploaded to the PC, the first parameter is the IP address of the PC, and the second parameter is the file name of the configuration file stored in the PC.	Privileged Mode
download configure <ip-address> <file-name>	The configuration file is uploaded to the PC, the first parameter is the IP address of the PC, and the second parameter is the file name of the configuration file stored in the PC.	Privileged Mode

The TFTP protocol is downloaded from the configuration file, the TFTP client software is run on the switch, and the TFTP server software is run on the PC. To download the configuration file, proceed as follows:

Step 1: Build a network environment.

Step 2: Start the TFTP server software on the PC and set the directory where the configuration file is stored.

Step 3: Save the configuration on the switch.

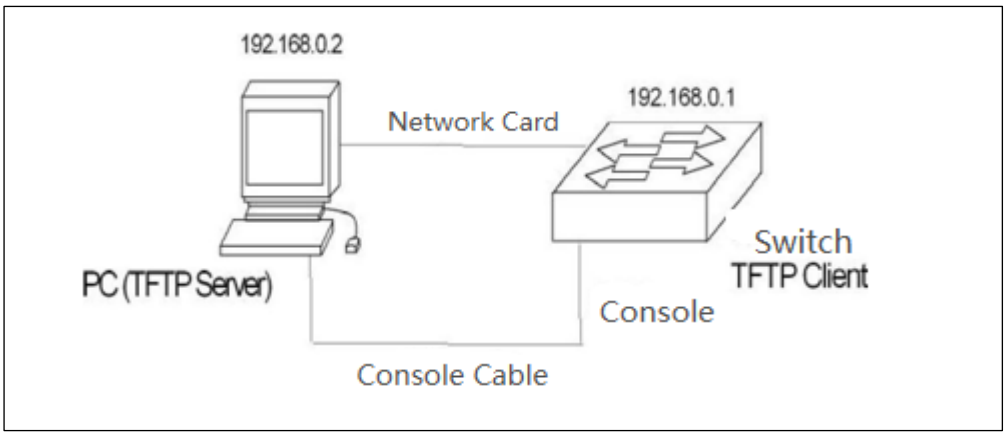
Step 4: Execute the configuration file upload command on the switch to back up the configuration file to the PC.

Step 5: When the switch needs the configuration file on the PC, execute the configuration file download command on the switch to download the configuration file on the PC to the switch.

Step 6: The switch must be restarted for the configuration to take effect

Example: a switch that has been configured with VLANs and interface addresses needs to upload and download configuration files.

Step 1: Set up the network environment as shown below.

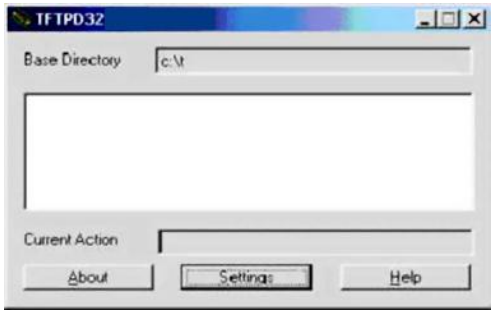


The configuration port of the switch is externally connected with a configuration terminal through a cable, and is connected with a PC through a network cable. Install TFTP Server on the PC and configure the IP address of the Ethernet port of the PC. Here, it is assumed that the IP address of the PC is 192. 168.0.2 。 Next, configure the IP address of the switch, assuming that the IP address of the switch is the 192.168. 0 . 1. Ensure connectivity between the PC and the switch.

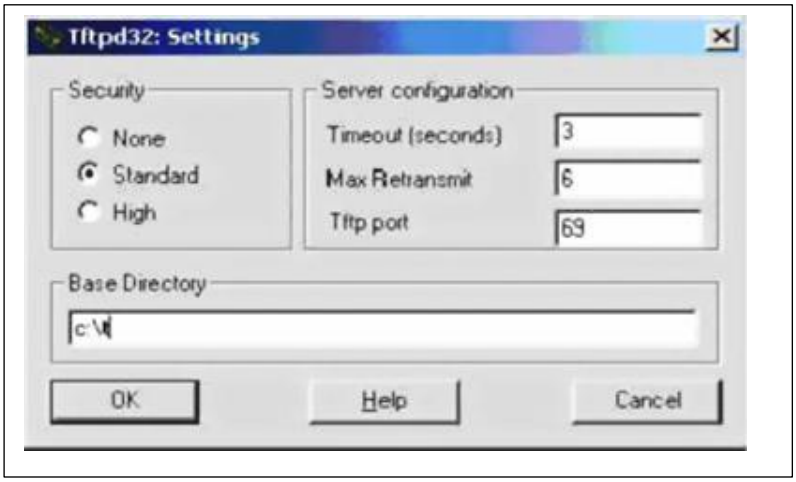
Step 2: Start TFTP Server and configure TFTP Server parameters.

Run TFTP Server, and the window interface is as shown below:

Diagram 2.3.4 TFTP Screen



Then, set the directory where the configuration files are backed up. The specific operation is to click the [Settings] button to enter the setting interface, as shown in the following figure:



Enter the file path in the Base Directory ". Click the [OK] button to confirm.

Step 3: Execute the write command on the switch to save the current configuration to the configuration file.

Step 4: Back up the file to the PC and execute the command Switch # upload configuration 192.168.0.2 beifen. CFG.

Step 5: If necessary, download the backup file to the switch and execute the command Switch # download configuration 192.168.0.2 beifen. CFG.

Step 6: For the downloaded configuration file to take effect, you must restart the switch and execute the command Switch # reset.

2.7 Software version upgrade

The switch supports online upgrades of software versions. The upgrade is done through the tool TFTP.

2.7.1 Commands for software version upgrade

1) Upgrade the switch file of the switch in the global configuration mode with the following command: **download switch <ip-address> <file-name>**
Where < ip-address > is the IP address of the PC running the TFTP server and < file-name > is the name of the switch file saved on the TFTP server.

2) Upgrade the kernel file of the switch in the global configuration mode with the following command: **download kernel <ip-address> <file-name>**
Where < ip-address > is the IP address of the PC running the TFTP server and < file-name > is the name of the kernel file saved on the TFTP server.

3) Upgrade the patch file of the switch in global configuration mode with the following command:
download patch <ip-address> <file-name>
Where < ip-address > is the IP address of the PC running the TFTP server and < file-name > is the name of the patch file saved on the TFTP server.

4) Upgrade the uboot file of the switch in the global configuration mode with the following command: **download uboot <ip-address> <file-name>**
Where < ip-address > is the IP address of the PC running the TFTP server and < file-name > is the uboot file name saved on the TFTP server.

Do not power off the switch during the upgrade process, otherwise the switch files may be damaged and the switch may not be able to start. After the download is complete, the switch needs to be rebooted to run the appropriate file program for the new download. The entire upgrade process will take a few minutes. Please be patient.

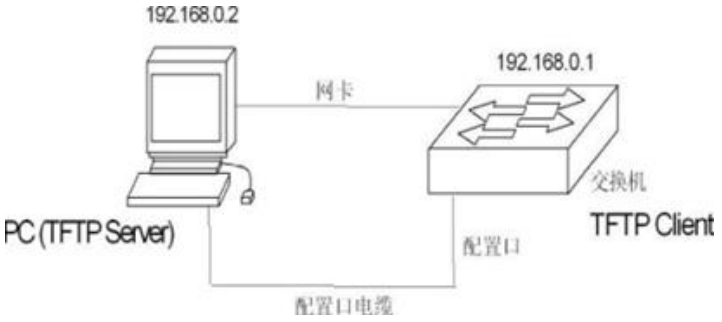
The software version can also be upgraded through WEB. For specific operation, please refer to the WEB Operation Manual.

2.7.2 Software upgrade process

Steps to upgrade switch and other files are as follows:

Step 1: Set up the upgrade environment. As shown in the figure below.

Diagram Software Upgrade



The Upgraded process is as follows:

Connect the Console port of the switch to a configuration terminal (PC) via a cable.

Connect the PC to the TFTP Server

Copy the new switch and other files to a certain path on the PC, assuming that the path is C: \ t;

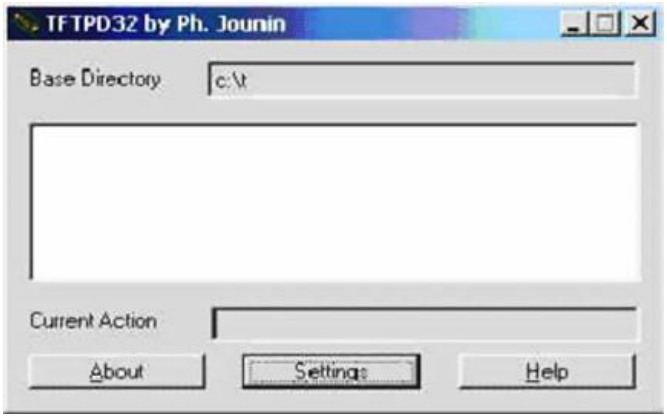
Configure the IP address of the Ethernet port of the PC. It is assumed that the IP address of the PC is 192.168.0.2.

Configure the IP address of the switch, assuming that the switch IP address is 192.168.0.1.

Step 2: Run TFTP Server and configure the TFTP server.

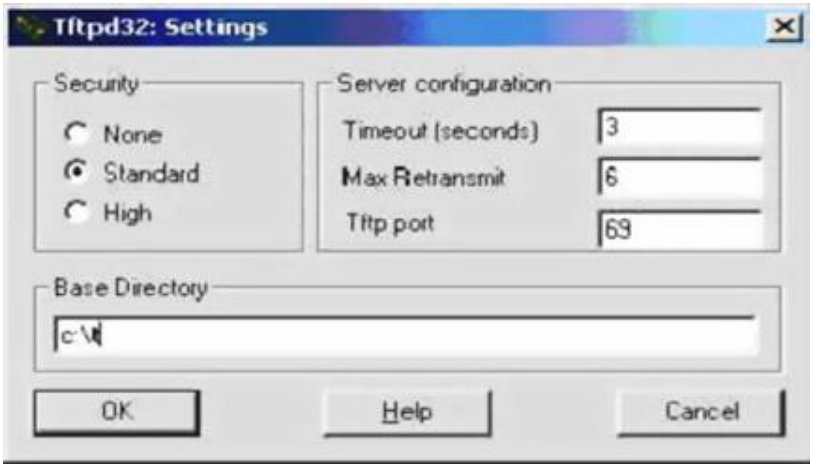
First: Run TFTP Server. The TFT PD32 window interface is shown in the figure below:

Software Upgrade Step 2



Then: Set the TFTP Server file directory. After starting the TFTP Server, reset the TFTP Server file directory, and copy the switch and other files to be loaded to this directory. To do this, click the [Settings] button to display the TFTPD32 setting interface, as shown below.

Software Upgrade Setting TFTP Server File



Enter the file path in the Base Directory ". Click the [OK] button to confirm.

Step 3: Upgrade the file.

First, connect the port on the switch to a PC running the TFTP Server program with an Ethernet cable. And use that ping command to detect connectivity between the host and the switch.

Then: Enter the command at the HyperTerminal Switch # prompt:

Switch# download switch 192.168.0.2 switch.img, press Enter,and wait for the completion of file upgrade.

Software is updating. Please wait and down't powerdown!

……

Updating is completed. Do you wish to reset?[Y/N]

After the file is transferred, the system will prompt you whether you need to restart the switch. Generally, we recommend you to restart the switch by selecting the 'Y', because the system upgrade can only take effect after the switch is restarted. If your configuration file is not saved, you can select the 'N' first, and then restart the switch after other operations such as saving are completed.

Switch#

Note:

The switch should not be powered down during the upgrade process.

Step 4: Reboot the switch.

Switch# reset

3. Configure Port

This chapter introduces the configuration related to the port, mainly including the following contents:

- General configuration of the port
- Configure MIRROR
- Configure STORM-CONTROL
- Configure flow-control
- Configure port bandwidth
- Configure TRUNK

3.1 General configuration of the port

The administrator can control the users under the port by configuring the port of the switch. If the users under the port are not allowed to access the network, the administrator can close the port. This section introduces the general configuration of ports, mainly including:

- Opening and closing of port
- Rate configuration of the port
- Displays information about the port

3.1.1 Opening and closing of port

The port of the switch is open by default. If the administrator wants the user under the port to be unable to access the network, he can close the port.

The following command turns on the management state of the port in interface configuration mode:

no shutdown

For example, open the administrative status of port ge1/1:

Switch(config-ge1/1)#no shutdown

The following command turns off the administrative state of the port in interface configuration mode:
Shutdown

For example, close the administrative state of port ge1/1:

Switch(config-ge1/1)#shut

3.1.2 Rate configuration of the port

The default rate configuration for all ports is autonegotiate.
The following command configures the port's rate in interface configuration mode:
speed
{autonegotiate |full-1000 |full-100 |full-10 |half-100 |half-10 }
autonegotiate---Self-adaptive
full-1000-------Full-duplex gigabit
full-100--------Full-duplex 100m
full-10 --------Full duplex 10 megabyte
half-100--------Half-duplex 100m
half-10---------Half-duplex 10 megabytes

For example, the rate of port 1/1 is configured as full-duplex 100M:
Switch(config-ge1/1)# speed full-10

3.1.3 Displays information about the port

The following command displays information for one or more ports in normal or privileged mode:
show interface [if-name]
For example, show the information for port ge1/1: **Switch# show interface ge1/1**
For example, display information for all ports: **Switch# show interface**

3.2 Configure Port Mirroring

Port mirroring is a very useful feature for monitoring the traffic of packets received and sent by one or more ports. It can use the mirroring port to monitor the packets received and sent by one or more ports. The switch supports the port mirroring function, and the mirroring port can listen to the incoming data and outgoing data of other ports. A mirror port can listen on multiple ports at the same time. This section focuses on the configuration of MIRROR, including the following:

- Configure the listening and listened ports of MIRROR
- Display MIRROR configuration

3.2.1 Configure the listening and listened ports of MIRROR

When configuring the monitoring port, the administrator needs to enter the interface configuration mode to set the monitored port. For example, to set the port ge1/1 to monitor the port ge1/2, the administrator needs to enter the port ge1/1 and type the command:

Switch(config-ge1/1)# mirror interface ge1/2 direction both

At this point, port ge1/1 is set as the listening port and ge1/2 is set as the listened port.
The command to set the listening port is as follows:
Switch(config-ge1/1)#mirror interface <if-name> direction {both | receive | transmit}
In this case, the port ge1/1 is set as the monitoring port, and < if-name > is set as the monitored port. At the same time, the following { both | receive | transmit } indicates the monitoring direction: receive means to monitor the received packets; transmit means to monitor the transmitted packets; Boss listens to all packets sent and received. For example：

Switch(config-ge1/1)#mirror interface ge1/2 direction both
Indicates that port ge1/1 is set to listen to packets sent and received by port ge1/2.
If you want to set up multiple listening ports, you need to execute multiple commands.

In the interface configuration mode, the administrator can cancel the monitored port with the following command:

Switch(config-ge1/1)#no mirror interface <if-name>

At this point, < if-name > is the port that is no longer being listened to. For example：

Switch(config-ge1/1)# no mirror interface ge1/2
Indicates that port ge1/1 is set to no longer listen to packets on port ge1/2.
When all listened ports are cancelled, the listening ports are cleared.

3.2.2 Display MIRROR configuration

An administrator can view the MIRROR configuration that has been set by using the following command in normal mode or privileged mode:

Switch# show mirror

The following points should be noted:

- A port cannot be set as both a listening port and a listening port.
- There can be only one listening port, but there can be more than one listened port. There can be only one listening port, but there can be more than one listened port.

3.3 Configure STORM-CONTROL

In real life, a NIC card sends high-speed unicast, multicast and broadcast packets, which can cause network failures. In this case, the suppression function on the switch is particularly important. It can prevent data packets from flooding into the network and causing network congestion. All ports of the switch support the suppression function of broadcast packets, multicast packets and DLF packets.

This section describes the configuration of STORM-CONTROL in detail, mainly including the following contents:

- Default configuration
- Broadcast Suppression Configuration
- Multicast suppression configuration
- DLF Suppression Configuration
- Display the STORM-CONTROL configuration

3.3.1 Default configuration

The switch supports setting broadcast, multicast, and dlf switches for each port, and the three settings share the same rate limit. Broadcast packet throttling is on for the default port at a rate of 64K to prevent a broadcast storm from forming on the network. DLF packets and multicast packets are not suppressed by default

3.3.2 Broadcast Suppression Configuration

The following command configures broadcast suppression for this port in interface configuration mode:
storm-control broadcast
The following command unconfigures broadcast suppression for this port in interface configuration mode:

no storm-control broadcast

3.3.3 Multicast suppression configuration

The following command configures multicast suppression for this port in interface configuration mode:
storm-control multicast
The following command unconfigures multicast throttling for this port in interface configuration mode:
no storm-control multicast

3.3.4 DLF Suppression Configuration

The following command configures DLF suppression for this port in interface configuration mode:
storm-control dlf
The following command unconfigures DLF throttling for this port in interface configuration mode:
no storm-control dlf

3.3.5 Inhibit rate configuration

The following command configures the throttle rate for this port in interface configuration mode:

storm-control ratelimit <1-1024000>

3.3.6 Display the STORM-CONTROL configuration

The following command displays the STORM-CONTROL configuration in normal or privileged mode:

show storm-control

3.4 Configure STORM-CONSTRAIN

The port traffic threshold control function is used to control the packet storm on the Ethernet. The port that enables this function will detect the unicast message traffic, multicast message traffic and broadcast message traffic arriving at the port periodically. If the traffic of a certain type of message exceeds the preset upper threshold, the user can decide whether to block or close the port and whether to record Log information through configuration.

When the traffic of a certain type of message exceeds the preset upper limit threshold of this type of message, the system provides two processing methods:

(1) **Block mode:** If the traffic of a certain type of message in unicast, multicast or broadcast on the port is greater than the upper threshold, the port will stop forwarding the message, and the port is in the blocking state, but the port still counts the traffic of this type of message. When the traffic of this type of message is less than the preset lower threshold, the port will resume forwarding the message.

(2) **Shutdown mode**: If the traffic of a certain type of message in unicast, multicast or broadcast on the port is greater than the upper threshold, the port will be shut down and the system will stop forwarding all messages. The port state can be restored by executing the no shutdown command or by unconfiguring the port traffic threshold.

Note: For a certain type of packet traffic, it can be suppressed by this function or the storm suppression function of the Ethernet port, but these two functions cannot be configured at the same time, otherwise the suppression effect is uncertain. For example, the unicast packet flow threshold control function and the unicast storm suppression function of the port cannot be configured at the same time.

The CLI configuration commands are as follows:

Command	Description	CLI Mode
storm-constrain (broadcast|multicast|unicast) min-rate <1-1488100> max-rate <1-1488100>	Storm control for broadcast, multicast or unknown unicast messages under the interface	Interface Configuration Mode
no storm-constrain (broadcast|multicast|unicast|all)	Cancel storm control	Interface Configuration Mode
storm-constrain action (block|shutdown)	Configure the action of storm control. By default, no storm control is performed on the message	Interface Configuration Mode
no storm-constrain action	Cancels the action of the configured storm control	Interface Configuration Mode
storm-constrain enable (trap)	Turn on the switch for logging during storm control	Interface Configuration Mode
no storm-constrain enable (log)	Switch for logging when storm control is turned off	Interface Configuration Mode
storm-constrain interval <6-180>	Configure the detection interval of storm control. By default, the	Interface Configuration Mode

	detection interval of storm control is 5 second	
no storm-constrain interval	Restore the storm control detection interval to the default values	Interface Configuration Mode
no storm-constrain	Remove the storm control feature from the interface	Interface Configuration Mode
show storm-constrain	View storm control information for all interfaces	Privileged Mode
show storm-constrain interface IFNAME	View the storm control information for an interface	Privileged Mode

Configuration description:

View the storm control information description table of the interface

Item	Description
interface	Interface Name
type	Message type (1) broadcast-broadcast message; (2) multicast-multicast message; (3) unicast-unicast message
rate	Min-low threshold; Max-high threshold
action	Actions of storm control, including (1) block-blocking message; (2) shutdown-shutting down the interface
punish-status	Message status of the current interface, including (1) block-when the rate is greater than max-rate and the storm control action is blocking message, the status is blocking message; (2) Normal-normal forwarding; (3) shutdown-when the rate is greater than max-rate and the storm control action is closing the interface, the status is closing the interface
log	Log switch status, on/off
interval	The detection time interval of storm control, the unit is second, and the default value is 5 second
last-punish-time	Time of last storm control penalty

(2) The storm message can be controlled to prevent flooding by executing the storm-constrain action command to configure the action of storm control and executing the storm-constrain command to configure the high and low thresholds of storm control. During the storm control detection interval, when the average rate of receiving broadcast, multicast or unicast messages on the interface is greater than the specified high threshold, the storm control will block the messages or close the interface according to the configured actions. When the storm control action is a blocking message, if the flow is lower than the minimum threshold, the interface will recover to the normal forwarding state; when the storm control action is to close the interface, the interface cannot recover automatically and needs to manually execute the no shutdown command to recover, which can be recovered by canceling the port storm control shutdown action configuration.

(3) When the port traffic exceeds the upper threshold or falls from the upper threshold to the lower threshold, log/trap information is output.

3.5 Configure flow-control

FLOW-CONTROL is used to prevent packet loss if a port is blocked. In the half-duplex mode, the flow control is realized by the Backpressure technology, so that the information source reduces the transmission rate. In full-duplex mode, the flow control follows the IEEE 802.3 X standard, and the blocking port sends a "Pause" packet to the information source to stop it from sending.
This section describes the configuration of FLOW-CONTROL in detail, mainly including the following contents:

- Default configuration
- Set Port Flow Control
- Close port flow control
- Display flow control information

3.5.1 Default configuration

The switch supports setting flow control for sending and receiving on each port. The default port does not have flow control turned on.

3.5.2 Set Port Flow Control

The following command configures port flow control on in interface configuration mode:
flowcontrol

3.5.3 Close port flow control

The following command turns off port transmit and receive side flow control in interface configuration mode:

no flowcontrol

3.5.4 Display flow control information

The following command displays flow control information for all ports in normal or privileged mode:
show flowcontrol

The following command displays flow control information for a port in normal or privileged mode:
show flowcontrol interface <if-name>
Where, < if-name > is the name of the port to query the flow control information

3.6 Configure port bandwidth

Port bandwidth control is used to control the rate at which a port sends and receives.
This section describes the configuration of port bandwidth in detail, mainly including the following contents:

- Default configuration
- Set port send or receive bandwidth control
- Remove port send or receive bandwidth control
- Show Bandwidth Control for Port Configuration

3.6.1 Default configuration

The switch supports setting the transmit and receive bandwidth for each port separately. The default port does not have bandwidth control.

3.6.2 Set port send or receive bandwidth control

The following command sets the port transmit or receive bandwidth control in interface configuration mode:

portrate {egress | ingress} <rate>

The egress indicates bandwidth control of the transmitted packets.

Ingress indicates bandwidth control of received packets.

< rate > indicates the value of the bandwidth to be set, in the range of 1-1024000, in kbits.

3.6.3 Remove port send or receive bandwidth control

The following command removes bandwidth control from a port in interface configuration mode:

no portrate {egress | ingress}

The egress indicates that the bandwidth control of the transmitted packet is cancelled.

The ingress indicates that the bandwidth control of the received packet is cancelled.

3.6.4 Show Bandwidth Control for Port Configuration

The following command views the bandwidth control of the port configuration in normal or privileged mode:

show portrate interface <if-name>

Where < if-name > is the name of the port you want to query for bandwidth control information.

3.7 Configure TRUNK

TRUNK aggregates multiple ports into one logical port, which can be used to increase bandwidth, provide redundant backup connections, and load balance. When the trunk group is used as the output logical port, the switch will select a port from the port group to send the packet according to the aggregation policy set by the user. The configuration of the port and aggregation policy of the trunk group is done by software, but the forwarding of the data stream is done by hardware.

All ports in a trunk group must be configured at the same speed and in full-duplex mode. The switch can support up to 32 groups of TRUNKs, with up to 8 TRUNK members per group. It is important to note that each port can belong to only one TRUNK group.

The LACP protocol is a protocol based on the IEEE 802.3 ad standard. The LACP protocol exchanges information with the peer through the LACPDU (Link Aggregation Control Protocol Data Unit, Link Aggregation Control Protocol Data Unit).

The interface in the aggregation group enables the LACP protocol, and the interface will inform the opposite end of its system LACP protocol priority, system MAC, port LACP protocol priority, port number and operation Key by sending LACPDU. After receiving the LACPDU, the opposite end compares the information in the LACPDU with the information received by other interfaces to select the interface that can be in the Selected state, so that both sides can reach an agreement on the interface in the Selected state.

The action Key is a combination of configurations that aggregation control automatically generates at link aggregation time based on certain configurations of member ports, including port rate, duplex mode, up/down status, VLAN allowed on the port, port default VLAN ID, link type of the port (i.e. Trunk, Hy brid, Access type), and so on. In an aggregation group, member ports in the Selected state have the same action Key.

This section describes the configuration of TRUNK in detail, mainly including the following contents:

- LACP protocol configuration
- Configuration of the trunk group
- TRUNK Member Port Configuration
- TRUNK Load Balancing Policy Configuration
- Display of TRUNK

3.7.1 LACP protocol configuration

Command	Description	CLI Mode
lacp system-priority <1-65535>	Set lacp system priority	Global Configuration Mode
no lacp system-priority	Restore System Priority Default 32 768	Global Configuration Mode
lacp max-active-link-number <1-8>	Set lacp activation aggregation port cap	Global Configuration Mode
no lacp max-active-link-number	Restore lacp activation aggregation port default upper limit 8	Global Configuration Mode
lacp port-priority <1-65535>	Set the lacp port priority	Interface Configuration Mode
no lacp port-priority	Restore Port Priority Default 32768	Interface Configuration Mode
lacp timeout (short|long)	Set lacp port timeout, default long ti meout	Interface Configuration Mode
show lacp summary	A simple case showing all lacp aggr egates	Privileged Mode
show lacp detail	Displays the condition of all lac p aggregates	Privileged Mode
show lacp <1-8>	Display the details of the lacp aggre gation port	Privileged Mode
show lacp port IFNAME	Displays the details of the lacp port	Privileged Mode
show lacp system-id	Display lacp system condition	Privileged Mode
show lacp counter <1-8>	Display statistics of lacp aggregatio n port	Privileged Mode
show lacp counter	Display statistics of all lacp aggrega tion ports	Privileged Mode
clear lacp <1-8> counters	Clear statistics of lacp aggregation port	Privileged Mode
clear lacp counters	Clear the statistics of all lacp aggre gation ports	Privileged Mode

3.7.2 Configuration of the trunk group

The following command creates a manual TRUNKgroup in global configuration mode:

trunk <trunk-id>

Create a TRUNK group. The < trunk-id > value range is 1-32, indicating the ID number of the TRUNK group to be created. Up to 8 groups of TRUNKs can be configured. After successful creation, the interface name of the TRUNK is trunk + ID number. For example, the interface name of a TRUnk group with a group ID of 1 is trunk1. You can use the "interface trunk + ID number" command in the configuration mode to enter the interface configuration mode, and then operate the TRUNK group. For example, use the command interface trunk1 to enter the interface mode of TRUNK 1 and configure TRUNK 1.

The following command creates a static LACP trunk group in global configuration mode:

trunk <1-32> dynamic

The following command removes a trunk group in global configuration mode:

no trunk <trunk-id>

When deleting a trunk group, you must ensure that the trunk group has no member ports.

3.7.3 TRUNK Member Port Configuration

The following command adds a new TRUNK-group member port in interface configuration mode:

trunk interface IFNAME (passive|)

< if-name > is the name of the port to be added to the TRUNKgroup, which must be a layer 2 interface. Each group of TRUNKs can add up to 8 Layer 2 interfaces. If the trunk group is a static LACP trunk group, the added interface defaults to the active state and can also be configured to the passive state.

The following command removes all member ports of the trunk group in interface configuration mode:

no trunk interface

The following command removes the specified TRUNK-group member port from interface configuration mode:

no trunk interface <if-name>

You can use this command multiple times to delete multiple ports that are members of the TRUNKgroup.

3.7.4 TRUNK Load Balancing Policy Configuration

The following command sets the load balancing policy for TRUNK in interface configuration mode:

trunk load-balance {dst-mac | dst-ip | src-dst-mac | src-dst-ip | src-mac | src-ip}

dst-mac--------Balancing strategy based on destination MAC

dst-ip----------Balancing strategy based on destination IP

src-dst-mac---Balancing strategy based on source MAC and destination MAC

src-dst-ip------Balancing strategy based on source IP and destination IP

src-mac--------Balance strategy based on source MAC

src-ip----------Source IP-based balancing strategy

The following command sets the default TRUNK load balancing policy in interface configuration mode:

no trunk load-balance

The default port load balancing policy is src-dst-mac (source and destination MAC based balancing policy).

3.7.5 Display of TRUNK

The following command views all TRUNKs in normal or privileged mode:

show trunk

The following command views the specified TRUNKs configuration in normal or privileged mode:

show trunk <trunk-id>

Where < trunk-id > is the ID number of the trunk group to be queried.

3.8 Configure Jumbo Frame

3.8.1 Introduction to Jumbo Frame

To enable a port to receive jumbo frames, the port can be set to support a specific jumbo frame length.

3.8.2 Jumbo Frame Configuration

Configure the port to support the very large frame length. In the config mode, enter the port configuration mode, such as interface ge1/1, and execute the following command:

Switch(config-ge1/1)#jumbo frame 2000

Displays the excessive frame length supported by the port

Switch#show jumbo frame ge1/1

Port	Jumbo frame(bytes)
ge1/1	2000

3.9 Configuring Redundant Port

In some special cases, such as the need to focus on ensuring the stability of some servers linked to the network, the redundant port of the switch can provide two ports linked to this server, and ensure that at a time the server has only one LINK UP port linked to the network, when a port occurs LINK DOWN, The system now enables another port.

When a port is in the LINK UP state in a redundant port group, we call it the Active state; otherwise, if a port is in the LINK DOWN state in a redundant port group, we call it the Disable state.

This section focuses on the configuration of redundant ports, including the following:

- Configuration of redundant port
- Display of Redundant Port

3.9.1 Configuration of redundant port

The switch can be configured with 8 groups of redundant ports. One group of redundant ports can only be configured with 2 ports. One port can only be configured in one redundant port group.

A redundant port group can be configured with one primary-port and one secondary-port. When configuring to enable redundant port groups:

(1) When both ports are in the LINK UP state, the primary-port is set to the Acitve state and the secondary-port is set to the Disable state;

(2) if only one port is in the LINK UP state, the current LINK UP port is set to be in the Active state, and the other port is in the Disable state;

(3) Otherwise both ports are in the Disable state.

If a LINK DOWN event occurs on a port that is in the Active state, the other port will attempt to be in the Active state.

Another configuration parameter is force-switch, which is used when the secondary-port is in the Active state and the primary-port is in the Disable state. If a LINK UP event occurs on the primary-port, Decide whether to switch back to the state where primary-port is Active and secondary-port is Disable. If force-switch is configured to enable, the switch is forced, otherwise the port state of the original redundant port group is retained.

Command	Description	CLI Mode
redundant-port <1-8> primary-port IFNAME secondary-port IFNAME [force-switch]	Configure a set of redundant ports, < 1-8 > is the group number Primary-port IFNAME is that interface name of the primary port, A secondary-port IFNAME is that interface name of the secondary port, Force-switch Whether the force toggle switch is enabled.	Global Configuration Mode
redundant-port <1-8> force-switch	Enable the force toggle switch for the redundant port.	Global Configuration Mode
no redundant-port <1-8>	Deletes a redundant port group.	Global Configuration Mode
no redundant-port <1-8> force-switch	Turn off the forced toggle switch for the redundant port.	Global Configuration Mode

3.9.2 Display of Redundant Port

Command to display redundant port

Command	Description	CLI Mode
show redundant-port	Displays the configuration of all redundant port groups in the system	Privileged Mode

3.10 UDLD Configuration

UDLD (device link detection protocol): It is a layer 2 protocol used to monitor the physical configuration of the Ethernet link connected by optical fibre or twisted-pair. When there is a unidirectional link (transmission can only be in one direction, for example, I can send data to you, and you can also receive it. But I can't receive the data you sent me), UDLD can detect this situation, shut down the corresponding interface and send a warning message. Unidirectional links can cause many problems, especially spanning trees, which can cause loopbacks. Note: UDLD requires support from both devices on the link for proper operation.

UDLD supports two modes of operation; normal mode (default) and aggressive mode.

Normal mode: In this mode, UDLD can detect unidirectional links and mark the port as undetermined to generate system logs, In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended period of time.

Aggressive mode: In this mode, UDLD can detect unidirectional links. It will try to rebuild the link and send UDLD messages for 8 seconds. If there is no UDLD echo reply during this period, the port will be placed in the errdisable state.

Command	Description	CLI Mode
UDLD enable	UDLD function enabled globally	Global Configuration Mode
UDLD message time <time>	UDLD message sending interval	Global Configuration Mode
UDLD port	Port enable UDLD	Interface Configuration Mode
UDLD aggressive	Enable port aggressive mode, default to normal mode	Interface Configuration Mode
show UDLD <ifname>	View Port UDLD Information	Privileged Mode

3.11 Configure LLDP

At present, there are more and more kinds of network devices and their configurations are complex. In order to make the devices of different manufacturers find each other and exchange their system and configuration information in the network, a standard information exchange platform is needed.

LLDP (Link Layer Discovery Protocol) is produced in this background, which provides a standard way of link layer discovery. Information such as main capability, management address, device identifier, and interface identifier of the local device may be organized into different TLVs (Type/Length/Value), and encapsulated in an LLDPDU (Link Layer Discovery Protocol Data Unit, Link Layer Discovery Protocol Data Unit) to its neighbours that are directly connected to it. After receiving this information, the neighbours save it in the form of standard MIB (Management Information Base) for the network management system to query and judge the communication status of the link.

This section focuses on the configuration of LLDP, mainly including the following:

- Configuration of LLDP
- Display of LLDP

3.11.1 Configuration of LLDP

There are four modes of operation for the LLDP port:

1. **TxRx:** send and receive LLDP messages.
2. **Tx: only** send but not receive LLDP messages.
3. **Rx: Only** receive LLDP message but not send it.
4. **Disable:** Neither send nor receive LLDP messages.

When the LLDP working mode of the port changes, the port will initialize the protocol state machine. In order to avoid the frequent change of the working mode of the port, which causes the port to continuously perform the initialization operation, the delay time of the port initialization can be configured, and when the working mode of the port is changed, the initialization operation can be performed after a period of time.

Command	Description	CLI Mode
lldp global enable	LLDP global enable command.	Global Configuration Mode
lldp hold-multiplier <num>	Lldp TTL multiples.	Global Configuration Mode
lldp timer [<reinit-delay><time>][< tx-delay><time>][< tx-interval ><time>]	Configure various timers for LLDP.	Global Configuration Mode
lldp enable	Enable interface LLDP	Interface Configuration Mode
lldp admin-status{ disable| rx|tx|rxtx}	Configure the operating mode of the LLDP port.	Interface Configuration Mode
lldp check-change-interval <time>	Configure the time interval for refreshing interface information.	Interface Configuration Mode
lldp management-address <A.B.C.D>	Configure interface LLDP management addr	Interface Configuration Mode
lldp tlv-enable{ dot1-tlv| dot3-tlv|med-tlv }	Configure Interface LLDP Extended Capability Set Switch	Interface Configuration Mode

3.11.2 Display of LLDP

Commands for LLDP

Command	Description	CLI Mode
show lldp configuration [ifname]	Display lldp configuration information	Privileged Mode
show lldp local-information [ifname]	Display lldp local information	Privileged Mode
show lldp neighbour - information [ifname]	Display lldp neighbour information	Privileged Mode
show lldp statistics [ifname]	Display lldp message statistics	Privileged Mode
show lldp status [ifname]	Display lldp status information	Privileged Mode

4. Configuring Port-Based Security

This chapter introduces the port-based MAC security configuration, mainly including the following contents:

Introduction

- MAC Binding Configuration
- MAC filtering configuration
- Port Learning Limit Configuration
- Protection port configuration

4.1 Introduction

Port-based MAC security can provide four functions: MAC binding, MAC filtering, port learning control and port protection to improve the security performance of Layer 2 forwarding.

MAC binding can bind MAC and port together, and limit a specified MAC address to access the network only at a specified port; meanwhile, the port can only allow these bound MAC addresses to access the network; a port can bind multiple MAC addresses at the same time. MAC binding can be applied to a given port at the same time as the 802.1 X. This feature is useful for devices that do not have 802.1 X capabilities or are not comfortable using 802.1 X, such as printers, file servers, and so on.

MAC filtering can prevent some specified MAC addresses from accessing the network. The main purpose is to prevent some illegal devices from accessing the network. When a MAC address is configured for MAC filtering, the MAC address cannot access the network on any port of the switch, nor can it receive packets destined for the specified MAC address. As with MAC binding, a port can be configured with multiple MAC addresses for MAC filtering at the same time. In the application, if some virus software attacks the network through forged MAC addresses, in addition to ACL, MAC filtering can also be used to access and control the attack of forged packets.

Port learning control can control the number of MAC addresses that a port can learn dynamically. If a port specifies the number of MAC addresses it can dynamically learn, when the number of MAC addresses learned by the port is equal to the number configured for the port, new MAC addresses will not be learned, and packets for these new MAC addresses will be discarded.

It should be noted that the MAC address referred to here is actually MAC + VID, and the description later in this chapter will not be repeated. In addition, the MAC binding function and the 802.1 X can be configured on one port at the same time; the MAC filtering and the port learning limit can be configured on one port at the same time; the MAC binding function, the 802.1 X, and the MAC filtering and port learning limit cannot be configured on the same port simultaneously.

4.2 MAC Binding Configuration

MAC binding configuration supports manual MAC address binding and automatic MAC address binding. Manually binding MAC addresses means that the user enters MAC addresses and ports one by one through commands to bind. Automatically binding the MAC address is to read out the existing entry of the port in the layer 2 hardware forwarding table and directly bind the MAC address. The command to read the Layer 2 hardware table is a Show bridge FDB.

Configuration Commands

Command	Description	CLI Mode
switchport-security mac-bind HHHH.HHHH.HHHH vlan <1-4094> qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7}	Manually bind a MAC address to an interface and configure the prio rity queue of the entry.	Interface Configuration Mode
switchport-security mac-bind auto-conversion number <1-8191> qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7}	Automatically translates a specifie d number of MAC addresses of an interface into a MAC binding con figuration and configures a priorit y queue for the entry.	Interface Configuration Mode
switchport-security mac-bind auto-conversion vlan <1-4094> qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7}	Automatically translates the MAC address of the specified VLAN of an interface into a MAC binding configuration and configures the p riority queue for that entry.	Interface Configuration Mode
show port-security mac-bind [IFNAME]	Display MAC binding configurati on	Privileged Mode

Notice:

- An invalid or failed MAC address binding can occur for the following reasons:
- The port is already configured with 802.1x
- The port has been configured with MAC filtering or port learning restrictions;
- The MAC address has been bound to another port, or MAC filtering has been configured;
- The L2 table of the switch is full.

4.3 MAC filtering configuration

MAC filtering configuration supports manual MAC address binding and automatic MAC address binding. Manually configuring MAC filtering means that the user inputs the MAC to be filtered and the port to be bound one by one through the command. Automatically configuring MAC filtering is to read out the existing entries of the port in the layer 2 hardware forwarding table and directly configure the MAC filtering. The command to read the Layer 2 hardware table is a Show bridge FDB.

Configuration Command

Command	Description	CLI Mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Manually configure MAC filtering for an interface	Interface Configurati on Mode
switch port-security mac- filter auto-conversion number <1-8191>	Automatically converts a specified number of MAC addresses for an interface to a MAC filtering configuration	Interface Configurati on Mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Automatically translates the MAC address of a specified VLAN on an interface to a MAC filtering configuration	Interface Configurati on Mode
show port-security mac-filter [IFNAME]	Display MAC binding configuration	Privileged Mode

Notice：

- MAC filtering configuration may be invalid or fail for the following reasons:
- The port has been configured with MAC binding or 802.1x protocol functionality enabled;
- The MAC address is already bound to another port, or MAC binding is configured;
- The L2 table of the switch is full.

4.4 Port Learning Limit Configuration

The switch can configure the maximum number of dynamically learned addresses per port. If a port is configured to dynamically learn the number of MAC addresses, the port can only learn the corresponding number of MAC addresses. When the number of MAC addresses exceeds this number, the port cannot learn and forward.

Without a configured learning limit, a port can learn up to 8191 MAC addresses.

Configuration Command

Command	Description	CLI Mode
switchport port-security learn-limit <0-8191>	Configure the number of MAC addresses th at an interface can learn.	Interface Configuration Mode
no switchport port-security learn-limit	Deletes the number of MAC addresses an int erface can learn.	Interface Configuration Mode
show port-security learn-lmit [IFNAME]	Show Port Learning Configuration	Privileged Mode

- Configuration examples
- Configure port ge1/5 to learn only 7 MAC addr
- Switch#configure terminal
- Switch(config)interface ge1/5
- Switch(config-ge1/5)switchport port-security learn-limit 7

Notice：

Port configuration may be invalid or fail for the following reasons:

The port has MAC binding configured or 802.1x protocol features enabled.

4.5 Protection port configuration

4.5.1 Introduction to Protection Port

In order to achieve layer 2 isolation between packets, ports can be divided into different VLANs, but VLAN resources will be wasted. The ports are configured as protection ports, so that the isolation of the ports in the same VLAN can be realized, and a safer and more flexible networking scheme is provided for a user.

Each port can be configured as a protected port. Protected ports cannot communicate with each other and can only communicate with unprotected ports. There are two application modes:

1.Only one port is not configured as a protection port, and all other ports are isolated;

2.Prevent some insecure ports from sniffing the data of other ports (connected to the server),and set these ports as protected ports.

4.5.2 Protection port configuration

Configure the port as a protection port. In the config mode, enter the port configuration mode, such as interface ge1/1, and execute the following command:

Switch(config-ge1/1)#switchport port-security protect

Displays the ports that are configured as protection port

Switch#show port-security protect

Port Port protected

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

ge1/1 ON

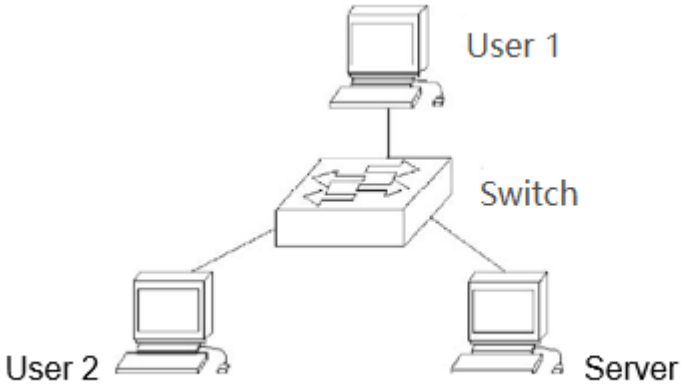
Example of typical configuration of protection port

Networking requirements

User 1 and user 2 servers are connected to switch ports ge1/1, ge1/2, ge1/3, respectively

User 1 and user 2 belong to the same VLAN. User 1 and user 2 cannot communicate with each other, but can communicate with the server

Network Diagram



Configuration steps
Switch>enable
Switch#config terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport port-security protect
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport port-security protect
Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show port-security protect
Port Port protected
----- --------------
ge1/1 ON
ge1/2 ON

5. Configure port IP and MAC bindings

This chapter introduces port IP and MAC binding configuration, mainly including the following content

1. Introduction

- IP and MAC binding configuration
- Configuration examples
- Configuration Troubleshooting

5.1 Introduction

Configuring IP and MAC binding on layer 2 switch ports is a static defense against ARP attacks. ARP attackers attack users by sending ARP packets with false MAC addresses, causing the user's local ARP cache table to be overwritten by the attacker's MAC address, causing normal data to flow to the attacker. ARP attack packets can be effectively filtered by statically binding the user IP address and MAC address in the switch port configuration command.

In addition to the function of preventing ARP spoofing, the IP MAC binding function can also guarantee the one-to-one mapping relationship between IP and MAC, that is to say, one IP can only correspond to one MAC, and one MAC can only correspond to one IP. If the access device modifies this mapping relationship, it will not be able to communicate in this network. The 802.1 X anti-ARP spoofing function and the DHCP snooping protocol are dynamic implementations of this function.

The four functions of IP MAC binding, ACL, 802.1 X anti-ARP spoofing and DHCP SNOOPING all use the same system resource CFP. Pay attention to whether the CFP resource is exhausted during configuration. At the time of design, we have formulated the compatibility relationship between them. See the following table:

	IP MAC Binding	**ACL**	**802.1x**	**DHCP SNOOPING**
IP MAC Binding	Compatible	Incompatibility	Compatible	Compatible
ACL	Incompatibility	Compatible	Incompatibility	Incompatibility
802.1x	Compatible	Incompatibility	Compatible	Incompatibility
DHCP SNOOPING	Compatible	Incompatibility	Incompatibility	Compatible

CFP is a limited hardware resource, and each port can only be configured with 16 IP MAC binding entries on average. Therefore, in a network with many access hosts, if only a few ports or a few IP and MAC addresses need to be controlled, the static IP MAC binding function can be used. And that data forward failure caused by the exhaustion of the CFP function is avoid.

In addition, whether to use the 802.1 X or the DHCP SNOOPING protocol depends on the current situation. If the static IP address configuration is used and the 802.1 X protocol is used to access the network, the 801.1 X anti-ARP spoofing must be used to be effective. If the dynamic IP address acquisition is used, Use the DHCP SNOOPING protocol.

5.2 IP and MAC binding configuration

IP and MAC binding is configured in interface mode

Configure port IP and MAC bindings

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#ip mac-bind A.B.C.D MAC

Remove Port IP and MAC Binding

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no ip mac-bind A.B.C.D MAC

Display Configuration

Display binding table entries for all ports

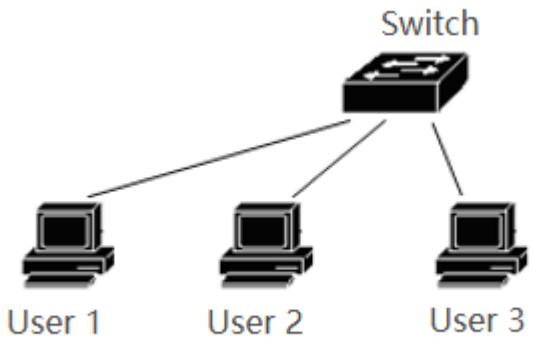
show ip mac-bind

Displays the binding table entries for an interface

show ip mac-bind IFNAME

5.3 Configuration examples

There are user 1, user 2 and user 3 in the network, and the IP and MAC of the user are bound on the port to defend against ARP attacks.



Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#ip mac-bind 192.168.1.100 0011.5b34.42ad

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#ip mac-bind 192.168.1.101 0011.6452.135d

Switch(config-ge1/2)#interface ge1/3

Switch(config-ge1/3)#ip mac-bind 192.168.1.102 0011.804d.a246
Switch(config-ge1/3)#end
Switch#show ip mac-bind
[ge1/1] sum: 1
MAC IP 0011.5b34.42ad 192.168.1.100
[ge1/2] sum: 1
MAC IP 0011.6452.135d 192.168.1.101
[ge1/3] sum: 1
MAC IP 0011.804d.a246 192.168.1.102
Switch#show ip mac-bind ge1/1
[ge1/1] sum: 1
MAC IP 0011.5b34.42ad 192.168.1.100
Switch#show running-config
!
spanning-tree mst configuration
!
Interface vlan1
ip address 10.10.10.1/24
!
interface ge1/1
ip mac-bind 192.168.1.100 0011.5b34.42ad
!
interface ge1/2
ip mac-bind 192.168.1.101 0011.6452.135d
!
interface ge1/3
ip mac-bind 192.168.1.102 0011.804d.a246
!
line vty
!
End

5.4 Configuration Troubleshooting

If the IP MAC binding configuration fails, it may be caused by the following reasons:

① System CFP resources are exhausted.

② The current interface is configured with ACL filtering.

③ The configured interface is a layer 3 interface or a TRUNK interface.

6. Port Loop Detection

This chapter mainly includes the following contents:

- Introduction
- Protocol principle
- Configuration Introduction

6.1 Introduction

When a loop appears under a certain port of the switch, it will cause a broadcast storm under this port, and the source MAC address of all broadcast packets will be learned to this looped port, which will cause the device forwarding to fail.

6.2 Protocol principle

The Ethernet loop detection protocol (Ethernet Loopback Detection, hereinafter referred to as ELD) can detect the loop through the exchange of data packets and block the port on which the loop occurs. The ELD protocol is a port-based protocol that can only detect loops that occur on this port.

6.2.1 Detection Process

When a port enables the ELD protocol, a timer period will be enabled on the port, and a loop detection packet will be sent when the timer expires. If the loop detection packet sent by the port is received within a timer period, it is considered that a loop exists on the port, and the operation of blocking the loop on the port will be executed, and the FDB table of the port will be cleared.

If a port is a port member of multiple VLANs, the port automatically sends loop detection packets to all VLANs. This means that the port automatically detects the presence of loops in all VLANs to which it belongs.

6.2.2 Recovery Mode

As mentioned above, when a port loop occurs, the port will be blocked. The ELD protocol has two recovery modes that the user can configure: automatic recovery and manual recovery.

Automatic recovery means that when a port is blocked, the ELD protocol enables a recovery timer. When the timer expires, it will perform a reverse operation of blocking the loop, and enable the loop detection timer again on this port.

Manual recovery means that after the port is blocked, the protocol no longer enables the timer to recover the port, and the user has to enter the command to perform the reverse operation of blocking the loop.

6.2.3 Protocol Security

The ELD protocol is vulnerable to attack in the network, that is, the user can send an ELD protocol packet to a port where the ELD protocol is enabled according to the packet format of the ELD protocol, causing the port to be blocked without a loop, resulting in a wrong decision.

The ELD protocol uses two strategies to prevent similar attacks and minimize errors.

First of all, the ELD protocol is a non-interactive protocol, that is to say, it does not depend on other devices, so the data packet itself can be simply encrypted. Our operation here is to send the ELD protocol packet with a key, and the user cannot disguise the protocol packet without the key.

The second decision is mainly to prevent the attacker from reflecting the protocol packet through the packet capture attack. The format of the data packet received by the switch in a certain period can be configured to prevent the attack, which requires the user to configure.

6.3 Configuration Introduction

The ELD protocol is implemented on a port basis, and there is no command to enable it uniformly.

6.3.1 Global Configuration

The global configuration is the uniform property of the configuration protocol.

Command	Description	Pattern
loop-detection detection-time <1-65535>	Configure the time period for loop detection. The time must be twice less than the recovery time period. The default value is 5 seconds.	Global Configuration Mode
loop-detection resume-time <10-65535>	Configures the time period for automatic recovery. The time for automatic recovery must be greater than 2 times the loop check time. This configuration will take effect if automatic recovery is enabled. The default recovery time is 600 seconds.	Global Configuration Mode
loop-detection protocol-safety	Enables protocol security checking, which is off by default.	Global Configuration Mode
loop-detection respond-packets	Configure the number of packets that must be received in a certain time. This configuration will take effect if protocol security checking is enabled. The default is 10.	Global Configuration Mode

Command describe Pattern

loop-detection detection-time <1-65535>

Configure the time period for loop detection. The time must be twice less than the recovery time period. The default value is 5 seconds. Global Configuration Mode

loop-detection resume-time <10-65535>

Configures the time period for automatic recovery. The time for automatic recovery must be greater than 2 times the loop check time. This configuration will take effect if automatic recovery is enabled. The default recovery time is 600 seconds.

Global Configuration Mode

loop-detection protocol-safety Enables protocol security checking, which is off by default.

Global Configuration Mode

loop-detection respond-packets

Configure the number of packets that must be received in a certain time. This configuration will take effect if protocol security checking is enabled. The default is 10. **Global Configuration Mode**

6.3.2 Interface configuration

The interface configuration is the configuration for each port.

The interface configuration is the configuration for each port.

Command	Description	Pattern
Loop-detection enable	Enable the ELD protocol on a port.	Interface Configuration Mode
Loop-detection resume	Resume manually and restart the loop check	Interface Configuration Mode
loop-detection resume-mode {automation | manual}	Configure the recovery mode and select manual recovery or automatic recovery. The default is automatic recovery.	Interface Configuration Mode
loopback-detection shutdown-mode {no-shutdown | shutdown}	The command configures whether the port shuts down when a loop occurs.	Interface Configuration Mode

6.3.2 Display Configuration

Show loop-detection [ifname]

Displays all configurations for a protocol and the configuration for an interface.

7. Configuring VLAN

VLAN is an important concept in the switch, which is widely used in practical applications. It is the basis of internal division of multiple networks. VLAN is short for Virtual Local Area Network, which is a network that logically organizes multiple devices together, regardless of their physical location. Each VLAN is a logical network that has all the features and attributes of a traditional physical network. Each VLAN is a broadcast domain. Broadcast packets can only be forwarded within a VLAN and cannot cross VLANs. Data traffic between VLANs must be forwarded through Layer 3.

This chapter mainly includes the following contents:

- Introduction to VLAN
- VLAN Configuration
- Example VLAN configuration

7.1 Introduction to VLAN

This section gives a detailed introduction to VLAN, mainly including the following contents:

- Benefits of VLAN
- VLAN ID
- VLAN Port Membership Type
- Default VLAN for the port
- VLAN mode of the port
- VLAN Trunk
- Forwarding of traffic within a VLAN
- Subnet of VLAN

7.1.1 Benefits of VLAN

VLANs greatly extend the size of the physical network. The traditional physical network can only have a very small scale, which can accommodate thousands of devices at most, while the physical network divided by VLAN can accommodate tens of thousands or even hundreds of thousands of devices. VLANs have the same functions and attributes as traditional physical networks.

Using VLANs has the following benefits:

- **VLANs can effectively control the traffic in the network.**

In a traditional network, all broadcast packets are delivered to all devices, whether they are needed or not, increasing the load on the network and devices. VLANs can organize devices in a logical network according to their needs. A VLAN is a broadcast domain. Broadcast packets are only transmitted within the VLAN and will not cross the VLAN. The division of VLANs can effectively control the traffic in the network.

- **VLANs can improve network security.**

A device in a VLAN can only perform Layer 2 communication with a device in the same VLAN. If it wants to communicate with another VLAN, it must be forwarded through Layer 3. If Layer 3 forwarding between VLANs is not established, communication between VLANs is not possible at all, which can play a role in isolation and ensure data security in each VLAN. For example, if the R & D department of a company does not want to share data with the marketing department, the R & D department can establish a VLAN, the marketing department can establish a VLAN, and the two VLANs do not establish a three-layer communication channel.

- VLANs facilitate the mobility of devices.

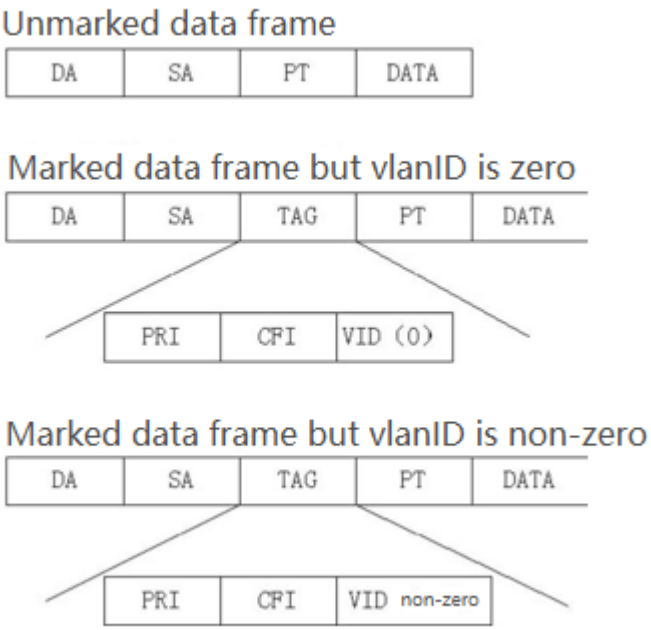
When a device in a conventional network moves from one location to another and belongs to a different network, the network configuration of the mobile device needs to be modified, which is very inconvenient for the user. A VLAN is a logical network, and devices that are not in the same physical location can be assigned to the same network. When a device moves, the device can also belong to the VLAN. In this way, the moving device does not need to modify any configuration.

7.1.2 VLAN ID

Each VLAN has an identification number called VLAN ID. VLAN IDs range from 0 to 4095, where 0 and 4095 are not used, and only 1 to 4094 are actually valid. The VLAN ID uniquely identifies a VLAN.

The switch supports 4094 VLANs. When creating a VLAN, select a VLAN ID ranging from 2 to 4094. The switch creates VLAN 1 by default, and VLAN 1 cannot be deleted.

There are three types of data frames transmitted within a VLAN in the network: untagged data frames, tagged data frames with a VID of 0, and tagged data frames with a VID other than 0. The following figure shows three different data frame formats.



Inside the switch, all data frames are tagged. If an untagged data frame enters the switch, the switch adds a tag to the frame, selecting a VLAN ID value to fill in the tagged VID. If a tagged data frame with a VID of 0 is entered into the switch, the switch selects a VLAN ID value to populate the tagged VID. If a data frame marked with a vid other than 0 is input to the switch, the frame is unchanged.

7.1.3 VLAN Port Membership Type

The switch supports port-based VLANs and 802.1 Q-based VLANs. A VLAN includes two types of port members: untagged and tagged. A VLAN can include both untagged and tagged port members.

A VLAN can have no port members or one or more port members. When a port belongs to a VLAN, it can be an untagged member or a tagged member of the VLAN.

A port can be a tagged or untagged member of one or more VLANs. If a port is a tagged member of two or more VLANs, it is called a VLAN trunk port. A port can be an untagged member of one or more VLANs and a tagged member of one or more other VLANs.

7.1.4 Default VLAN for the port

A port has one and only one default VLAN, which is used to determine the VLAN to which an untagged or tagged packet with a VID of 0 is input from the port. The default VLAN is also known as the port VID or PVID. By default, the default VLAN for the port is 1.

7.1.5 VLAN mode of the port

Ports have three VLAN modes: ACCESS mode, TRUNK mode, and HYBRID mode. The user must first specify the VLAN mode of the port when configuring the VLAN of the port.

A port in the ACCESS mode is an access port that directly faces the user. The port can only be an untagged member of one VLAN. The default VLAN is the VLAN specified by the user. When a port is an untagged member of only one VLAN, you can specify that the port's VLAN mode is ACCESS.

A port in TRUNK mode is a trunk port directly connected to a switch. The port can be a tagged member of one or more VLANs, but cannot be an untagged member of any VLAN. The port's default VLAN is 1 and cannot be changed.

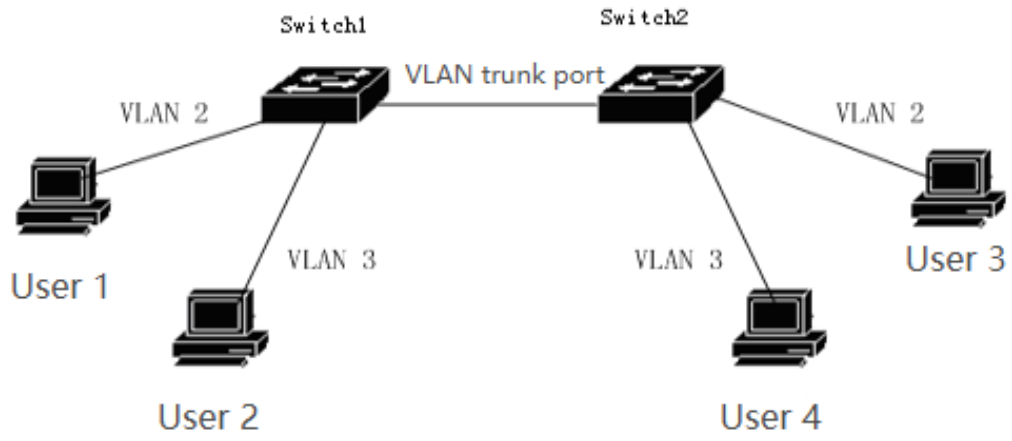
A port in HYBRID mode is a trunk port, directly connected to the switch, that can be a tagged member of one or more VLANs and/or an untagged member of one or more VLANs. The default VLAN for this port can be changed.

In practice, the user can select the VLAN mode of the port according to the specific situation.

7.1.6 VLAN Trunk

A port that is a tagged member of two or more VLANs is called a VLAN trunk port. Two switches can be connected by VLAN trunk ports, so that two or more common VLANs can be divided between the two switches.

The following figure is an example of a VLAN trunk. Two switches are connected by VLAN trunk ports, which are the trunk ports of VLAN 2 and VLAN 3. Each switch is divided into two VLANs, VLAN 2 and VLAN 3, and each VLAN has a user. Thus, User 1 can communicate with User 3, User 2 can communicate with User 4, and User 1 and User 3 cannot communicate with User 2 and User 4.



7.1.7 Forwarding of traffic within a VLAN

When a switch receives a packet from a port, it performs Layer 2 forwarding according to the following steps:

- Determine the VLAN to which the packet belongs.
- Determine whether the packet is a broadcast packet, a multicast packet, or a unicast packet.
- The output port is determined according to different data packets (zero, one or more output ports are allowed), and if there is no output port, the data packet is discarded.
- According to the membership type of the output port in the VLAN, whether the outgoing packet is tagged or not is determined.
- Sent out the output port.

1) How to determine the VLAN to which a packet belongs:

If a packet is received with a tag and the VID field in the tag is non-zero, the VLAN to which the packet belongs is the V I D value in the tag.

If a packet is received without a tag or with a tag with a VID value of 0, the VLAN to which the packet belongs is the port's default VLAN.

2) How to determine the type of packet:

A received packet is a broadcast packet if its destination MAC address is FF: FF: FF: FF: FF: FF.

A received packet is a multicast packet if it is not a broadcast packet and bit 40 of the destination MAC address is a 1.

A packet is unicast if it is neither a broadcast packet nor a multicast packet.

3) How to determine the output port of a packet:

If the incoming packet is a broadcast packet, all member ports of the VLAN to which the packet belongs are the outgoing ports for the packet.

If the input data packet is a multicast data packet, firstly, searching a two-layer hardware multicast forwarding table according to the destination multicast MAC address and the VLAN to which the data packet belongs; if a matched multicast entry is found, the common port (and operation) in the output port in the multicast entry and the member port in the VLAN to which the data packet belongs is the output port of the data packet; if no common port exists, The packet is dropped. If a matched multicast entry is not found in the two-layer hardware multicast forwarding table, an output port is determined according to the forwarding mode of the two-layer hardware multicast forwarding table, if the multicast forwarding mode is an unregistered multicast forwarding mode, the multicast packet is treated as a broadcast, all member ports of the VLAN to which the multicast packet belongs are the output ports of the data packet, if the multicast forwarding mode is a registered forwarding mode, no output port exists, The packet is dropped.

If the input data packet is a unicast data packet, the layer 2 hardware forwarding table is searched according to the destination MAC address and the VLAN to which the data packet belongs. If a matched entry is found the common port (and operation) in the output port in the entry and the member port of the VLAN to which the data packet belongs is the output port of the data packet. If there is no common port, the data packet is discarded. If no matching entry is found in the Layer 2 hardware forwarding table, the packet is treated as a broadcast packet, and all member ports of the VLAN to which it belongs are the output ports of the packet.

4) Send packets:

After determining the output port of the incoming packet, the packet is sent from all output ports. If an output port is an untagged member of the VLAN to which the packet belongs, the packet is sent out that output port untagged.

If an output port is a tagged member of the VLAN to which the packet belongs, the packet is sent out of that output port with a tag in which the vid value is the value of the VLAN to which the packet belongs.

7.2 VLAN Configuration

This section describes the VLAN configuration in detail, mainly including the following contents:

- Create and delete VLAN
- Configure the VLAN mode of the port
- VLAN Configuration in ACCESS Mode
- VLAN Configuration in TRUNK Mode
- VLAN Configuration in HYBRID Mode
- VLAN Subnet Configuration
- Viewing VLAN Information

7.2.1 Create and delete VLAN

Before creating and deleting VLANs, the user needs to use the VLAN database command in global configuration mode to enter VLAN configuration mode, where VLANs are created and deleted.

The system has created VLAN 1 by default, and VLAN 1 cannot be deleted by the user. The commands for creating and deleting VLANs are shown in the following table:

Command	Description	CLI Mode
vlan <vlan-id>	Create a VLAN. If the VLAN already exists, it will not be pro cessed, otherwise the VLAN will be created. The parameters r ange from 2 to 4094.	VLAN Configuration Mode
no vlan <vlan-id>	Delete a VLAN. If the VLAN does not exist, do not process it. Otherwise, delete the VLAN. The range of parameters is from 2 to 4094.	VLAN Configuration Mode

7.2.2 Configure the VLAN mode of the port

Before configuring the VLAN of the port, you need to specify the VLAN mode of the port, which is ACCESS mode by default. The commands to specify the VLAN mode of a port are listed in the following table:

Command	Description	CLI Mode
switchport mode access	The VLAN mode of the specified port is ACCESS mode. When this command is executed, the port is an untagged m ember of VLAN 1, and the port's default VLAN is 1.	Interface Configuration Mode
switchport mode trunk	The VLAN mode for the specified port is TRUNK mode. When this command is executed, the port is a tagged mem ber of VLAN 1. The default VLAN for the port is 1.	Interface Configuration Mode
no switchport trunk	The VLAN mode of the port is no longer TRUNK mode an d returns to the default, ACCESS mode.	Interface Configuration Mode
switchport mode hybrid	The VLAN mode of the specified port is HYBRID mode. When this command is executed, the port is an untagged m ember of VLAN 1, and the port's default VLAN is 1.	Interface Configuration Mode
no switchport hybrid	The VLAN mode of the port is no longer HYBRID mode a nd returns to the default, ACCESS mode.	Interface Configuration Mode

7.2.3 VLAN Configuration in ACCESS Mode

The VLAN mode of the port needs to be specified as ACCESS mode before VLAN configuration. In this VLAN mode, the port defaults to being an untagged member of VLAN 1, and the default VLAN for the port is 1.ACCESS

VLAN configuration commands in ACCESS mode are shown in the following table:

Command	Description	CLI Mode
switchport access vlan <vlan-id>	The port is configured to be an untagged member of the specified VLAN, and the default VLAN for the port is the specified VLAN. Parameters range from 2 to 4094.	Interface Configuration Mode
no switchport access vlan	The port's VLAN configuration returns to the default, where the port is an untagged member of VLAN 1 and the port's default VLAN is 1	Interface Configuration Mode

7.2.4 VLAN Configuration in TRUNK Mode

VLAN mode of the port shall be specified as TRUNK mode before VLAN configuration. In this VLAN mode, the port defaults to a tagged member of VLAN 1, and the port defaults to VLAN 1. The VLAN configuration commands in the TRUNK mode are shown in the following table:

Command	Description	CLI Mode
switchport trunk native vlan <vlan-id>	Configure the port's default VLAN, also known as pvid. Parameters range from 2 to 4094.	Interface Configuration Mode
switchport trunk allowed vlan all	The configured port is a tagged member of all VLANs, and for new VLANs created later, the port is also a tagged member of those VLANs.	Interface Configuration Mode
switchport trunk allowed vlan none	The port is no longer a tagged member of all VLANs except VLAN 1.	Interface Configuration Mode
switchport trunk allowed vlan add <vlan-list>	Configures the port to be a tagged member of one or more specified VLANs. The parameter < vlan-list > can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameters can be "1", "2-4", or "1,3,5".	Interface Configuration Mode
switchport trunk allowed vlan remove <vlan-list>	Removes a port from one or more specified VLANs and removes it from being a tagged member of those VLANs. The parameter < vlan-list > can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameters can be "1", "2-4", or "1,3,5".	Interface Configuration Mode

7.2.5 VLAN Configuration in HYBRID Mode

The VLAN mode of the port shall be specified as HYBRID mode before VLAN configuration of the port. In this VLAN mode, the port is an untagged member of VLAN 1 by default, and the port's default VLAN is 1. The VLAN configuration commands in HYBRID mode are shown in the following table

Command	Description	CLI Mode
switchport hybrid native vlan <vlan-id>	The configuration port is an untagged member of the specified VLAN and the port's default VLAN is the specified VLAN. The parameters range from 2 to 4094.	Interface Configuration Mode
no switchport hybrid native vlan	The port is removed from the default VLAN and is no longer a t agged or untagged member of the default VLAN, and the port's default VLAN is returned to 1.	Interface Configuration Mode
switchport hybrid allowed vlan all	Configure the port to be a tagged member of all VLANs except VLAN1, and to be a tagged member of new VLANs created in the future.	Interface Configuration Mode
switchport hybrid allowed vlan none	The port is no longer a tagged or untagged member of all VLAN s except VLAN 1, and the port's default VLAN returns to 1.	Interface Configuration Mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged enable	Configures the port to be a tagged member of one or more specified VLANs. The parameter < vlan-list > can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameters can be "1", "2-4", or "1,3,5"..	Interface Configuration Mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	Configures the port to be an untagged member of one or more specified VLANs. The parameter < vlan-list > can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameters can be "1", "2-4", or "1,3,5"	Interface Configuration Mode
switchport hybrid allowed vlan remove <vlan-list>	Removes a port from one or more specified VLANs and removes it from being a tagged or untagged member of those VLANs. If the port's default VLAN belongs to the specified VLAN, the default VLAN returns to 1.	Interface Configuration Mode

7.2.6 Viewing VLAN Information

The commands for viewing VLAN information are shown in the following table:

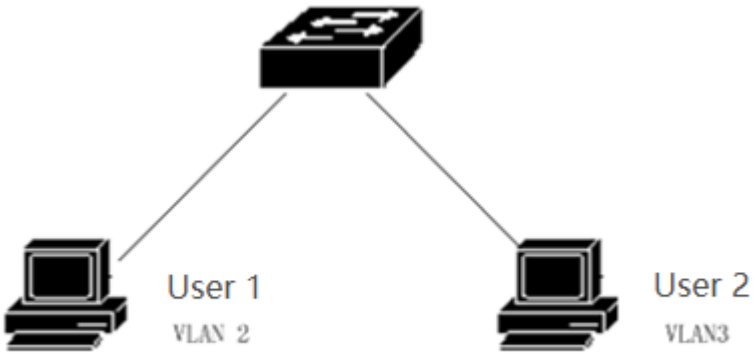
Command	Description	CLI Mode
show vlan [vlan-id]	If no parameter is entered, all VLAN information is dis played. If a parameter is entered, the information of a s pecified VLAN is displayed. The parameter range is fr om 1 to 4094.	Normal mode, privileged mode
show interface	Displays VLAN-related information of all ports of the system, such as VLAN mode, default VLAN, etc.	Normal mode, privileged mode
show running-config	View the current configuration of the system to view t he configuration of the VLAN.	Privileged mode

7.3 Example VLAN configuration

7.3.1 PORT-based VLAN

1) configurations

There are two users, User 1 and User 2. The two users need to be in different VLANs because of the different network functions and environments they use. User 1 belongs to VLAN2 and is connected to port ge1/1 on the switch. User 2 belongs to VLAN3 and is connected to port ge1/2 on the switch.



The switch is configured as follows:

Create VLAN

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Assign a port to a VLAN

Switch#config t

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 2

Switch(config-ge1/1)#exit

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 3

2) Debug

After configuration, it is found that the PCs between different VLANs cannot communicate, which is a normal phenomenon, because the communication between different VLANs must be forwarded through three layers of routing. If PCs in the same VLAN cannot communicate, verify the following:

show vlan

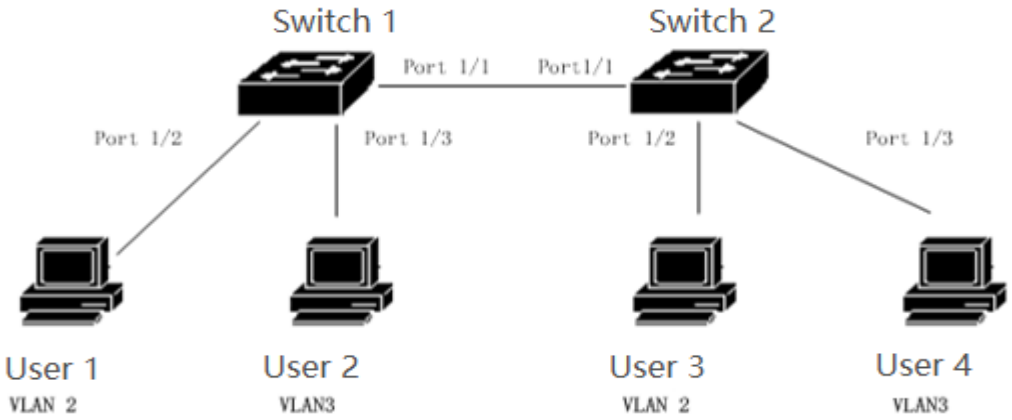
View the member ports of all VLAN

show vlan <vlan-id>

Check whether the port connected to a specific PC is in the specified VLAN

7.3.2 802.1Q-based VLAN

1) configurations



There are two switches connected to two users:

User	Belonging VLAN	Connection Port	Owned switch	Cascade port
User1	2	1/2	switch1	1/1
User2	3	1/3	switch1	1/1
User3	2	1/2	switch2	1/1
User4	3	1/3	switch2	1/1

Configuration is required on both switches.

Switch 1 Configuration:

Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 2
Switch(config-ge1/1)#switchport trunk allowed vlan add 3
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 3

Switch 2 Configuration:

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Switch#config t

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk allowed vlan add 2

Switch(config-ge1/1)#switchport trunk allowed vlan add 3

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 2

Switch(config-ge1/2)#exit

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode access

Switch(config-ge1/3)#switchport access vlan 3

2) Debug

Vlans across switches, PCs in the same VLAN are able to communicate, if not. The following must be checked:

- Whether the port connected to the PC belongs to the corresponding VLAN and applies ACCESS mode to join the VLAN.
- Cascade port 1/1 is added to each VLAN and port 1/1 is in TRUNK mode.

7.4 MAC, IP subnet, protocol VLAN

7.4.1 Introduction to MAC, IP Subnet and Protocol VLAN

MAC-based VLANs are partitioned based on the source MAC address of the message. After the device receives an untagged (or tag 0) packet from the port, it will determine the VLAN to which the packet belongs according to the source MAC address of the packet, and then automatically divide the packet into the specified VLAN for transmission;

VLANs based on IP subnets are divided according to the source IP address and subnet mask of the message. After receiving the untagged message from the port, the device will determine the VLAN to which the message belongs according to the source address of the message, and then automatically divide the message into the specified VLAN for transmission. This feature is mainly used to transmit the message sent by the specified network segment or IP address in the specified VLAN;

A protocol-based VLAN assigns different VLAN IDs to packets received by a port according to the protocol type to which the packets belong. The protocols that can be used to divide VLANs are IP, IPV6, IPX, and so on.

7.4.2 MAC, IP Subnet, Protocol VLAN Configuration

Before configuring VLANs based on MAC, IP subnets, and protocols, the corresponding VLANs must be created.

Command	Description	CLI Mode
mac-vlan mac WORD vlan <1-4094>	Create a VLAN based on the source MAC addr	VLAN Configuration Mode
no mac-vlan mac WORD	Deletes a VLAN based on the source MAC addr	VLAN Configuration Mode
no mac-vlan	Remove all VLANs based on source MAC addr	VLAN Configuration Mode
mac-vlan enable	Enable the MAC-VLAN feature on the interface	Interface Configuration Mode
mac-vlan disable	Turn off the MAC-VLAN function of the interface	Interface Configuration Mode
show mac-vlan	Displays all VLANs based on the source MAC addr	Privileged mode
ip-subnet-vlan ip A.B.C.D A.B.C.D vlan <1-4094>	Create a VLAN based on the source IP subnet	VLAN Configuration Mode
no ip-subnet-vlan ip A.B.C.D A.B.C.D	Delete a VLAN based on the source IP subnet	VLAN Configuration Mode
no ip-subnet-vlan	Delete all VLANs based on the source IP subnet	VLAN Configuration Mode
ip-subnet-vlan enable	Initiates the VLAN functionality of the interface based on the source IP subnet	Interface Configuration Mode
ip-subnet-vlan disable	Turn off the VLAN function based on the source IP subnet of the interface	Interface Configuration Mode
show ip-subnet-vlan	Displays all VLANs based on the source IP subnet	Privileged mode
protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>) vlan <1-4094>	Create a protocol-based VLAN	Interface Configuration Mode
no protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>)	Delete a protocol-based VLAN	Interface Configuration Mode
no protocol-vlan	Remove all protocol-based VLAN	Interface Configuration Mode
show protocol-vlan	Displays all protocol-based VLAN	Privileged mode
show vlan-partition interface IFNAME	Hows MAC, IP subnet-based VLANs enabled on an interface	Privileged mode

7.5 Voice VLAN

7.5.1 Introduction to Voice VLAN

Voice VLAN is a VLAN specially divided for the voice data flow of users. By dividing the Voice VLAN and adding the port connected to the voice device to the Voice VLAN, QoS (Quality of Service) parameters can be configured for the voice data to improve the priority of the voice data packet and ensure the call quality.

The device may determine whether the data stream is a voice data stream according to the OUI field of the source MAC address in the data packet entering the port. The message whose source MAC address conforms to the voice equipment OUI address set by the system is regarded as voice data flow and is divided into Voice VLAN for transmission.

The user can preset the OUI address or use the default OUI address as the judgment standard, as follows:

Serial number	OUI Addr	Manufacturer
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

Manually add the IP phone access port to the Voice VLAN. Then the OUIaddress is matched by identifying the source MAC of the message. After successful matching, the system will issue ACL rules and configure the priority of the message

7.5.2 Voice VLAN Configuration

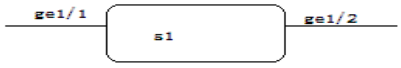
Before configuring Voice VLANs, you must create the corresponding VLANs.

Command	Description	CLI Mode
voice-vlan oui WORD mask WORD	Configure User OUI	Global Configuration Mode
voice-vlan oui WORD mask WORD description WORD	Configure the user OUI and name it	Global Configuration Mode
no voice-vlan oui WORD mask WORD	Delete user OUI configuration by OUI ad dress and mask	Global Configuration Mode
no voice-vlan oui description WORD	Delete User OUI Configuration by Namin g	Global Configuration Mode
no voice-vlan oui	Delete all user OUI configuration	Global Configuration Mode
no voice-vlan default-oui WORD mask WORD	Remove defualt OUI configuration by O UI address and mask	Global Configuration Mode
no voice-vlan default-oui description WORD	Remove defualt OUI configuration by na me	Global Configuration Mode
no voice-vlan default-oui	Delete all defualt OUI configuration	Global Configuration Mode
voice-vlan default-oui resume	Restore all defualt OUI configuration	Global Configuration Mode

show voice-vlan oui	Display all defualt and user OUI configur ation	Privileged mode
voice vlan <1-4094> (enable|disable)	Voice VLAN enabled on the interface	Interface Configuration Mode
voice vlan qos remark cos <0-7> dscp <0-63>	The interface is configured with QoS prio rity, cos value is 6, and dscp value is 46	Interface Configuration Mode
no voice vlan qos	Restore interface QoS priority default con figuration	Interface Configuration Mode
no voice vlan	Deleting an Interface Configuration Voic e VLAN	Interface Configuration Mode
show voice-vlan	Shows how Voice VLANs are configured on all interface	Privileged mode

7.5.3 Voice VLAN Configuration Example

Configure the voice data flow (0009.ca00.0000) to flow in from the port ge1/1 and flow out from the port ge1/2 with tag 2, as shown in the following figure



Switch S1 is configured as follows:

Switch#con t
Switch(config)#vlan da
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#int ge1/1
Switch(config-ge1/1)#sw mod hy
Switch(config-ge1/1)#sw hybrid allowed vlan add 2 egress-tagged disable
Switch(config-ge1/1)#voice vlan 2 en
Switch(config-ge1/1)#voice vlan 2 enable
Switch(config-ge1/1)#int ge1/2
Switch(config-ge1/2)#sw mod tr
Switch(config-ge1/2)#sw trunk allowed vlan add 2
Switch(config-ge1/2)#exit
Switch(config)#voice-vlan oui 0009.ca00.0000 mask ffff.ff00.0000
Switch(config)#

7.6 VLAN mapping

7.6.1 Introduction to VLAN Mapping

The VLAN Mapping function can modify the VLAN Tag carried by the message and provide the following mapping relationship: 1:1 VLAN Mapping: Modify the VLAN ID in the VLAN Tag carried by the message to another VLAN ID.

Before you can configure VLAN mappings, you must create the corresponding VLANs.

7.6.2 VLAN mapping configuration

Command describe CLI Mode

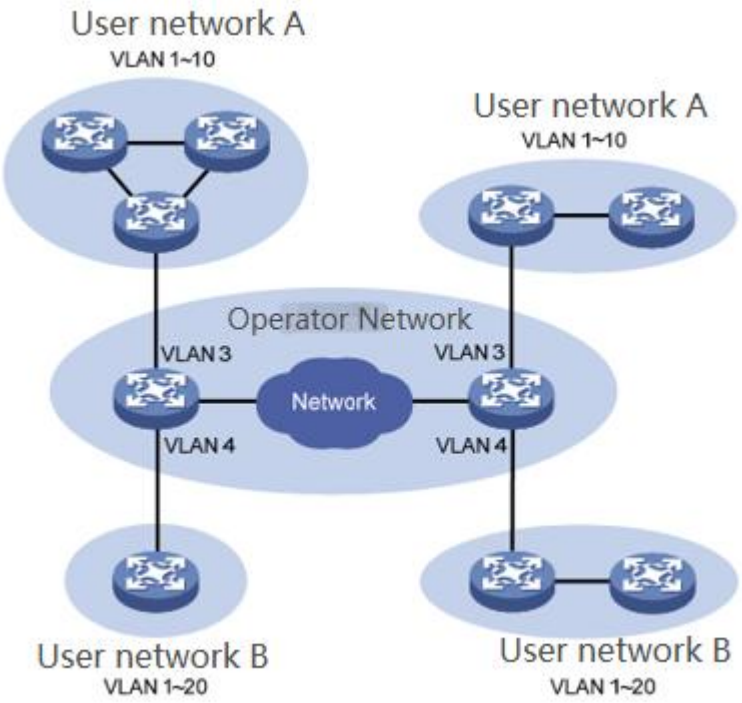
Command	Description	CLI Mode
vlan-mapping vlan <1-4094> map-vlan <1-4094>	Configure a VLAN mapping for the port	Interface Configuration Mode
no vlan-mapping vlan <1-4094>	Deletes a VLAN mapping for a port	Interface Configuration Mode
no vlan-mapping	Deletes all VLAN mappings for a port	Interface Configuration Mode
vlan-mapping enable	VLAN mapping of the boot port	Interface Configuration Mode
vlan-mapping disable	Close the VLAN mapping relationship of the port	Interface Configuration Mode
show vlan-mapping	Displays all configured VLAN mapping	Privileged mode

7.7 Q-in-Q

7.7.1 Introduction to QinQ

The port Q-in-Q feature provided by the device is a simple and flexible two-layer VPN technology, which encapsulates the outer VLAN Tag for the user's private network packet on the operator's network edge device, so that the packet carries the two-layer VLAN Tag across the operator's backbone network (public network). In the public network, the device forwards the message only according to the outer layer VLAN Tag, and learns the source MAC address table of the message into the MAC address table of the VLAN where the outer layer Tag is located, while the private network VLAN Tag of the user is transmitted as the data part of the message in the transmission process.

The QinQ feature allows operators to use one VLAN to serve a user network that contains multiple VLANs. As shown in the figure below, the private VLANs of user network A are VLANs 1 to 10, and the private VLANs of user network B are VLANs 1 to 20. The VLAN assigned by the operator to the user network A is VLAN 3, and the VLAN assigned to the user network B is VLAN 4. When the message with the VLAN Tag of the user network A enters the operator network, The outside of the packet will be encapsulated with the VLAN Tag with the upper layer VLAN ID of 3. When the packet with the VLAN Tag of the user network B enters the operator network, the outside of the packet will be encapsulated with the VLAN Tag with the upper layer VLAN ID of 4. In this way, the messages of different user networks are completely separated during transmission in the public network, and even if the VLAN ranges of the two user networks overlap, no confusion occurs during transmission in the public network.



The QinQ feature enables the network to provide up to 4094X4094 VLANs to meet the requirements of the metropolitan area network for the number of VLANs. It mainly solves the following problems:

(1) Alleviate the problem of increasingly scarce public network VLAN ID resources.

(2) Users can plan their own private network VLAN ID, which will not cause conflict with the public network VLAN ID.

(3) This paper provides a simple solution of layer 2 VPN for small man or enterprise network.

QinQ can be divided into two types: basic QinQ and flexible QinQ.

(1) Basic QinQ: Basic QinQ is implemented in a port-based manner. After the basic QinQ function of the port is enabled, when the port receives a packet, the device will tag the packet with the VLAN Tag of the default VLAN of the port. If a message with VLAN Tag is received, the message becomes a double-tag message; if a message without VLAN Tag is received, the message becomes a message with port default VLAN Tag.

(2) Flexible QinQ: Flexible QinQ is a more flexible implementation of QinQ, which is based on the combination of ports and VLANs. In addition to realizing all basic QinQ functions, different actions can be taken for messages received by the same port according to different VLANs, and different outer VLAN Tags can be added for messages with different inner VLAN IDs.

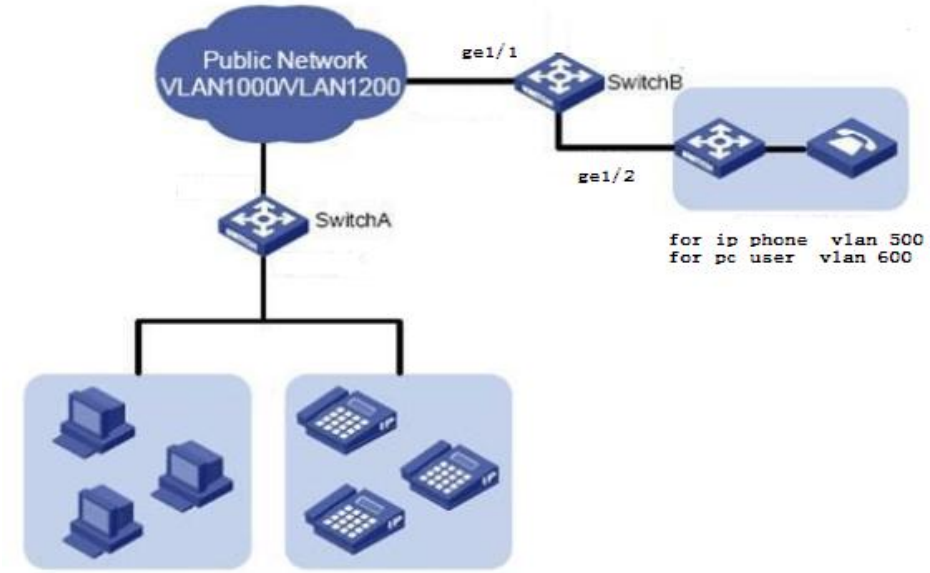
7.7.2 Q in Q configuration

Command	Description	CLI Mode
qinq tpid WORD	Configure the tpid value carried in the port VLAN Tag, which is 0x8100 by default	Interface Configuration Mode
no qinq tpid	Restore port default tpid	Interface Configuration Mode
qinq uplink	Configure the port as an uplink port	Interface Configuration Mode
no qinq uplink	Unconfigure the port for uplink	Interface Configuration Mode
qinq customer	Configure the port as customer port	Interface Configuration Mode
no qinq customer	Unconfigure the port from customer	Interface Configuration Mode
qinq outer-vid <1-4094> inner-vid VLAN_ID	Configure one VLAN translation for the interface	Interface Configuration Mode
no qinq outer-vid <1-4094> [inner-vid VLAN_ID]	Deletes a VLAN translation for an interface	Interface Configuration Mode
show qinq	Display qinq status for all configurations	Privileged mode

7.7.3 QinQ configuration examples

SwitchB ports ge1/1 to the public network and ge1/2 to the PC and telephony server. The VLAN used by the PC is 600, and the VLAN used by the IP phone is 500. The VLAN 100 and the VLAN 200 are allowed to pass through the public network. In order to transmit the user data of the PC in the public network through the VLAN 200, the data of the IP phone is transmitted in the public network through the VLAN 100.

The networking diagram is as follows



Switch B is configured as follows:

```
Switch#con t
Switch(config)#vlan da
Switch(config-vlan)#vlan 100
Switch(config-vlan)#vlan 200
Switch(config-vlan)#exit
Switch(config)#int ge1/1
Switch(config-ge1/1)#sw mod tr
Switch(config-ge1/1)#switchport trunk allowed vlan add 100
Switch(config-ge1/1)#switchport trunk allowed vlan add 200
Switch(config-ge1/1)#qinq uplink
Switch(config-ge1/1)#int ge1/2
Switch(config-ge1/2)#switchport mode hybrid
Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged dis
Switch(config-ge1/2)#switchport hybrid allowed vlan add 200 egress-tagged dis
Switch(config-ge1/2)#qinq customer
Switch(config-ge1/2)#qinq outer-vid 100 inner-vid 500
Switch(config-ge1/2)#qinq outer-vid 200 inner-vid 600
Switch(config-ge1/2)#
```

Switch#show qinq

ifname	tpid	dtag-mode	outer-vid	inner-vid
ge1/1	**0x8100**	**uplink**	**-**	**-**
ge1/2	**0x8100**	**customer**	**100**	**500**
ge1/2	**0x8100**	**customer**	**200**	**600**

Switch#

8. Configuring QoS

This chapter describes QoS and its configuration, mainly including the following contents:

- QoS Introduction
- QoS Configuration
- QoS Configuration Example

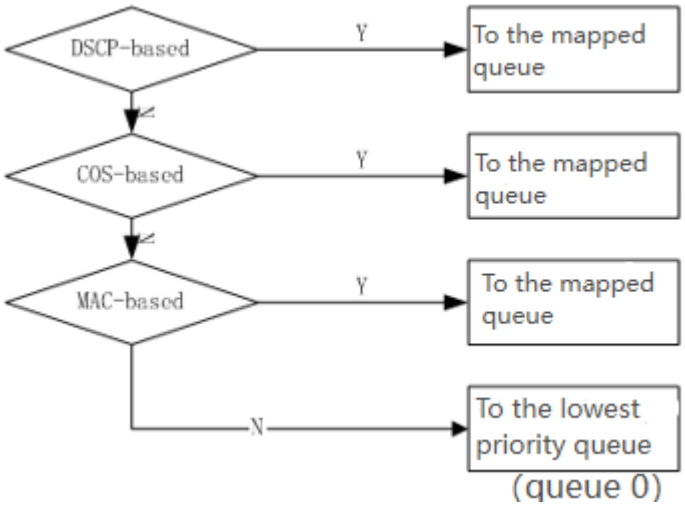
8.1 QoS Introduction

Using the QoS features of the switch, you can prioritize the important traffic being forwarded through the switch, making more rational use of your network's bandwidth and making network performance predictable.

In a switch, the priority information of a data packet at an input terminal determines the queue of the data packet at an output terminal.

The switch implements QoS based on COS (802.1 p), QoS based on DSCP (DiffServ) and QoS based on MAC. QoS based on DSCP can be configured on a physical port; QoS based on COS is enabled by default on all physical ports. The MAC-based Qos function is configured in the MAC binding function. Only one QoS feature can be configured per physical port.

The following figure shows the packet forwarding process with QoS enabled:



The switch supports eight priority queues from 0 to 7, with queue 7 having the highest priority and queue 0 having the lowest priority. There are four scheduling modes of priority queue: SP, RR, WRR and WDRR. SP is strict priority scheduling, that is, it always gives priority to forwarding the data packets of queue 7, and does not begin to forward the data packets of queue 6 until the data packets of queue 7 are forwarded, and does not begin to forward the data packets of queue 5 until the data packets of queue 6 are forwarded, and finally forwards the data packets of queue 0.RR is a round-robin scheduling method. When the switch forwards a packet, it polls and forwards the packet from the high priority queue to the low priority queue, and each queue forwards one packet. WRR refers to polling with priority. When forwarding a data packet, the switch forwards the data packet by polling from the high priority queue to the low priority queue according to the configuration of the priority. First, the data packet with the number of priorities is forwarded from the high priority queue, and then the data packet with the number of priorities is forwarded from the second high priority queue until the lowest priority queue finishes forwarding, and then the data packet is forwarded from the high priority queue, and so on. WDRR is a weighted round-robin scheduling mode, that is, the weight of queue 3 is 4, so in

a certain round, it can forward 5 packets, and in the next round, it can only forward 3 packets. This flexibility is more suitable for highly aggregated network environments.

For the convenience of user configuration, we introduce the concept of QosProfile. QosProfile is an attribute that configures the mapping relationship between the 802.1 p and the priority queue. This attribute cannot be configured by the user. Their mapping relationship is shown in the following table:

Qos Profile	802.1p (CoS) values	Priority Queue
Qp0	0	0
Qp1	1	1
Qp2	2	2
Qp3	3	3
Qp4	4	4
Qp5	5	5
Qp6	6	6
Qp	7	7

8.1.1 QoS based on COS

By default, the port has QoS over COS enabled. The switch obtains the priority value of the VLAN TAG in the data packet entering the port, and determines the output queue of the data packet according to the mapping relationship between the COS value configured by the user and the queue. If the packet has no VLAN TAG or the VID of the VLAN TAG is 0, the switch fills the packet according to the default VID of the port configured by the user and the default priority of the port, and then determines the output queue of the packet according to the default priority.

8.1.2 DSCP based QoS

If DSCP-based QoS is enabled on a port, the switch obtains the DSCP value in the IP packet entering the port and determines the output queue for the packet based on the mapping between the user-configured DSCP value and the queue.

8.1.3 MAC-based QoS

When a data packet enters the switch, the switch searches the two-layer forwarding table of the switch according to the destination MAC of the data packet and the VID of the VLAN TAG of the data packet, and if a target table item is found, the output queue of the data packet is determined according to the queue mapping relationship configured by the target table item.

8.1.4 Policy-based QOS

QoS policies include classes, policies, and actions. Classes are used to identify flows, and users can define a series of rules through commands to classify packets. Policy actions are used to define the QoS actions taken by packets matching the rules. If a port is enabled with policy-based QoS, the switch will classify the data packets entering the port. For the data packets meeting the classification requirements, the switch will process the data packets of the port according to the corresponding policy action, and for the data packets not meeting the classification requirements, the switch will not process them, and then determine the output queue of the data packets according to the priority mapping relationship.

8.2 QoS Configuration

8.2.1 Default configuration for QoS

Configuration Item	Value	Configurable or not
Number of queue	8	No
Dispatching Mode	WRR	Yes
Whether to enable SP scheduling method	disable	Yes
Whether to enable RR scheduling method	disable	Yes
Whether to enable WDRR dispatching mode	disable	Yes
Queue Weight	QP0[1],QP1[2],QP2[4],QP3[8] QP4[16],QP5[32],QP6[64] QP7[127]	Yes
Mapping relationship between COS and qosprofile	COS0~ [qp0] COS1~ [qp1] COS2~ [qp2] COS3~ [qp3] COS4~ [qp4] COS5~ [qp5] COS6~ [qp6] COS7~ [qp7]	No
Mapping relationship between DSCP and qosprofile	DSCP0~DSCP7[qp0] DSCP8~DSCP15[qp1] DSCP16~DSCP23[qp2] DSCP24~DSCP31[qp3] DSCP32~DSCP39[qp4] DSCP40~DSCP47[qp5] DSCP48~DSCP55[qp6] DSCP56~DSCP63[qp7]	Yes
Whether the interface has dscp-based QoS enabled	disable	Yes
Whether the interface is enabled for COS based QoS	enable	No
Interface user priority (COS value)	0	Yes

8.2.2 Configure the scheduling method

The default scheduling mode of the switch is WRR. SP, RR and WDRR scheduling modes can be configured through commands.

Command	Description	CLI Mode
qos sched {rr | sp | wrr | wdrr}	Configure QoS scheduling mode	Interface Configuration Mode

8.2.3 Configure queue weight

Command	Description	CLI Mode
qos qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7} weight<1-127>	Configure the weight of each priority queue	Interface Configuration Mode
no qos qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7} weight	The weight configuration of the recovery queue is the default configuration	Interface Configuration Mode

The queue weight refers to the number of packets forwarded by the priority queue in one round of polling. Therefore, when configuring the queue weight, it should be noted that the weight of the low priority queue should not exceed the weight of the high priority queue.

8.2.4 Configure the mapping relationship between DSCP and QosProfile

Command	Description	CLI Mode
qos dsc-map-qp <0-63> qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7}	Configure the mapping relationship between DSCP and QosProfile	Interface Configuration Mode
no qos qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7} weight	Restore the mapping relationship between DSCP and qosprofile to the default configuration.	Interface Configuration Mode

8.2.5 Configuring Port DSCP Based QoS

Qos functions can only be configured on physical ports, not on TRUNK or Layer 3 interfaces.

Command	Description	CLI Mode
qos dscp-based	Enables the port's DSCP-based Qos functionality.	Interface Configuration Mode
no qos dscp-based	Turn off the port's DSCP based Qos feature.	Interface Configuration Mode

8.2.6 Configure port user priority (COS value)

Command	Description	CLI Mode
qos user-priority <0-7>	Configure the user priority of the port (COS value)	Interface Configuration Mode
no qos user-priority	The user priority (COS value) of the recovery port is the default configuration.	Interface Configuration Mode

8.3 QoS Configuration Example

Configure the ge1/3 user priority (COS value) as 3, and the QoS function based on COS is enabled by default:

Switch#configure terminal

Switch#(config)#interface ge1/3

Switch#(config-ge1/3)#qos user-priority 3

Switch#(config-ge1/3)#end

Configure interface ge1/3 to enable DSCP based QoS with DSCP value 3 mapped to priority queue 2:

Switch#configure terminal

Switch#(config)#interface ge1/3

Switch#(config-ge1/3)#qos dscp-map-qp 3 qosprofile qp2

Switch#(config-ge1/3)#qos dscp-based

Switch#(config-ge1/3)#end

8.3.1 Policy QoS Configuration Example

Configure ACLs to capture traffic from source MAC1, MAC2, and MAC3 \n

(The ACL rules can be modified as required. This is just a simple example.)

access-list 700 permit host 0000.0000.1111 vid any ip any any
access-list 701 permit host 0000.0000.2222 vid any ip any any
access-list 702 permit host 0000.0000.3333 vid any ip any any

Configure the QOS class to match the data flow of source MAC1, MAC2 and MAC3 respectively

(The matching rule cos or dscp can be modified as required. This is just a simple example.)

qos class 10 match acl 700
qos class 11 match acl 701
qos class 12 match acl 702

Configure the QOS policy, and re-mark the 802.1p priority of the data flows whose sources are MAC1, MAC2 and MAC3 respectively

(the policy can be modified as required, and this is only a simple example).

qos policy 10 class 10 remark cos 7
qos policy 10 class 11 remark cos 5
qos policy 10 class 12 remark cos 3
Send QOS policy to port
interface ge1/2
qos apply-policy 10

9. Configuring MSTP

This chapter describes MSTP and its configuration, mainly including the following contents:

- MSTP Introduction
- MSTP Configuration
- MSTP Configuration Example

9.1 MSTP Introduction

The switch supports the IEEE 802.1d, IEEE 802.1w, and IEEE 802.1s STP protocols.

9.1.1 Overview

MSTP uses RSTP to quickly converge multiple VLANs into a spanning-tree instance, with each instance having a spanning-tree topology that is independent of other spanning-tree instances. This architecture provides multiple forwarding paths for traffic, enables load balancing, and reduces the number of spanning tree instances required to support a large number of VLANs.

9.1.2 Multiple spanning tree domain

For instances to participate in Multiple Spanning Tree (MST) calculations, the switch must be configured consistently with the same MST configuration information. A collection of connected switches with the same MST configuration constitutes an MST domain.

The MST configuration determines the domain to which each switch belongs. The configuration includes the domain name, revision number, and MST instance and VLAN assignment mappings; this information is generated as a unique Digest in the MST configuration. The summaries in the same domain are the same and must be the same, which can be seen with the show spanning- tree MST config command.

A domain can have one or more members with the same MST configuration; each member must be capable of handling RSTP BPDUs. There is no limit to the number of MST domains in a network, but each domain supports up to 16 instances. You can assign only one VLAN to a spanning-tree instance at a time.

9.1.3 IST, CIST, and CST

Internal Spanning Tree (IST). A spanning tree that runs within the MST domain.

At each MSTP domain, the MSTP maintains multiple generated instances. Instance 0 is a special instance of a domain called IST. All other MST instances are the numbers 1 through 15.

This IST is simply a Spanning Tree instance that receives and sends BPDUs; all other Spanning Tree instance information is compressed in MSTI BPDUs. Because MSTI BPDUs carry information for all instances, the number of BPDUs that need to be processed by a switch that supports multiple spanning tree instances means simplification.

All MST instances in the same domain share the same protocol timer, but each MST instance has its own topology parameters, such as a root switch ID, root path cost, and so on. By default, all VLANs are assigned to ISTs.

The Common and Internal Spanning Tree (CIST) is the collection of all ISTs in each MST domain and the Common Spanning Tree (which connects the MST domain to a single spanning tree).

A spanning tree computed within a domain looks like a subtree of the CST that contains all the switch domains. The CIST is formed as a result of a spanning tree computation run between switches that

support the 802.1 W and 802.1 D protocols. The CIST in the MST domain is the same as the CST outside the domain.

Common Spanning Tree (CST), a spanning tree that runs between MST domains.

9.1.4 Intra-domain operation

ISTs connect all MSTP switches in a domain. When the IST converges, the root of the IST becomes the IST master, which is the switch with the lowest bridge ID and path cost to the CST root in the domain. If there is only one domain in the network, the IST master is also the CST root. If the CST root is outside the domain, an MSTP switch at the boundary of the domain is selected as the IST master.

When an MSTP switch initializes, it sends BPDUs requesting itself as the CST root and IST master, with the path cost to the CST root and IST master set to 0. The switch also initializes all MST instances and asks to be their root. If the switch receives the MST root information in preference to the information stored on the current port (low bridge ID, low path cost, etc.), it relinquishes its claim to be the IST master.

In initialization, a domain may have many subdomains, each with its own IST master. When the switch receives a higher priority IST message, it leaves its old subdomain to join a new subdomain that may contain a true IST master. Thus all subdomains are contracted, except for the subdomain containing the true IST master.

For correct operation, all switches in the MST domain must recognize the same IST master. Therefore, any two switches in the domain synchronize the roles of the ports of one of their MST instances only if they converge to a common IST master.

9.1.5 Interdomain operation

If there are multiple domains or legacy 802.1 D switches in the network, the MSTP establishes and maintains the CST, which includes all the MST domains and all the legacy STP switches in the network. MST instances are associated with ISTs at the domain boundary to become CSTs.

The IST connects all switches within the MSTP domain and looks like a subtree of the CST (enclosing all switch domains). The root of the subtree becomes the IST master. The MST domain looks like a virtual switch adjacent to the STP switch and the MST domain.

Only the CST instances send and receive BPDUs, and the MST instances add their spanning-tree information to the BPDUs to interact with neighbour ing switches and compute the final spanning-tree topology. Because of this, the spanning tree parameters related to BPDU delivery (e.g., hello time, forward time, max-age, and max-hops) are configured only in the CST instance and do not affect all MST instances. Parameters related to the spanning tree topology (e.g., switch priority, port VLAN cost, port VLAN priority) can be configured in the CST instance and the MST instance.

MSTP switches use version 3 RSTP BPDUs or 802.1D BPDUs to communicate with 802.1D switches. MSTP switches use MSTP BPDUs to communicate with MSTP switches.

9.1.6 Count of hop

The message-age and maximum-age information is not used by the IST and MST instances in BPDUs that are configured to compute the spanning-tree topology. Instead, the path to the root is spent and a hop-count mechanism equivalent to the IP TTL is used.

You can configure the maximum hop count for that domain and apply it to that domain IST and all MST instances. The hop count implementation is the same as the message-age result (determined after causing a reconfiguration). The root switch of the instance always sends a BPDU (or-M-record) with a cost of 0 and a hop-count of Max. When a switch receives a BPDU, it decrements the remaining hop

count by one and propagates the remaining hop count in the BPDU it generates. When the count reaches 0, the switch discards the BPDU and ages the information for that port.

Within a domain, the Message-age and maximum-age information in the RSTP BPDU portion remains consistent, and the same value is propagated across the specified ports of the boundary domain.

9.1.7 Boundary Port

A boundary is a port that connects the MST domain to a spanning-tree domain running RSTP alone, or a spanning-tree domain running 801.1 D alone, or an MST domain configured differently. A boundary port is also connected to a LAN whose designated switch is either a single spanning-tree switch or a switch with a different MST domain configuration.

On the border ports, the MST port role is not important, and their state is forced to be the same as the IST port state (when the IST port is forwarding, the MST port on the border is forwarding). An IST port at the border can have any role other than a backup port.

On a shared boundary connection, the MST port waits in the blocking state for the forward-delay time to expire before transitioning to the learning state. The MST port waits for another forward-delay time to expire before transitioning to forwarding.

If the border port is a point-to-point connection and is the IST root port, the MST port transitions to the forwarding state as soon as the IST port transitions to the forwarding state.

If a boundary port transitions to the forwarding state in an instance, it is forwarding in all instances, and a topology change is triggered. If a boundary port with an IST root or designated port role receives a topology change advertisement, the MSTP switch triggers a topology change on the IST instance and all MST instances on that port that are active.

9.1.8 Interoperability of MSTP and 802.1d STP

A switch running MSTP supports a built-in protocol migration mechanism that enables it to coordinate with 802.1 D. If the switch receives a BPDU from a port that is 802.1 D configuration, it sends the 802.1 D BPDU on that port. An MSTP switch can detect when a 802.1 BPDU is received on a border port of a domain, and when an MSTP BPDU or RSTP BPDU is received on a border port of a different domain.

However, if a switch no longer receives 802.1 D BPDUs, it does not automatically revert to MSTP mode because it cannot determine whether the other switch has been removed from the connection unless the other switch is the designated switch. Also, when the switch connected to this switch has joined the domain, the switch may continue to assign a boundary port role to a port. Restart the migration process for the protocol (force negotiation with the neighbour switch).

If all of the other switches in the connection are RSTP switches, they can process MSTP BPDUs and process RSTP BPDUs. Therefore, the MSTP switch sends either a version 0 configuration and TCN BPDU or a version 3 MSTP BPDU at the border port. A boundary port connected to a LAN whose designated switch is either a single spanning-tree switch or a switch with a different MST configuration.

9.1.9 Port Role

MSTP adopts the fast convergence algorithm of RSTP. MSTP port roles and fast convergence are briefly described below in conjunction with RSTP.

RSTP provides fast convergence for specifying port roles and determining the active topology. RSTP is based on the IEEE 802.1 DSTP, which chooses the high-priority switch as the root switch. When RSTP assigns a port role to a port:

- Root port-Provides optimal path cost when the switch forwards packets to the root switch.
- Designated port-Connect to a designated switch. The lowest path cost is incurred when forwarding packets from the LAN to the root switch. The port through which a designated switch connects to a LAN is called a designated port.
- Alternate port-Provides an alternate path to the root switch for the current root port.
- Backup port-Acts as a backup specifying the port to the path of the leaves of the spanning tree. A Backup port exists only when two ports are connected together in a point-to-point loop or when a switch has two or more ports connected to a shared LAN segment.
- Disable port-There is no port role in the spanning-tree operation.
- Master Port-Located at the domain root or on the shortest path to the overall root, it is the port that connects the domain to the overall root.

The root port or designated port role is included in the active topology. Alternate or backup port roles are not included in the active topology.

In a stable topology and with fixed port roles throughout the network, RSTP ensures that every root port and designated port immediately migrates to the forwarding state while all alternate ports and backup ports are always in the discarding state. Port state controls forwarding and learning processing.

Fast Convergence

RSTP provides fast recovery in the event of a switch failure, port failure, or LAN failure, and it provides fast recovery for edge ports, new root ports, and connections to a point-to-point connection:

- Edge ports-If you configure a port as an edge port, the edge port immediately transitions to the forwarding state. You can open it for boundary ports only if the port is connected to a single terminal or device that is determined not to need to compute the spanning tree.
- Edge ports-If you configure a port as an edge port, the edge port immediately transitions to the forwarding state. You can open it for boundary ports only if the port is connected to a single terminal or device that is determined not to need to compute the spanning tree.
- Root ports-If RSTP selects a new root port. It blocks an old root port and immediately migrates the new root port to forwarding state.

Topological change

This section describes the differences between RSTP and 802.1D in handling spanning-tree topology changes.

- **Detection**-Unlike 802.1 D where any transition between blocking and forwarding States causes a topology change, only a transition from blocking to forwarding state causes a RSTP topology change (topology changes are only considered to increase connectivity). A state change at an edge port does not cause a topology change. When an RSTP switch detects a topology change, it floods the information it learned to all nonedge ports except the port that received the TC information.
- **Notification**-Unlike 802.1 D, which uses the TCN BPDU, RSTP does not use it. However, the RSTP switch processes and generates TCP BPDUs for interoperability with 802.1 D. Acknowledgement-When a RSTP switch receives a TCN message on a specified port from a 802.1 D switch, it responds with a D BPDU with the 802.1 and the TCA flag set.However, if the TC-while timer (which is the same topology-change timer as 802.1 D) is active, is connected to the 802.1 D switch at the root port and receives a configuration BPDU with a TCA, the TC-while timer is reset. This behavior is only required to support 802.1 D switches.

RSTP BPDUs never have the TCA flag.

- **Propagation**-When an RSTP switch receives a TC message from another switch on a designated or root port, it is propagated to all non-edge ports, designated ports, and root ports (except the receiving port). All such ports on the switch start a TC-while timer and flood the information they learn.
- **Protocol migration**-For backward compatibility with 802.1D switches, RSTP selectively sends 802.1D configuration BPDUs and TCN BPDUs on a per-port basis.

When one has been initialized, the migrate-delay timer starts (specifying the minimum value during which RSTP BPDUs are sent) and RSTP BPDUs are sent. When the timer is active, the switch processes all BPDUs received from the port and ignores the protocol type.

If the switch receives a 802.1 D BPDU after the port's migration-delay timer has been aborted, it assumes that it is connected to a 802.1 D switch and starts using the 802.1 D Protocol BPDU. However, if the RSTP switch is using 802.1 D BPDUs on a port, and receives an RSTP BPDU after the timer aborts, that port restarts the timer and begins using RSTP BPDUs.

9.1.10 Introduction to 802.1D Spanning Tree

The Spanning Tree Protocol is based on the following:

1) There is a unique group address (01-80-C2-00-00-00) that identifies all switches on a particular LAN. This group address is recognized by all switches;

2) Each switch has a unique identifier (Brideg Identifier);

3) Each switch port has a unique Port Identifier. Managing the configuration of the spanning tree also requires coordinating a relative priority for each switch, a relative priority for each port of each switch, and a path cost for each port.

The switch with the highest priority is called the root switch. Each switch port has a root path cost, which is the sum of the path costs from the switch to the network segments traversed by the root switch. The port with the lowest value of the root path cost in a switch is called the root port. If there are multiple ports with the same root path cost, the port with the highest priority is the root port.

In each LAN, there is one switch, called the designated switch, that belongs to the switch with the least cost for the root path in that LAN. The port that connects the LAN to the designated switch is the designated port of the LAN. If more than two ports in the designated switch are connected to this LAN, the port with the highest priority is selected as the designated port.

Elements of a decision necessary to form a spanning tree:

1) Decide on the root switch

a. Initially, all switches consider themselves to be the root switch;

b. Switches broadcast configuration BPDUs to the LANs to which they are connected, with the root _ ID and bridge _ ID \n The values are the same;

c. When a switch receives a configuration BPDU from another switch, if it finds the received configuration BPDU If the value of the root _ ID field in the is greater than the value of the root _ ID parameter in the switch, the frame is discarded, otherwise the values of the root _ ID, root _ path _ cost, and other parameters of the switch are updated, and the switch will continue to broadcast configuration BPDUs with the new values.

2) Determines the root port

a. The port in a switch that has the lowest root path cost is called the root port.

b. If there are multiple ports with the same lowest root cost, the port with the highest priority is the root Mouth. If there are two or more ports with the same lowest root cost and highest priority, the port with the lowest port number is the default root port.

3) Identify the designated switch for the LAN

a. Initially, all switches consider themselves designated switches for the LAN.

b. When a switch receives a message from another switch (in the same LAN) that has a lower root path cost BPDU, the switch no longer claims to be the designated switch. If there are two or more switches with the same root path cost in a LAN, the switch with the highest priority is selected as the designated switch.

c. If, at some point, that designate switch receives a call from other switch on the LAN due to competition for the designated switch The specified switch will send a configuration BPDU back to redetermine the specified switch.

4) Decide to assign a port

The port on the designated switch for the LAN that is connected to the LAN is the designated port. If a given switch has two or more ports connected to the LAN, the port with the lowest ID is the given port.

All ports except the root port and the designated port are placed in the blocking state. Thus, after determining the root switch, the root port of the switch, and the designated switch and designated port for each LAN, a spanning-tree topology is determined.

9.2 MSTP Configuration

9.2.1 Default configuration

Command parameter	Default Value
spanning-tree mst enable(Start mstp)	shut
Spanning-tree mst priority(Switch cist priority)	32768
spanning-tree mst hello-time(Switch cist hello-time)	2 seconds
spanning-tree mst forward-time(Switch cist forward-time)	15 seconds
spanning-tree mst max-age(Switch cist max-age)	20 seconds
spanning-tree mst max-hops(Switch cist max-hops)	20 seconds
instance 1 priority (Instance Priority)	32768
spanning-tree mst instance 1 priority(Port instance priority)	128
spanning-tree mst instance 1 path-cost(Port instance path-cost)	20000000
spanning-tree mst priority （Port cist priority）	128
spanning-tree mst path-cost（Port cist path-cost）	20000000

9.2.2 General configuration

Start MSTP

The system is configured with MSTP off by default at startup.

The configuration process to start MSTP is:

Switch#configure terminal

Switch(config)#spanning-tree mst enable

The command to turn off MSTP is:

Switch#configure terminal

Switch(config)#no spanning-tree mst

Configure max-age

The configuration max-age is the configuration for all instances, and the max-age is the number of seconds the switch waits to receive spanning-tree configuration information before triggering a reconfiguration.

The default configuration is 20 seconds, and the configuration range is 6 to 40 seconds.

：Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst max-age <seconds>

Configuration max-hops

Max-hops is the number of hops specified in a domain before a BPDU is dropped.

The default value is 20 and the configuration range is 1 to 40.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst max-hops <hop-count>

Configuration forward-time

Configuring forward-time is for all instances. Forward-time is the number of seconds the port waits from discarding to learning and from learning to forwarding.

The default configuration is 15 seconds, and the configuration range is 4 to 30 seconds. According to the generation number protocol, forward-time must satisfy the following condition: 2 * (forward-time – 1) > = max-age.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst forward-time <seconds>

Configuration hello-time

Configuring hello-time is the configuration for all instances. Hello-time is the interval between the generation of configuration information by the root switch.

The default configuration time is 2 seconds, and the configuration range is 1 to 10 seconds. According to the spanning tree protocol, hello-time must satisfy the following condition: 2 * (hello-time + 1) = < max-age.

Configuration process:

Switch#configure terminal

Switch(config)# spanning-tree mst hello-time <seconds>

Configure the priority of the CIST bridge

Default configuration 32768, configuration range < 0-61440 >; CIST priority value can only be a multiple of 4096.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst priority <priority>

Configuration and CISCO compatibility

The network switch adopts the MSTP protocol based on the 802.1 s, and the length of each MSTI message is 16 bytes, while the length of each MSTI message of the BPDU of the CISCO switch is 26 bytes. To interoperate with CISCO switches, enable CISCO-compatible switches when configuring the network's switches.

In the case of the startup and CISCO compatible configuration, when determining whether the domains are the same, the domains are considered to be the same as long as the domain name and the revision number are the same.

This feature is not enabled by default.

Open and CISCO compatible:

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability enable

Off and CISCO compatible:

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability disable

Reset Protocol Check Task

In order to be compatible with the 802.1D STP protocol, the system can automatically detect the protocol running on the other system. Fy determines the protocol running on this port based on the protocol running on the other side.

In some cases, the protocol is reset. For example, the system negotiates a port to run the STP protocol, and after a period of time, the device running the STP protocol of the other party has been replaced by a host. At this time, I need to configure the port as fast port, but the port has already run the STP protocol, and the protocol negotiation task has stopped. At this time, I need to reset the protocol negotiation task to renegotiate the protocol between it and the host.

Resets the protocol reconnaissance task for the entire device:

Switch#clear spanning-tree detected protocols

Reset the protocol reconnaissance task of a port:

Switch#clear spanning-tree detected protocols interface <if-name>

9.2.3 Domain Configuration

If two or more devices are in the same domain, they must have the same VLAN instance mapping, the same revision number, and the same domain name.

A domain has one or more members with the same MST configuration, each of which can handle the RSTP BPDUS capability. There is no limit on the number of members in a network, but each domain can support up to 16 instances.

The configuration of the instance is described in the'Instance Configuration '. Only the domain name configuration and the revision number configuration are described here.

Configure the domain name:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#region <region-name>

Configuration Revision Number:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)# revision <revision-num>

9.2.4 Instance Configuration

The system supports 16 instances with instance ID numbers ranging from 0 to 15. A VLAN can be assigned to only one spanning-tree instance at a time.

By default, there is only one instance, 0, to which all VLANs belong.

The process of configuring an instance:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> vlan <vlan-id>

Configure the priority of the MSTI bridge

Default configuration 32768, configuration range < 0-61440 >; the value of MSTI priority can only be a multiple of 4096.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> priority <priority>

9.2.5 Port configuration

The following describes the port configuration information related to MSTP. Only the simple configuration part is described here, and port fast and root guard are described separately later.

The process of configuring a port to join an instance:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id>

Configure the priority of the CIST port

The default configuration is 128, the configuration range is < 0-240 >, and the priority value of the CIST port can only be a multiple of 16.

Configuration process:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst priority <priority>

Configure the priority of the MSTI port

The default configuration is 128, and the configuration range is < 0-240 >. The priority value of the MSTI port can only be a multiple of 16.

Configuration process:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> priority <priority>

Configure path cost for CIST port

The default configuration is 20000000, and the configuration range is 1-200000000. The following is the bandwidth and path cost mapping table:

Broadband	Path Flower Elimination
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>1000000000000	2

Configuration process:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst path <path-cost>

Configure path-cost for MSTI port

The default configuration is 20000000, and the configuration range is 1-200000000. Bandwidth and path costs are the same as in the table above.

Configuration process:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> path-cost <path-cost>

Configure the version number of the sending protocol package

The default configuration sends the MSTP protocol packet, the configuration range is 0-3, and the mapping relationship is 0-stp, 2-rstp, and 3-mstp.

Configuration process:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)# spanning-tree mst force-version <version-id>

Configure Connection Type

If a port is connected to other ports in a point-to-point manner and the local port becomes a designated port, RSTP determines a loop-free topology by negotiating a quick migration of the port to which it is connected through the proposal-agreement process.

The following is a brief description of the negotiation process of the proposal-agreement.

When a switch receives a proposal message on one of its ports and that port is selected as the new root port, RSTP forces all other ports to synchronize the new root port information.

The switch is synchronized if all other ports are synchronized with the superior root information received from the root port.

When RSTP forces it to synchronize new root information, it moves to the blocking state if a designated port is in the forwarding state and is not configured as an edge port. Normally, when RSTP forces a port to synchronize new root messages and the port cannot meet the above conditions, the port state is set to blocking.

While ensuring that all ports are synchronized, the switch sends an agreement message to the root port corresponding to the designated port. When a switch is connected to a point-to-point connection in agreement with their port role, RSTP immediately migrates the port status to forwarding.

In the case of a shared connection, the state of the port is determined by an 802.1D calculation.

The default port connection type is point-to-point.

The connection type of the configuration port is a point-to-point connection:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst link-type point-to-point

The connection type of the configuration port is a shared connection:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config-ge1/2)#spanning-tree mst link-type shared

9.2.6 PORTFAST related configuration

1) Port Fast

Port Fast immediately transfers an access or trunk port from blocking to forwarding, bypassing listening and learning. You can use Port Fast to connect to a single workstation and server, allowing these devices to connect to the network immediately without waiting for the spanning tree to converge.

Configure one port as fast port:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast

2) BPDU Filtering

BPDU filtering can be turned on globally based on the switch or on a per-port basis, but their characteristics are different.

At the global level, you can use the spanning-tree MST portfast bpdu-filter command to enable BPDU filtering for ports in the portfast bpdu-filter default state.

At the port layer, you can turn on the BPDU filter on any port with spanning-tree MST portfast bpdu-filter enable.

This feature prevents the port fast port from receiving or sending BPDUs.

Configure BPDU Filtering

In global configuration mode:

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-filter

In interface configuration mode:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-filter enable

3) BPDU Guard

The BPDU protection feature can be turned on globally at the switch or on a per-port basis, but their characteristics are different.

At the global level, you can use spanning-tree MST portfast bpdu-guard to turn on BPDU guard for ports in the portfast bpdu-gurad default state.

At the port level, you can turn on BPDU guard on any port.

When the port on which the BPDU gurad is configured receives the BPDU, the spanning tree shuts down the port. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. BPDU guard enters an error-disabled state when a BPDU is received on a Port Fast-enabled port indicating an invalid configuration, such as the connection of an unauthorized device.

Error-disabled means that when the port that initiates the BPDU gurad receives the BPDU, the error-disable timer is initiated if the system is configured with the error-disable mechanism. Error-disable restarts the port after a system-configured timeout.

In global configuration mode:

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-guard

In interface configuration mode:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-guard enable

Configuration of error-disable

Start the error-disable mechanism

Switch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout enable

Configure the error-disable timeout

Switch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout interval <seconds>

9.2.7 Root Guard related configuration

An SP's Layer 2 network can contain many connections to switches that are not its own. In such a topology, the spanning tree can reconfigure itself and select a customer switch as the root switch. You can avoid this situation by configuring root guard on the SP switch's port that connects to the switch on the customer network. If the spanning tree calculation results in a port on the customer network being selected as the root port, the root guard configures the port to a root-inconsistent (blocked) state to prevent the customer switch from becoming the root switch or having a path to the root.

If a switch outside the SP network becomes the root switch, the port is blocked (root-inconsistent stat) and the spanning tree selects a new root switch. The customer's switch does not become the root switch and there is no path to the root.

If the switch is operating in MST mode, root guard forces the port to be a designated port. If a boundary port is blocked because of root guard in the IST instance, the port is blocked in all MST instances. A boundary port is a port that is connected to a LAN. The designated switch is either a 802.1 D switch or a switch with a different MST domain configuration.

Root guard apply to all VLANs to which a port belong when that port is turned on. VLANs can be aggregated and mapped to an MST instance.

Configuration process:
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst guard root

9.3 MSTP Configuration Example

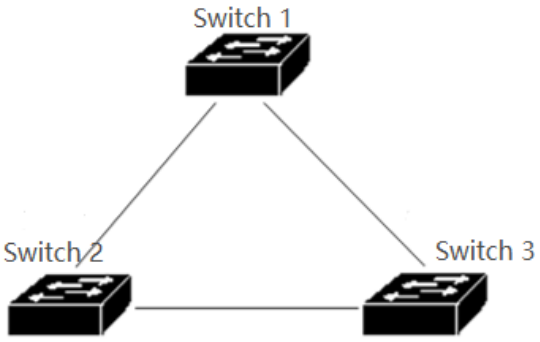
(1) Configuration:

Three switches are connected in a ring, and the spanning tree protocol of each switch needs to be turned on to avoid loops. Perform the configuration on each switch individually.

Switch 1 Configuration:
Switch>en
Switch#configure terminal
Switch(config)#spanning mst enable

Switch 2 Configuration:
Switch>en
Switch#configure terminal
Switch(config)#spanning mst enable

Switch 3 Configuration:
Switch>en
Switch#configure terminal
Switch(config)#spanning mst enable



(2) Debugging:

To see which switch is selected as the root bridge:
Execute the show spanning-tree MST, and observe that the value of CIST Root is the lowest MAC address of the three switches, that is, the root election result is correct.
Switch#show spanning-tree mst

To view the port status of a switch in the spanning tree:
Execute the show spanning-tree MST interface ge1/1 instruction to observe the State value of PORT ge1/1 in instance 0
Switch#show spanning-tree mst interface ge1/1

10. Configuring EAPS

This chapter describes EAPS and its configuration, mainly including the following contents：

- EAPS introduction
- EAPS Basic concepts
- EAPS Protocol introduction
- EAPS configuration
- Restrictions
- Configuration example

10.1 EAPS introduction

EAPS is the abbreviation of Ethernet automatic protection switching. EAPS uses standard Ethernet and VLAN technology to provide loop topology and loop recovery mechanism. In case of failure in the ring, EAPS has the ability to resume data communication within 1 second. The number of nodes running in EAPS is not limited, and the recovery time of EAPS is not limited. EAPS does not rely on other devices, that is, there can be devices in the EAPS ring that do not support EAPS protocol.

10.2 EAPS Basic concepts

Here are some basic concepts involved in EAPS:

1. EAPS domain: in a network, an EAPS domain runs in a separate ring. It is a series of node devices that form a separate loop. An EAPS domain includes a master node and one or more transit nodes.

2. A master node is a switch running EAPS or an EAPS node device. An EAPS domain has only one master node.

3. Transit node, a switch running EAPS or an EAPS node device, is a node other than the master node in an EAPS domain.

4. Primary port: the port connecting EAPS node devices in an EAPS domain. A node device has and only one primary port in an EAPS domain connected to this ring.

5. Secondary port: a port connecting EAPS node devices in an EAPS domain. A node device has only one secondary port in an EAPS domain connected to this ring.

6. Control VLAN, control VLAN, VLAN responsible for EAPS domain protocol packet transmission. There is only one control VLAN in an EAPS domain.

7. Protected VLAN, protected VLAN, VLAN that transmits business data in EAPS domain. There must be one protected VLAN or more than one protected VLAN in an EAPS domain.

10.3 EAPS Protocol introduction

An EAPS domain runs on an EAPS ring. An EAPS domain contains a master node and one or more transit nodes; Each EAPS node contains one same control VLAN and multiple protected VLAN; Each EAPS node contains a primary port and a secondary port in an EAPS domain. These two ports belong to the control VLAN and all protected VLANS of this ring. Connect all nodes in the EAPS domain through the primary port and secondary port of each EAPS node device to form an EAPS ring.

Under normal circumstances, when all primary ports and secondary ports in the EAPS domain are linked up, block the secondary port of the master node (set the port state of the secondary port to blocking) and eliminate the loop of business data in the EAPS domain. When the EAPS domain fails, immediately open the secondary port of the master node (set the state of the secondary port to forwarding), allow it to forward business data and restore the normal forwarding of business data.

The transit node has no difference in the processing of primary port and secondary port
The following describes two kinds of fault checking and loop recovery of EAPS：

10.3.1 Link-Down Give an alarm

When the transit node finds that its primary port or secondary port has link down, it will immediately send a link-down protocol package from the control VLAN to the master node through another link up port.

When the master node receives the link-down protocol package:

The master node immediately enters the failed state from the complete state, opens the secondary port (set the state of the secondary port to forwarding), refreshes its layer 2 and 3 forwarding, sends a ring-down-flush-fdb to notify EAPS domain of other transits, refreshes its forwarding table, and re learns the layer 2 and 3 forwarding.

When the master node finds that the local primary port has link down, its operation is the same as that of receiving the link-down protocol package.

When the master node finds that the local secondary port has a link down, the master node immediately enters the failed state from the complete state, refreshes its layer 2 and layer 3 forwarding, sends the ring-down-flush-fdb protocol package, and notifies EAPS domain of other transits to refresh its forwarding table and re learn the layer 2 and layer 3 forwarding。

10.3.2 Loop check

The master node will regularly send the health protocol package from the primary port. If the ring is complete, the master node can receive the health protocol package at its secondary port. At this time, the master node will restart its fail period timer, and the state of the master node is complete.

If the health protocol package is not received before the expiration of the fail period, the master node will leave the complete state, enter the failed state, open the secondary port (set the state of the secondary port to forwarding), refresh its layer 2 and layer 3 forwarding, send ring-dsown-flush-fdb to notify EAPS domain of other transits, refresh its forwarding table, and relearn the layer 2 and layer 3 forwarding.

10.3.3 Ring recovery

The master node will send the health protocol package from its primary port no matter whether the ring is complete or failed or otherwise. When the master node is in the failed state, once the health protocol packet is received from its secondary port, the ring will return to the complete state. At this time, the master node will set the state of the secondary port to blocking, refresh its layer 2 and 3 forwarding, and send a ring-up-flush-fdb package to notify other devices to refresh their layer 2 and 3 forwarding and relearn the layer 2 and 3 forwarding.

When the port of the transit node returns from link down to link up and the master node finds that the ring is restored, the secondary port of the master node may still be in the forwarding state. In this case, a temporary ring will be caused. Therefore, when one port of the transit node is in the link up state and the other port of the link down becomes link up, the transit node will enter a "pre forwarding state". In this state, the port of the subsequent link up will also be in the pre forwarding state, which cannot forward business data and interrupt the possible data loop. When the master node recovers and sends the ring-up-flush-fdb, the transit node will switch the node state to the link-up state after receiving the protocol packet, set the port in the pre forwarding state to the forwarding state, and resume the normal forwarding of business data.

If the transit node cannot receive the ring-up-flush-fdb protocol packet, it will set the port in pre forwarding status to forwarding status after double the fail time.

10.3.4 EAPS compatible with extreme

The products of extreme company are the first manufacturers to support EAPS, and the EAPS protocol supported by the switch follows the standard of rfc3619; There are some differences between the EAPS protocol package of extreme device and the protocol package definition of rfc3619. The EAPS protocol supported by the switch is fully compatible with the extreme device, and the compatibility switch is on by default.

10.3.5 More EAPS Domain

The switch can support multiple EAPS domains, a total of 16.

10.4 EAPS configuration

The basic configuration of EAPS protocol includes the following basic elements: control VLAN, node mode, primary port, secondary port, protected VLAN, hello time and fail time. Hello time and fail time are configured by default. Hello time is 1 second and fail timer is 3 seconds.

10.5 Restrictions

1. The primary port must belong to the control VLAN of an EAPS domain and the trunk mode member of all protected VLANs.

2. EAPS protocol cannot run simultaneously with MSTP protocol. If MSTP is started or MSTP instance is configured, EAPS protocol cannot be started.

3. When a VLAN starts the vllp protocol, it cannot be configured as the control VLAN or protected VLAN of EAPS

4. The control VLAN of EAPS can only contain primary port and secondary port, and can only be the trunk mode of VLAN

5. If a VLAN is configured as the control VLAN of EAPS domain and the domain has been started, the VLAN cannot be deleted, and its port members cannot be modified or deleted. Control VLAN cannot be configured with layer 3 interfaces.

6. Primary port and secondary port in protected VLAN can only be trunk mode. Other member ports are not limited.

7. One port can only be configured as the primary port or secondary port of one EAPS domain.

8. The same VLAN can only belong to the control VLAN or protected VLAN of one EAPS domain.

9. The control VLAN of all nodes in an EAPS domain must be the same.

10.6 EAPS Brief introduction of command

To create an EAPS domain, first ensure that the VLAN and port configurations meet the above conditions.

There are certain sequence requirements for configuring EAPS. First, create an EAPS domain. Before starting the EAPS domain, configure other parameters according to the previous requirements; Otherwise, the startup will not succeed. If you want to change Hello time to a value greater than the current fail time, first change the fail time to a larger number; Otherwise, the configuration will not succeed. There are no special requirements for other configuration sequences.

When an EAPS domain has been started, the control VLAN, mode, primary port and secondary port cannot be modified; Protected VLAN, fail timer, hello time, and extreme interoperability can be modified.

The primary port and secondary port support LACP ports (i.e. trunk groups).

10.6.1 EAPS Configuration command

Command	Description	Mode
EAPS create <ring-id>	Create an EAPS domain	Global configuration mode
EAPS control-vlan <ring-id> <vlan-id>	Configure a control VLAN of EAPS domain.	Global configuration mode
EAPS protected-vlan <ring-id> <vlan-id>	Add a protected VLAN of EAPS domain.	Global configuration mode
EAPS mode <ring-id> <master|transit>	Configure the running node mode of an EAPS domain.	Global configuration mode
EAPS primary-port <ring-id> <ifname>	Configure the primary port of an EAPS domain.	Global configuration mode
EAPS secondary-port <ring-id> <ifname>	Configure a secondary port of EAPS domain.	Global configuration mode
EAPS data-span <ring-id>	Configure EAPS ring data cross ring forwarding	Global configuration mode
EAPS fail-time <ring-id> <secs>	Configure the timeout time of the fail period timer of an EAPS domain. The default is 3 seconds. The unit is seconds.	Global configuration mode
EAPS hello-time <ring-id> <secs>	Configure the time when an EAPS domain sends health packets regularly. The default is 1 second. The unit is seconds. Hello timer must be less than fail time.	Global configuration mode
EAPS extreme-interoperability <ring-id> <enable|disable>	Enable or disable compatibility with extreme devices. The default is startup compatibility.	Global configuration mode
EAPS enable <ring-id>	Start an EAPS domain	Global configuration mode
EAPS disable <ring-id>	Close an EAPS domain	Global configuration mode
show EAPS	Displays the information of EAPS domain started in the system	Normal mode / privileged mode
Show EAPS <ring-id>	Displays the details of an EAPSdomain	Normal mode / privileged mode

10.7 Single ring configuration example

There are three switches, Switch1, switch2 and switch3. VLAN 1 will not form a loop during traffic forwarding through EAPS protocol. At the same time, it is guaranteed to enable the standby link when one link between Switch1, switch2 and switch3 is disconnected. According to the above requirements, Switch1 can be configured as master mode; Configure switch2 and switch3 to transit mode. Add a control VLAN VLAN 2 for protocol packet transmission.

Switch1 configuration:

Switch1 is configured as the master of EAPS domain ring 1. The control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary port is GE1 / 1, and the secondary port is GE1 / 2. Other configurations adopt default values.

Switch#configure terminal
#Add VLANs 2 and 3
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-3
Switch(config-vlan)#exit

#Configure GE1 / 1 as a trunk member of VLAN 1 and VLAN 2。
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk native vlan 3
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#Configure GE1 / 2 as a trunk member of VLAN 1 and VLAN 2。
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk native vlan 3
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan

VLAN Name	State	Member ports ([u]-Untagged, [t]-Tagged)
VLAN 1	Active	[t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10 [u]ge1/11 [u]ge1/12
VLAN 2	Active	[t]ge1/1 [t]ge1/2
VLAN 3	Active	[u]ge1/1 [u]ge1/2

Switch#configure terminal
 # Create an EAPS Domain ring 1
Switch(config)#EAPS create 1

#Configure VLAN 2 as the control VLAN
Switch(config)#EAPS control-vlan 1 2

#Configure VLAN 1 as a protected VLAN
Switch(config)#EAPS protected-vlan 1 1

#Configure Switch1 as the master node
Switch(config)#EAPS mode 1 master

#Configure GE1 / 1 as primary port
Switch(config)#EAPS primary-port 1 ge1/1

#Configure GE1 / 2 as secondary -port
Switch(config)#EAPS secondary-port 1 ge1/2

#start-upEAPS Domain ring 1
Switch(config)#EAPS enable 1

Switch2 Configuration

Switch2 is configured as the transport of EAPS domain ring 1, the control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary port is GE1 / 1, the secondary port is GE1 / 2, and other configurations adopt default values.

Switch#configure terminal
#Add VLANs 2 and 3
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-3
Switch(config-vlan)#exit

#Configure GE1 / 1 as a trunk member of VLAN 1 and VLAN 2。
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk native vlan 3
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#Configure GE1 / 2 as a trunk member of VLAN 1 and VLAN 2。
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk native vlan 3
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan

VLAN	Name	State	Member ports ([u]-Untagged, [t]-Tagged)
1	vlan1	active	[t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
2	vlan2	active	[t]ge1/1 [t]ge1/2
3	vlan3	active	[u]ge1/1 [u]ge1/2

Switch#configure terminal
#Create an EAPS domain ring 1
Switch(config)#EAPS create
#Configure VLAN 2 as the control VLAN
Switch(config)#EAPS control-vlan 1 2
#Configure VLAN 1 as a protected VLAN

Switch(config)#EAPS protected-vlan 1
#Configure switch as a transit node
Switch(config)#EAPS mode 1 transit
#Configure GE1 / 1 as primary port
Switch(config)#EAPS primary-port 1 ge1/1
#Configure GE1 / 2 as secondary port
Switch(config)#EAPS secondary-port 1 ge1/2
#Start EAPS domain ring 1
Switch(config)#EAPS enable 1

Configuration of switch3

Switch3 is configured as the transport of EAPS domain ring 1, the control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary port is GE1 / 1, the secondary port is GE1 / 2, and other configurations adopt default values.

Switch#configure terminal

 # Add VLANs 2 and 3
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-3
Switch(config-vlan)#exit

 # Configure GE1 / 1 as a trunk member of VLAN 1 and VLAN 2。
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk native vlan 3
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

 # Configure GE1 / 2 as a trunk member of VLAN 1 and VLAN 2。
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk native vlan 3
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2
Switch(config-ge1/2)#exit
Switch(config)#exit

Switch#show vlan

VLAN Name	State	Member ports ([u]-Untagged, [t]-Tagged)
VLAN 1	Active	[t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10 [u]ge1/11 [u]ge1/12
VLAN 2	Active	[t]ge1/1 [t]ge1/2
VLAN 3	Active	[u]ge1/1 [u]ge1/2

Switch#configure terminal
#Create an EAPS domain ring 1
Switch(config)#EAPS create 1
#Configure VLAN 2 as the control VLAN
Switch(config)#EAPS control-vlan 1
#Configure VLAN 1 as a protected VLAN

Switch(config)#EAPS protected-vlan 1 1
#Configure switch3 as a transit node
Switch(config)#EAPS mode 1 transit

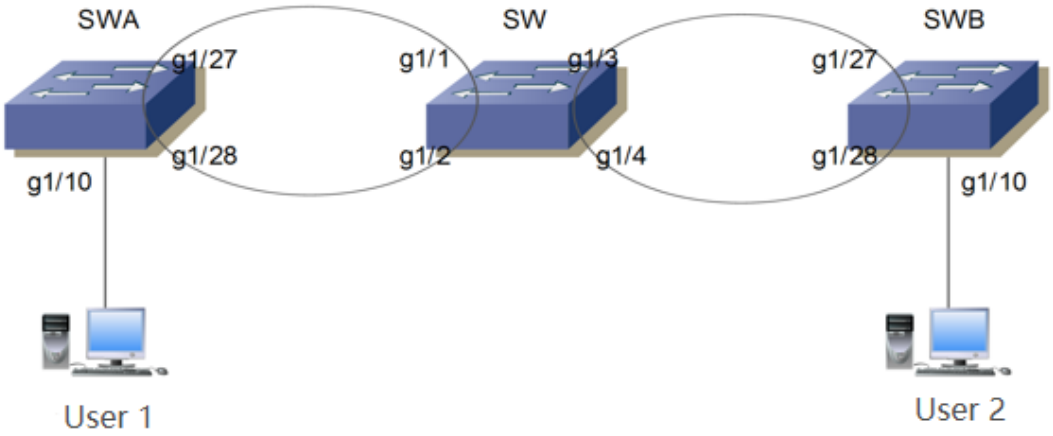
#Configure GE1 / 1 as primary portSwitch(config)#EAPS primary-port 1 ge1/1

#Configure GE1 / 2 secondary -port
Switch(config)#EAPS secondary-port 1 ge1/2

#start-upEAPS Domain ring 1
Switch(config)#EAPS enable 1

10.8 Cross ring data forwarding configuration example

There are three switches SWA, SW and SWB, which realize vlan1 and vlan2 interworking across the ring through EAPS protocol. The topology is as follows：



SWA ring 1 controls VLAN 111 and protects VLAN 1 and 2. The configuration is as follows：
vlan database
vlan 2
vlan 111

interface ge1/10
switchport access vlan 2
interface ge1/27
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111

interface ge1/28
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111
EAPS create 1
EAPS mode 1 Transit
EAPS primary-port 1 ge1/27
EAPS secondary-port 1 ge1/28
EAPS control-vlan 1 111
EAPS protected-vlan 1 1
EAPS protected-vlan 1 2
EAPS enable 1

SW ring 1 is connected with SWA to control VLAN 111 and protect VLAN 1 and 2. Ring 2 connects with SWB, controls VLAN 222 and protects VLAN 3333 (virtual VLAN, and the interface needs to be added). If you want to realize the cross ring forwarding of ring 1 and ring 2 data, you need to configure the command EAPS data span. The configuration is as follows：

vlan database
vlan 2
vlan 111
vlan 222
vlan 3333

interface ge1/1
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111
interface ge1/2
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111

interface ge1/3
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222
switchport trunk allowed vlan add 3333 ###Add virtual vlan 3333

interface ge1/4
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222
switchport trunk allowed vlan add 3333 ###Add virtual vlan 3333

EAPS create 1
EAPS mode 1 Master
EAPS primary-port 1 ge1/1
EAPS secondary-port 1 ge1/2
EAPS control-vlan 1 111
EAPS protected-vlan 1 1
EAPS protected-vlan 1 2
EAPS data-span 1
EAPS enable 1

EAPS create 2
EAPS mode 2 Transit
EAPS primary-port 2 ge1/3
EAPS secondary-port 2 ge1/4
EAPS control-vlan 2 222
EAPS protected-vlan 2 3333 ###Here is virtual protection vlan
EAPS data-span 2
EAPS enable 2

SWB ring 2 is connected with SW ring 2 to control VLAN 222 and protect VLAN 1 and 2. The configuration is as follows :

vlan database
vlan 2
vlan 222

interface ge1/10
switchport access vlan 2

interface ge1/27
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222

interface ge1/28
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222

EAPS create 2
EAPS mode 2 Master
EAPS primary-port 2 ge1/27
EAPS secondary-port 2 ge1/28
EAPS control-vlan 2 222
EAPS protected-vlan 2 1
EAPS protected-vlan 2 2
EAPS enable 2

After vlan1 and vlan2 are configured to communicate with each other. EAPS node mode can be modified as required

11. Configuring ERPS

11.1 ERPS Overview

ERPS (Ethernet Ring Protection Switching) is a ring protection protocol developed by ITU, also known as G.8032. It is a link layer protocol specifically for Ethernet ring networks. It can prevent the broadcast storm caused by the data loop when the Ethernet ring network is complete, and can quickly restore the communication between the nodes on the ring network when one link on the Ethernet ring network is broken. ERPS protocol provides a fast Ethernet ring network protection mechanism, which can quickly restore network transmission when the ring network fails, so as to ensure the high availability and reliability of the switch in the case of ring network topology.

11.2 Introduction to ERPS Technology

11.2.1 ERPS ring

The ERPS ring is based on the principle of minimizing the ring, and each ring must be the smallest ring, which is divided into a main ring and a sub-ring: the main ring is a closed ring; the sub-ring is an unclosed ring or a closed ring; all of which need to be configured by a command.

Each ERPS ring (whether the main ring or the sub-ring) has five States: (1) Idle state: the state when each physical link in the ring network is connected; (2) Protection state: the state when one or more physical links in the ring network are disconnected; (3) Manual switch state: the state of the ring is manually changed; (4) Forced switch state: forced to change the state of the ring; (5) Pending state: pending intermediate state.

11.2.2 ERPS Node

The Layer 2 switching devices that join the ERPS ring are called nodes. No more than two ports of each node can join the same ERPS ring, one port is an RPL port and the other port is a normal ring port.

Globally, the roles of nodes are divided into the following two types: (1) Intersecting nodes: In an intersecting ERPS ring, nodes that belong to multiple rings at the same time are called intersecting nodes; (2) Non-intersecting nodes: In an intersecting ERPS ring, nodes that belong to only one ERPS ring are called non-intersecting nodes.

The node modes specified in ERPS protocol mainly include RPL owner node, RPL neighbour node and ordinary ring node.

(1) RPL owner node: There is only one RPL owner node in an ERPS ring, which is determined by user configuration. The RPL port is blocked to prevent the generation of loops in the ERPS ring. When the RPL owner node receives a failure message and learns that other nodes or links on the ERPS ring fail, it will automatically release the RPL port. This port resumes the receiving and sending of traffic to ensure that the traffic is not interrupted;

(2) RPL neighbour node:A node that is directly connected to the RPL port of the RPL owner node. Normally, both the RPL port of the RPL owner node and the RPL port of the RPL neighbour node are blocked to prevent loops. When the ERPS ring fails, both the RPL port of the RPL owner node and the RPL port of the RPL neighbour node are released;

(3) ordinary ring nodes: in the ERPS ring, all nodes except the RPL owner node and the RPL neighbour node are ordinary ring nodes, the RPL ports of the ordinary ring nodes are not different from the ordinary ring ports, and the ring ports of the ordinary ring nodes are responsible for monitoring the link state of the ERPS protocol directly connected with the ordinary ring nodes, And inform other nodes of the change message of the link state in time;

11.2.3 Link and channel

(1)RPL (Ring Protection Link): Each ERPS ring has only one RPL, that is, the link where the RPL port of the RPL owner node is located. When the Ethernet ring is in the Idle state, the RPL link is in the blocking state and does not forward the data packet to avoid the formation of a loop;

(2) subring link: a link belonging to a subring and controlled by the subring in an intersecting ring;

(3) RAPS (Ring Auto Protection Switch) virtual channel: In an intersecting ring, the path between intersecting nodes, which is used to transmit sub-ring protocol messages but does not belong to the sub-ring, is called the RAPS virtual channel of the sub-ring.

11.2.4 ERPS VLAN

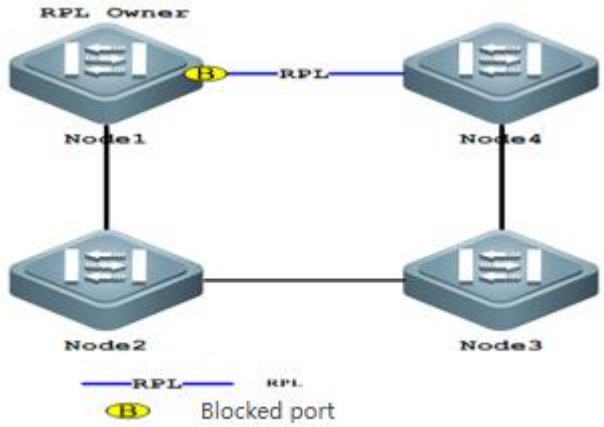
There are two types of VLANs in ERPS:

(1) RAPS VLAN: It is used to transmit ERPS protocol messages. All the ports on the device that access the ERPS ring belong to the RAPS VLAN, and only the ports that access the ERP ring can join this VLAN. RAPS VLANs must be different for different rings. IP address is not allowed to be configured on the interface of RAPS VLAN;

(2) Data VLAN: As opposed to the RAPS VLAN, the data VLAN is used to transmit data packets. The data VLAN can include both ERP ring ports and non-ERP ring ports.

11.3 ERPS operating principle

11.3.1 Normal State

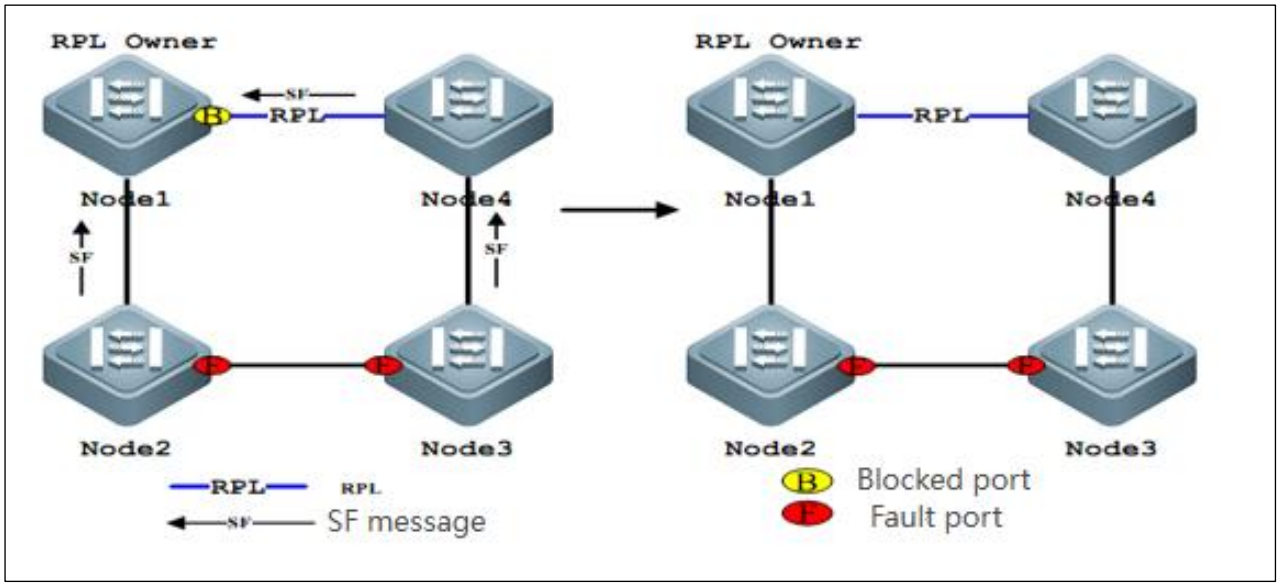


(1) All nodes are connected in a physical topology in a ring manner;

(2) The loop protection protocol ensures that no loop is formed by blocking the RPL link. As shown in the figure above, the link between Node1 and Node4 is a RPL link;

(3)Performing fault detection on each link between adjacent nodes.

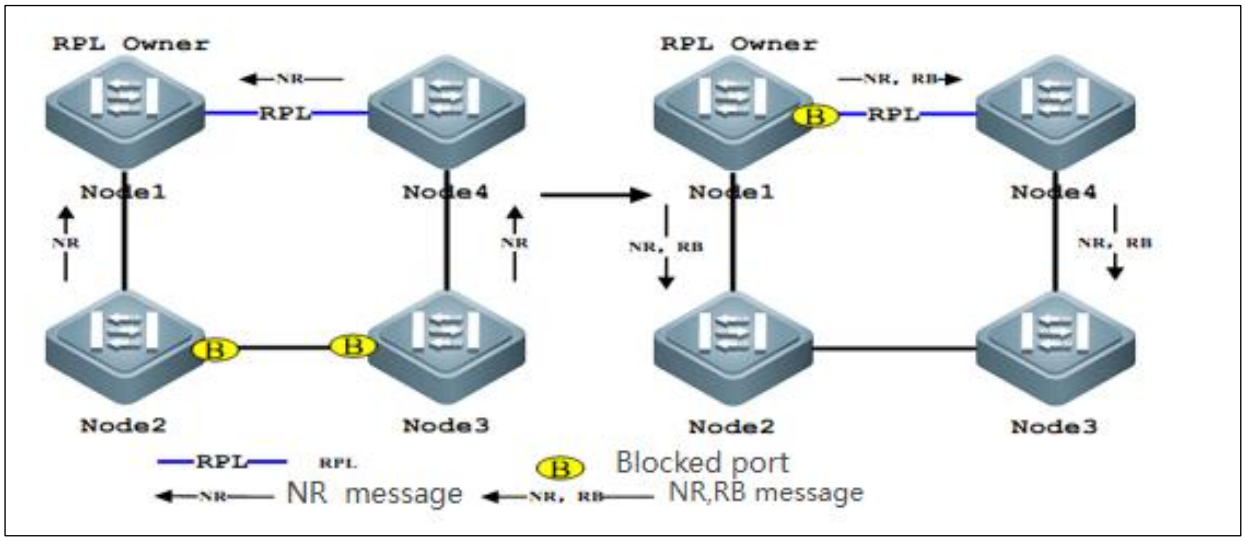
11.3.2 Link failure



(1) The node adjacent to the failed link blocks the failed link and reports the failure to other nodes on the ring by using the RAPS (SF) message, as shown in the figure above. Suppose that the link between Node2 and Node3 fails, Node2 and Node3 will block the failed link after waiting for the holdoff timer to expire. Respectively sending a RAPS (SF) message to each node on the ring network;

(2) The RAPS (SF) message triggers the RPL owning node to open the RPL port. The RAPS (SF) message also triggers all nodes to update their respective MAC entries, and then the nodes enter the protection state.

11.3.3 Link Recovery



(1)when the fault is recovered, the adjacent node of the fault continues to maintain the blocking state and sends a RAPS (NR) message indicating that there is no local fault;

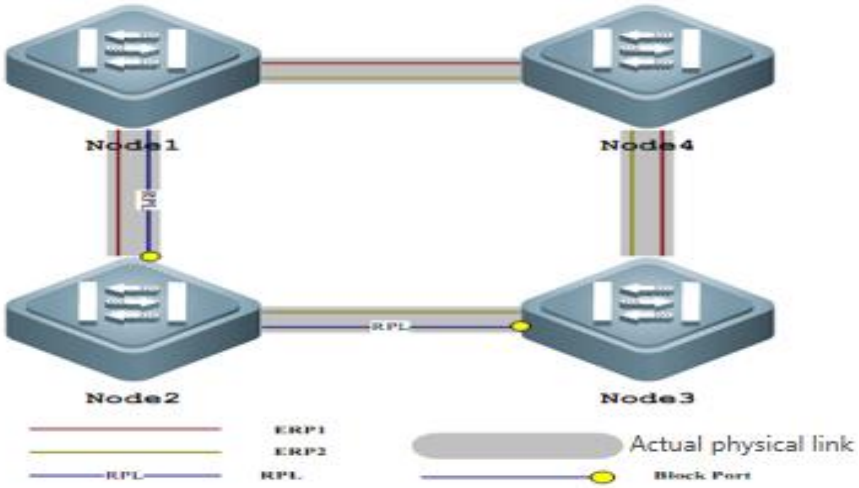
(2)after the guard timer is exhausted, the RPL Owner node starts the WTR timer after receiving the first RAPS (NR) message;

(3)when the WTR timer is exhausted, the RPL Owner node blocks the RPL and sends a RAPS (NR, RB) message;

(4)aft receiving that message, other node update respective MAC table entries, and the node sending the RAPS (NR) message stops periodically sen the message and opens the originally blocked port. The ring network has returned to its original normal state.

11.4 Technical features of ERPS

11.4.1 ERPS Load Balancing

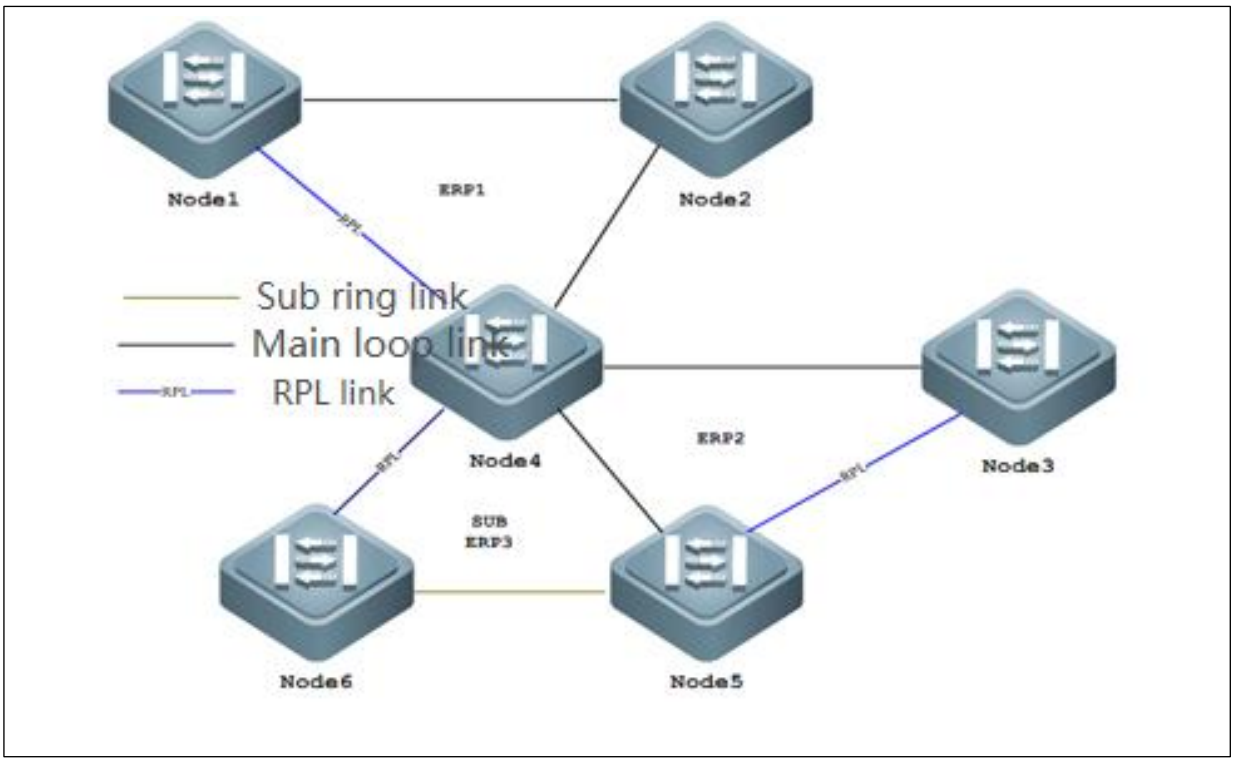


A plurality of instance and a plurality of ERPS rings are configure on that same physical ring network, and different ERPS rings send the traffic of different VLANs (refer to as protection VLANs), so that the topology of the data traffic of different VLANs in the ring network is different, and the purpose of load sharing is achieved. As shown in the figure above, one physical ring network corresponds to two instances and two ERPS rings. The VLANs protected by the two ERPS rings are different. Node2 is the RPL owner node of ERP 1, and Node3 is the RPL owner node of ERP 2. Through configuration, different VLANs can block different links respectively, so as to realize the load sharing of a single ring.

11.4.2 Good safety

. There are two types of VLANs in ERPS, one is the RAPS VLAN and the other is the data VLAN. The RAPS VLAN is only used to transmit the protocol message of the ERPS, and the ERPS only processes the protocol message from the RAPS VLAN, and does not process any protocol attack message from the data VLAN, so as to improve the security of the ERPS.

11.4.3 Support multi-loop intersection tangency



As shown in the figure above, ERPS supports joining multiple rings at the same node (Node4) in the form of tangency or intersection, which greatly increases the flexibility of networking.

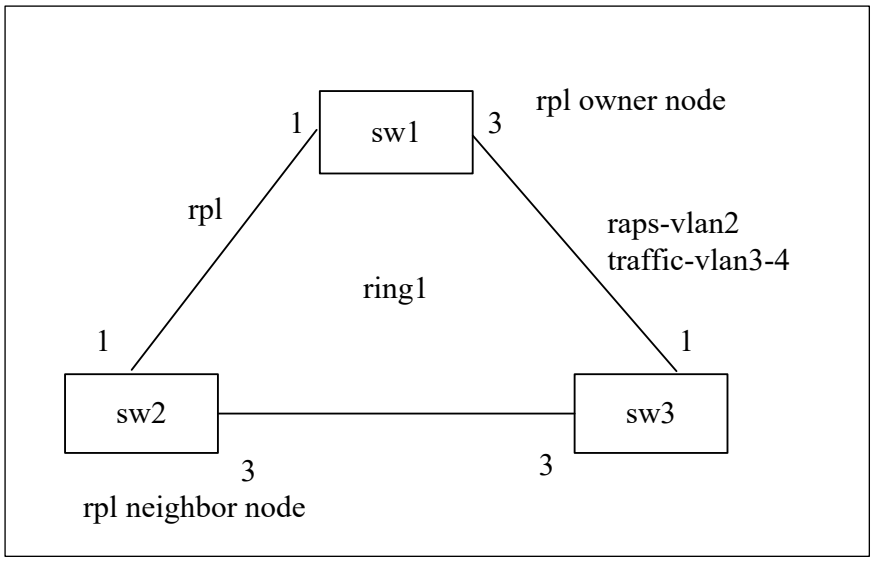
11.5 ERPS protocol command

Command	Description	CLI Mode
erps predefine configuration (ring-node | rpl-owner-node)	Enable ERPS predefined configuration	Global Configuration Mode
no erps predefine configuration	Disable ERPS predefined configuration	Global Configuration Mode
erps <1-8>	Create an ERPS instances	Global Configuration Mode
no erps <1-8>	Delete an ERPS instance	Global Configuration Mode
node-role (interconnection | none-interconnection)	Configure the role of the node in the ERPS r ing, interlink or non-interlink	ERPS mode
ring <1-32>	Create an ERPS ring	ERPS mode
no ring <1-32>	Delete an ERPS ring	ERPS mode
ring <1-32> ring-mode (major-ring | sub-ring)	Configure ERPS ring mode, primary or subring	ERPS mode
ring <1-32> node-mode (rpl-owner-node | rpl-neighbour -node | ring-node)	Configure the ERPS ring node mode, RPL owner node, RPL neighbour node, or normal ring nod	ERPS mode
ring <1-32> raps-vlan <2-4094>	Configure the ERPS ring protocol VLAN	ERPS mode
no ring <1-32> raps-vlan	Deleting an ERPS Ring Protocol VLAN	ERPS mode
ring <1-32> traffic-vlan <1-4094>	Configuring the ERPS Ring Data VLAN	ERPS mode
no ring <1-32> traffic-vlan <1-4094>	Deleting the ERPS Ring Data VLAN	ERPS mode
ring <1-32> (rpl-port|rl-port) IFNAME	Configure ERPS ring port, RPL port, or normal ring port	ERPS mode
no ring <1-32> (rpl-port|rl-port)	Configure ERPS ring port, RPL port, or normal ring port	ERPS mode
ring <1-32> revertive-behaviour (revertive|non-revertive)	Configure the ERPS ring recovery behavior, recoverable or non-recoverable	ERPS mode
ring <1-32> hold-off-time <0-10000>	Configure ERPS ring hold-off times	ERPS mode
no ring <1-32> hold-off-time	Resume ERPS ring hold-off default times	ERPS mode
ring <1-32> guard-time <10-2000>	Configure ERPS loop guard times	ERPS mode
no ring <1-32> guard-time	Restore default time for ERPS loop	ERPS mode
ring <1-32> wtr-time <1-12>	Configuring the ERPS Ring wtr Time	ERPS mode
no ring <1-32> wtr-time	Restore ERPS Ring wtr Default Time	ERPS mode
ring <1-32> wtb-time <1-10>	Configure ERPS ring WTB times	ERPS mode
no ring <1-32> wtb-time	Restore ERPS ring WTB default times	ERPS mode
ring <1-32> raps-send-time <1-10>	Configure sending time of ERPS ring protocol message	ERPS mode
no ring <1-32> raps-send-time	Restore the default sending time of ERPS ring protocol message	ERPS mode
ring <1-32> (enable|disable)	Turn the ERPS ring on or off	ERPS mode
ring <1-32> forced-switch IFNAME	Forced-switch ERPS ring port	ERPS mode
ring <1-32> clear forced-switch	Clear Forced Switchover of ERPS Ring	ERPS mode
ring <1-32> manual-switch IFNAME	Manually switch ERPS ring port	ERPS mode
ring <1-32> clear manual-switch	Manual switching to clear the ERPS ring	ERPS mode
ring <1-32> clear recovery	Manual recovery when unrecoverable behaviour of ERPS ring is cleared or manual recovery before WTR/WTB expires	ERPS mode
show erps	Displays a summary of all ERPS instances and rings for the device	Privileged mode
show erps <1-8>	Displays the details of a single ERPS instance and ring for a device	Privileged mode

11.6 ERPS Typical Application

11.6.1 Single Ring Example

As shown in the figure below, sw1, sw2 and sw3 nodes form an ERPs single ring ring1, ports 1 and 3 of each node are used as ERPs ring ports, the protocol VLAN of the ring is 2, the data VLANs are 3 and 4, the sw1 node is the RPL owner node, and the sw2 node is the RPL neighbour node. The link between sw1 and sw2 is an RPL link



(1) Configure SW 1:

Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

(2) Configure SW 2:

Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbour -node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 rpl-port ge1/1

Switch(config-erps-1)# ring 1 rl-port ge1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

(3) Configure SW 3:

Switch>enable

Switch#configure terminal

Create ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk allowed vlan add 2

Switch(config-ge1/1)# switchport trunk allowed vlan add 3

Switch(config-ge1/1)# switchport trunk allowed vlan add 4

Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3

Switch(config-ge1/3)# switchport mode trunk

Switch(config-ge1/3)# switchport trunk allowed vlan add 2

Switch(config-ge1/3)# switchport trunk allowed vlan add 3

Switch(config-ge1/3)# switchport trunk allowed vlan add 4

Switch(config-ge1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode ring-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 1

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 rpl-port ge1/1

Switch(config-erps-1)# ring 1 rl-port ge1/3

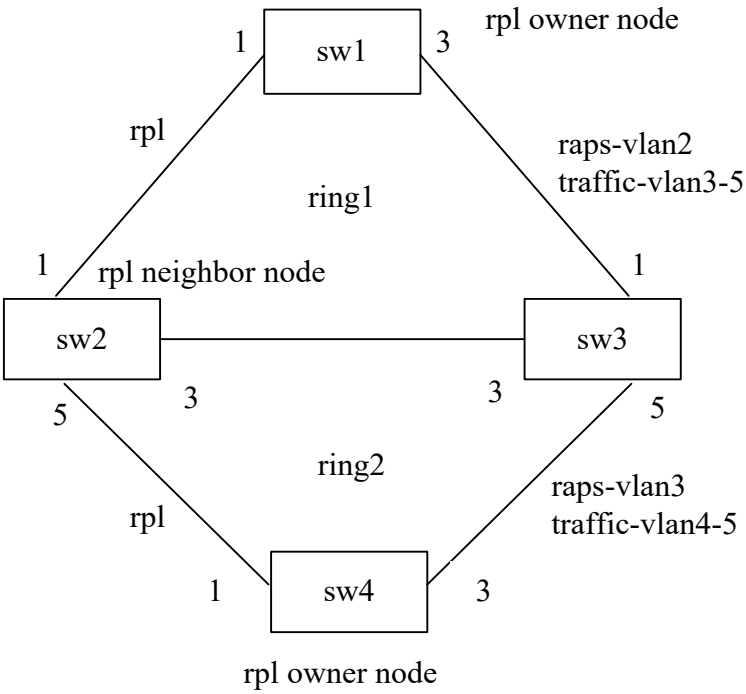
Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

11.6.2 Multi-loop examples

As shown in the figure below, the nodes sw1, sw2 and sw3 form an ERPs main ring ring1, the ports 1 and 3 of the nodes sw1, sw2 and sw3 serve as the ring ports of the main ring ring1, the protocol VLAN of the main ring ring1 is 2, and the data VLANs are 3, 4 and 5. The sw1 node is the main ring ring1 RPL owner node, the sw2 node is the main ring ring1 RPL neighbour node, and the link between sw1 and sw2 is the main ring ring1 RPL link.

The nodes sw2, sw3 and sw4 form an ERPs subring ring2, the 5 ports of the nodes sw2 and sw3 and the 1 and 3 ports of the node sw4 are used as the ring ports of the subring ring2, the protocol VLAN of the subring ring2 is 3, and the data VLANs are 4 and 5. The sw4 node is the subring ring2 RPL owner node, and the link between sw2 and sw4 is the subring ring2 RPL link.



(1) Configure SW 1:

Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit

Configure ERPs instance 1, ERPs primary ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

(2) Configure SW 2:
Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit

Switch(config)# interface ge1/5
Switch(config-ge1/5)# switchport mode trunk
Switch(config-ge1/5)# switchport trunk allowed vlan add 3
Switch(config-ge1/5)# switchport trunk allowed vlan add 4
Switch(config-ge1/5)# switchport trunk allowed vlan add 5
Switch(config-ge1/5)#exit

Configure ERPs instance 1, ERPs primary ring 1, subring 2

Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbour -node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit

(3) Configure SW 3:
Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3

```
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit

Switch(config)# interface ge1/5
Switch(config-ge1/5)# switchport mode trunk
Switch(config-ge1/5)# switchport trunk allowed vlan add 3
Switch(config-ge1/5)# switchport trunk allowed vlan add 4
Switch(config-ge1/5)# switchport trunk allowed vlan add 5
Switch(config-ge1/5)#exit
```

Configure ERPs instance 1, ERPs primary ring 1, subring 2

```
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

(4) Configure SW 4:

```
Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 3-5
Switch(config-vlan)#exit
```

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit

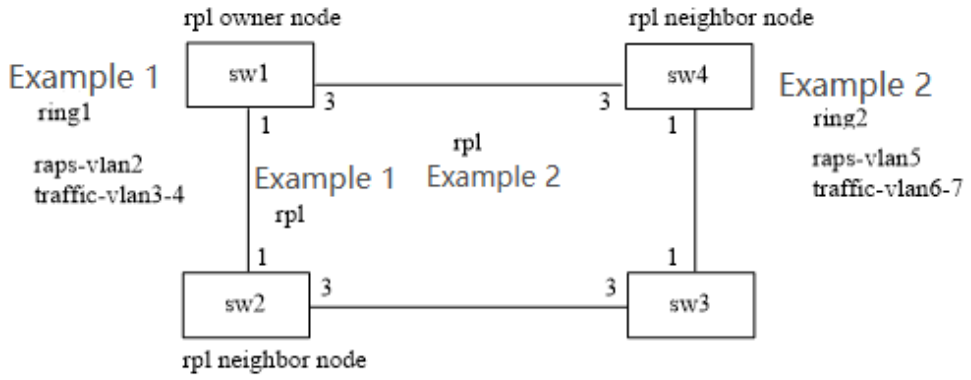
Configure ERPs instance 1, ERPs subring 2

Switch(config)#erps 1
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode rpl-owner-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 1
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/1
Switch(config-erps-1)# ring 2 rl-port ge1/3
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit

11.6.3 Multi-Instance Load Balancing Example

As shown in the figure below, the nodes sw1, sw2, sw3 and sw4 form a single ring 1 of the ERPs instance 1, the ports 1 and 3 of each node are used as the ERPs ring ports, the protocol VLAN of the ring is 2, the data VLANs are 3 and 4, the node sw1 is the RPL owner node, and the node sw2 is the RPL neighbour node. The link between sw1 and sw2 is an RPL link.

The node sw1, sw2, sw3 and sw4 form a single ring 2 of that ERPs instance 2, the port 1 and 3 of each node are used as the ports of the ERPs ring, the protocol VLAN of the re is 5, the data VLANs are 6 and 7, the node sw1 is the RPL owner node, the node sw4 is the RPL neighbour node, The link between sw1 and sw4 is an RPL link.



(1) Configuration example 1:

Configure SW 1:

Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

Configure SW 2:

Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2

Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit

Configure ERPs instance 1, ERPs single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbour -node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

Configure SW 3:
Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure ERPs instance 1, ERPs single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

Configure SW 4:
Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit

Configure ERPs instance 1, ERPs single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

(2) Configuration example 2:

Configure SW 1:

Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add the ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit

Configure ERPs instance 2, ERPs single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-owner-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/3
Switch(config-erps-2)# ring 2 rl-port ge1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit

Configure SW 2:

```
Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
```

Configure the VLAN mode of the ring port as trunk, the ERPs protocol and data VLAN

```
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
```

Configure ERPs instance 2, ERPs single ring 2

```
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/1
Switch(config-erps-2)# ring 2 rl-port ge1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

Configure SW 3:

```
Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
```

Configure the VLAN mode of the ring port as trunk, adding the ERPs protocol and data VLAN

```
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
```

Configure ERPs instance 2, ERPs single ring 2

```
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/1
Switch(config-erps-2)# ring 2 rl-port ge1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

Configure SW 4:

```
Switch>enable
Switch#configure terminal
Create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, adding the ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit

Configure ERPs instance 2, ERPs single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-neighbour -node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/3
Switch(config-erps-2)# ring 2 rl-port ge1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

12. Configure AAA

This chapter describes how to configure the switch 802.1 X and RADIUS to prevent unauthorized users from accessing the network. For the use of the 802.1 X Client and HyperBoss, refer to the respective instruction manuals. This chapter mainly includes the following contents:

- 802.1x Introduction
- RADIUS Introduction
- Configuring 802.1x
- Configure RADIUS

AAA stands for Authentication, Authorisation, and Accounting. It provides a consistent framework for configuring authentication, authorization, and accounting security functions. The configuration of AAA is actually a kind of management of network security, and network security here mainly refers to access control. Including which users can access the network? What services are available to users with access? How do I account for users who are using network resources?

- **Authentication:** Verifies whether the user can gain access.
- **Authorisation:** What services are available to authorized users.
- **Accounting**: Record the use of network resources by users.

Network companies have launched a set of AAA solutions, including 802.1 X clients, various switches supporting authentication and HyperBoss authentication and accounting system. The 802.1 X client is installed on the PC of the user. When the user needs to access the network, he needs to use the 802.1 X client for authentication. Only the authenticated user can use the network. It receives the authentication request from the client and transmits the user name and password to the authentication and accounting system HyperBoss. The switch itself does not do the actual authentication work. HyperBoss receives the authentication request sent by the switch to perform actual authentication, and performs billing processing on the user who is successfully authenticated.

The 802.1x protocol is used to communicate between the 802.1x client and the switch, and the RADIUS protocol is used to communicate between the switch and HyperBoss.

12.1 802.1x Introduction

The 802.1 X protocol is an access control and authentication protocol based on a port, and the port here refers to a logical port, which may be a physical port, a MAC address, or a Vlan ID, etc. The switches of the network implement the 802.1 X protocol based on the MAC address.

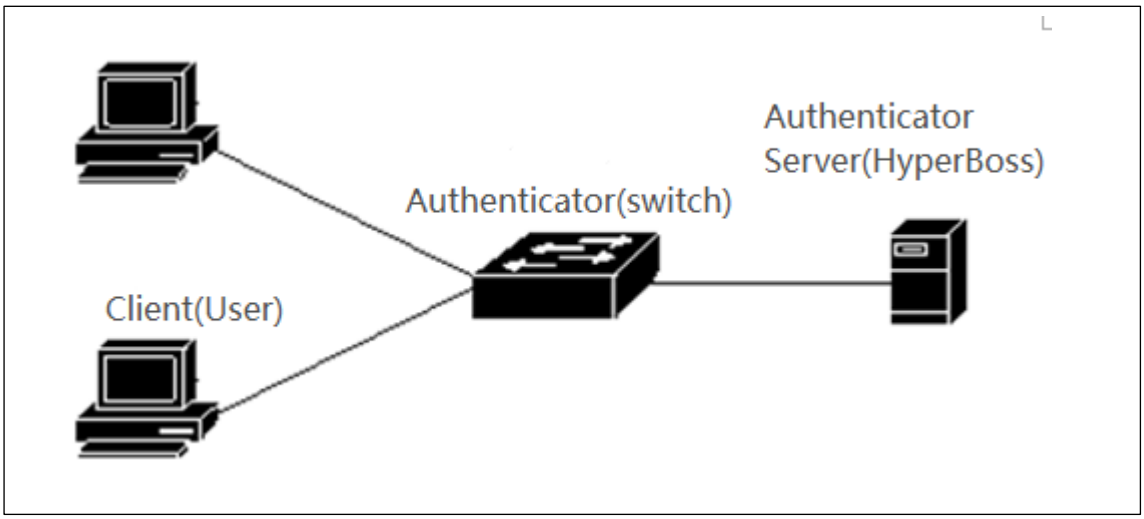
The 802.1 X is a layer 2 protocol. The authenticated switch and the user's PC must be in the same subnet, and the protocol packet cannot cross the network segment. 802.1 X authentication uses a client-server model, and there must be a server to authenticate all users. Before the user passes the authentication, only the authentication flow can pass through the port of the switch. After the authentication is successful, the data flow can pass through the port of the switch. That is to say, the user must pass the authentication before accessing the network.

This section mainly includes the following contents:

- 802.1x device composition
- Introduction to Protocol Package
- Protocol flow interaction
- 802.1x Port Status

12.1.1 802.1x device composition

An 802.1x device consists of three parts: a client (Supplicant System), an authentication system (Authenticator System), and an authentication server (Authentication Server System). As shown in the following figure.



802.1x device

The client refers to the device that requests to access the network, generally the user terminal system, such as the user's PC. A 802.1 X client software must be installed on the user terminal system, which implements the client part of the 802.1 X protocol. The client initiates a 802.1 X authentication request to request the authentication server to authenticate its user name and password. If the authentication is successful, the user can access the network.

An authentication system refers to an authenticated device, such as a switch. The authentication system controls whether the user can access the network through the status of the logical port (referring to the MAC address) of the user. If the status of the logical port of the user is unauthorized, the user cannot access the network. If the status of the logical port of the user is authorized, the user can access the network.

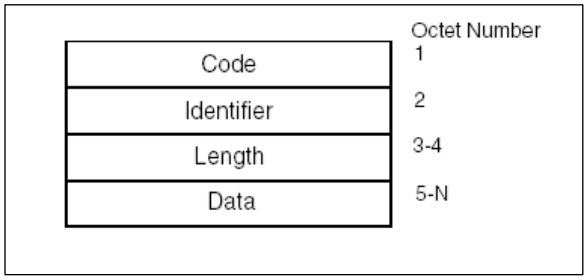
The authentication system is a relay between the client and the authentication server. The authentication system requests the identity information of the user, forwards the identity information of the user to the authentication server, and forwards the authentication result sent by the authentication server to the client. The authentication system needs to realize the server part of the 802.1 X protocol at a terminal close to a user and needs to realize the client part of the RADIUS protocol at a terminal close to the authentication server, the RADIUS protocol client of the authentication system packages the EAP information sent by the 802.1 X client in the RADIUS and sends the information to the authentication server, And the EAP information is decapsulated from the RAIDUS protocol packet sent by the authentication server and transmitted to the 802.1 X client through the 802.1 X server part.

The authentication server refers to the device that actually authenticates the user. The authentication server receives the identity information of the user sent by the authentication system and verifies it. If the authentication is successful, the authentication server authorizes the authentication system and allows the user to access the network. If the authentication fails, the authentication server tells the authentication system that the user authentication fails and the user cannot access the network. The authentication server communicates with the authentication system through the RADIUS protocol extended by EAP. The network provides an authentication and accounting system HyperBoss to authenticate and account for users.

12.1.2 Introduction to Protocol Package

The authentication data stream transmitted by the 802.1 X protocol on the network is in the format of an EAPOL (EAP Over LAN) frame, all user identity information (including a user name and a password) is encapsulated in an EAP (Extensible Authentication Protocol), and the EAP is further encapsulated in an EAP frame. The user name exists in the EAP as clear text, and the password exists in the EAP as MD5 encryption.

The EAPol frame format is shown in the following figure. The PAE Ethernet Type is the Ethernet protocol type model for EAPOL, with a value of 0x888E. Protocol Version is the EAPOL version number, with a value of 1. Packet Type refers to the EAPol frame type. Packet Body Length is the length of the EAPOL frame content. Packet Body refers to the contents of the EAPol frame.



EAPol frame format

The switch uses three types of EAPOL protocol frames:

EAPOL-Start: When the value of Packet Type is 1, the authentication initiates the frame. When the user needs to be authenticated, this frame is first initiated and sent by the client to the switch.

EAPOL-Logoff: The value of Packet Type is 2. The exit request frame is sent to notify the switch when the user does not need to use the network.

EAP-Packet: The value of Packet Type is 0. The authentication information frame is used to carry authentication information.

The format of the EAP packet is shown in the following figure. Code refers to the type of EAP package, including Request, Response, Success, and Failure. Identifier refers to an identifier, which is used to match Response and Request. Length refers to the length of the EAP packet, including the header. Data refers to EAP package data.

EAP packets include the following four types:

a. **EAP-The value of Request:** Code is 1. The EAP request packet is sent from the switch to the client to request the username and/or password.

b. **EAP-Response**: The value of Code is 2. The EAP response packet is sent from the client to the switch, and the username and/or password are sent to the switch.

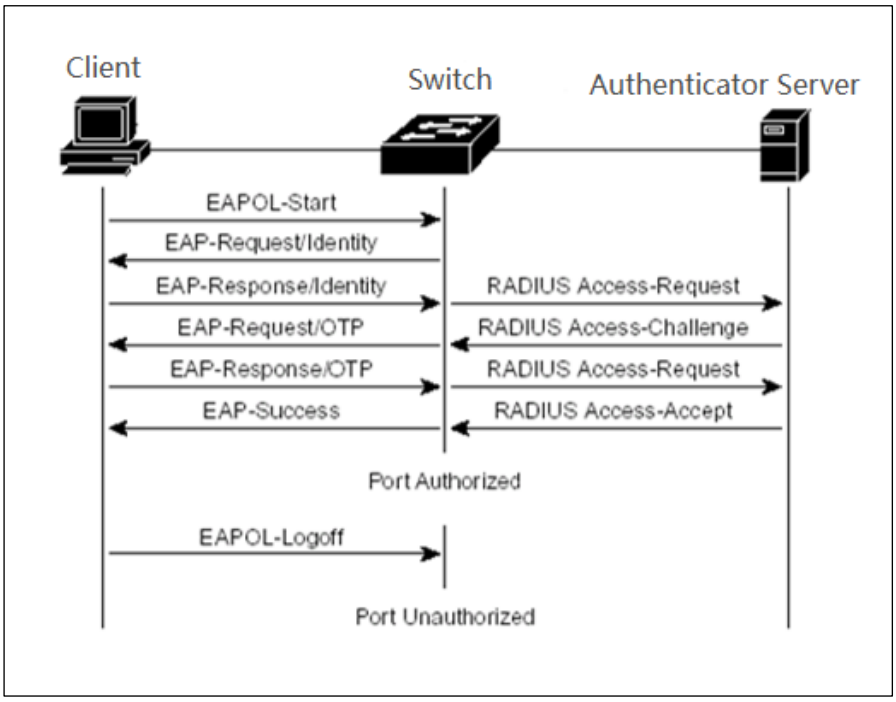
c. **EAP-The Success:** Code value is 3. The EAP success packet is sent from the switch to the client to inform the client that the user authentication is successful.

d. EAP-The value of Failure: Code is 4. The EAP failure packet is sent from the switch to the client to inform the client that the user authentication has failed.

EAP packet format

12.1.3 Protocol flow interaction

When 802.1x is enabled on the switch and the status of the port is Auto, all users accessing the port must be authenticated before they can access the network. The protocol interaction is shown in the figure below.

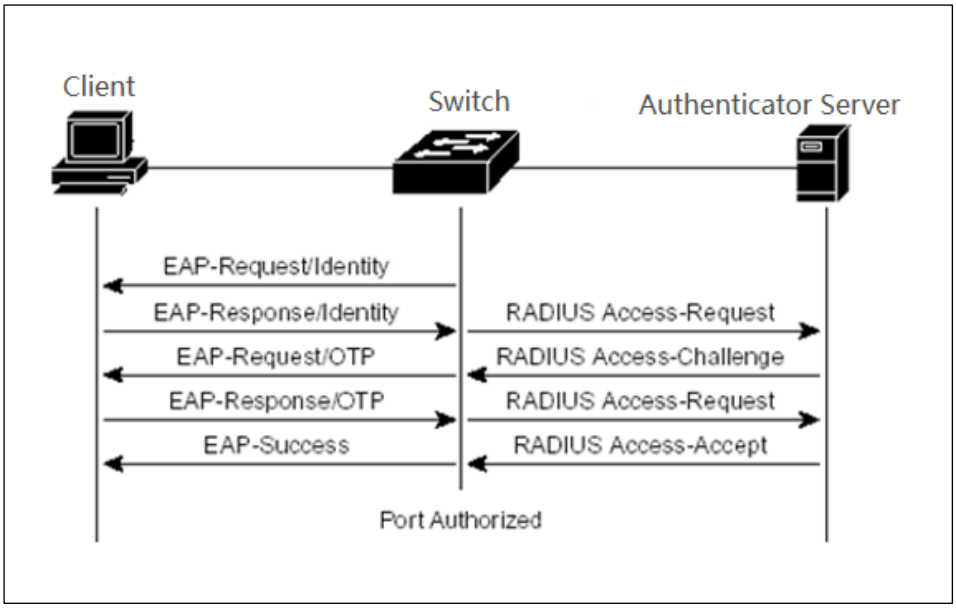


Client initiates authenticated protocol interaction

When a user needs to access the network, the client first sends an EAPOL-Start to the switch to request authentication, the switch sends an EAP-Request to request the username of the user after receiving the authentication request, the client returns an EAP-Response, the switch extracts the EAP information and encapsulates the EAP information in a RADIUS packet to send the EAP information to the authentication server, The authentication server requests the user's password, and the switch sends an EAP-Request to the client requesting the user's password.The client sends back an EAP-Response, the switch encapsulates the EAP information in a RADIUS packet and sends it to the authentication server, and the authentication server authenticates the user according to the user name and password. If the authentication is successful, the authentication server notifies the switch, and the switch sends EAP-Success to the client and places the user's logical port in an authorized state. When the client receives EAP-Success, it indicates that the authentication is successful and the user can access the network.

When the user no longer needs to use the network, the client sends the EAPOL-Logoff to the switch, and the switch changes the logical port state of the user to the unauthorized state, and the user cannot access the network at this time.

In order to prevent the client from going offline abnormally, the switch provides a re-authentication mechanism. The time interval for re-authentication can be set on the switch. When the authentication time is up, the switch initiates re-authentication. If the authentication is successful, the user can continue to use the network. If the authentication fails, the user cannot use the network. The protocol interaction is shown in the figure below.



Protocol Interaction for Recertification

12.1.4 802.1x Port Status

The port state referred to here is the physical port state of the switch. A physical port on a switch has four States: N/a, Auto, Force-authorized, and Force-unauthorized. When the switch does not open 802.1 X, all ports are in the N/A state. When a switch port is to be set to the Auto state, the Force-authorized state, or the Force-unauthorized state, the switch 802.1 X must be enabled.

When the port of the switch is in the N/A state, all users under the port can access the network without authentication. When the switch receives 802.1 X protocol packets from the port, it discards them.

When a port on a switch is in the Force-authorized state, all users under the port can access the network without authentication. When the switch receives an EAPOL-Start packet from the port, the switch sends back an EAP-Success packet, and when the switch receives other 802.1 X protocol packets from the port, the switch discards these protocol packets.

When the port of the switch is in the Force-unauthorized state, all users under the port cannot access the network all the time, and the authentication request can never pass. When the switch receives 802.1 X protocol packets from the port, it discards them.

When the port of the switch is in the Auto state, all users under the port must be authenticated before accessing the network. The 802.1 X protocol interaction is shown in the figure. If the user needs to be authenticated, the port is generally set to the Auto state.

When the switch port is set to the Auto state, the anti-ARP spoofing function is also enabled; The anti-ARP spoofing function can control that only the data packet of which the source MAC and source IP of the IP packet conform to the information provided by the client when being authenticated and the data packet of which the sender IP and sender MAC of the ARP packet conform to the information provided by the client when being authenticated can be forwarded by the port, otherwise, the data packet can be discarded. When configuring this function, the client must have a statically configured IP address. If the IP address is obtained dynamically through the DHCP protocol, the DHCP SNOOPING protocol can be enabled to realize this function. If you need a more detailed introduction, please refer to the IP MAC binding configuration.

12.2 RADIUS Introduction

When the user is authenticated, the RADIUS protocol supporting EAP extension is used for interaction between the switch and the authentication server. The RADIUS protocol uses the client/server model, the switch needs to implement the RADIUS client, and the authentication server needs to implement the RADIUS server.

In order to ensure the security of the interaction between the switch and the authentication server and prevent the interaction between illegal switches or illegal authentication servers, the switch and the authentication server should authenticate each other. The switch and the authentication server need the same key; when the switch or the authentication server sends a RADIUS protocol packet, all protocol packets generate a message digest by adopting an HMAC algorithm according to the key; when the switch and the authentication server receive the RADIUS protocol packet, the message digests of all protocol packets are verified by using the key; if the verification is passed, It is considered to be a legal RADIUS protocol packet, otherwise, it is an illegal RADIUS protocol packet and is discarded.

This section mainly includes the following contents:

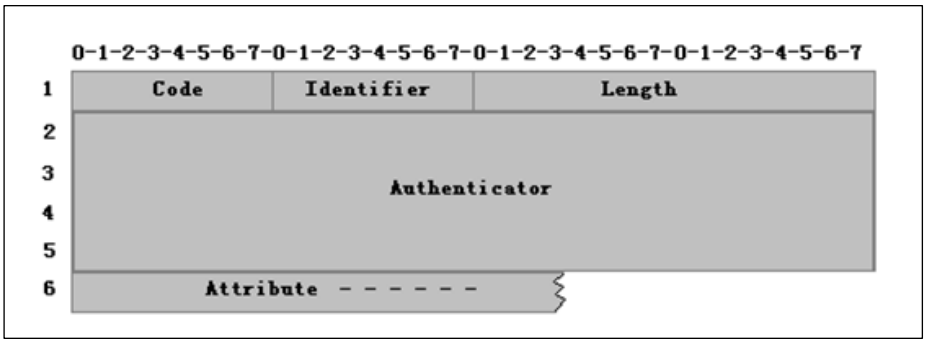
- Introduction to Protocol Package
- Protocol flow interaction
- User authentication method

12.2.1 Introduction to Protocol Package

RADIUS is a protocol based on UDP. RADIUS can encapsulate authentication information and accounting information. The early RADIUS authentication port was 1645 and currently uses port 1812. The early RADIUS billing port was 1646 and currently uses port 1813.

Because RADIUS is carried over UDP, RADIUS requires a timeout retransmission mechanism. At the same time, in order to improve the reliability of the communication between the authentication system and the RADIUS server, two RADIUS servers are generally used, that is, the standby server mechanism is used.

The format of RADIUS message is shown in the figure below. Code refers to RADIUS protocol message type. Identifier, which is used to match requests and replies. Length refers to the length of the whole message (including the message header). Authenticator is a 16-byte string, a random number for a request packet, and an MD5-generated message digest for a reply packet. Attribute refers to an attribute in the RADIUS package.



RADIUS message format

The network uses the following RADIUS protocol packages:

a. **Access-Request:** The value of Code is 1. It is an authentication request packet sent from the authentication system to the authentication server. The user name and password are encapsulated in this packet.

b. **Access-Accept:** The value of Code is 2. The response packet sent from the authentication server to the authentication system indicates that the user authentication is successful.

c. **Access-The value of Reject:** Code is 3. It is a response packet sent from the authentication server to the authentication system, indicating that the user authentication has failed.

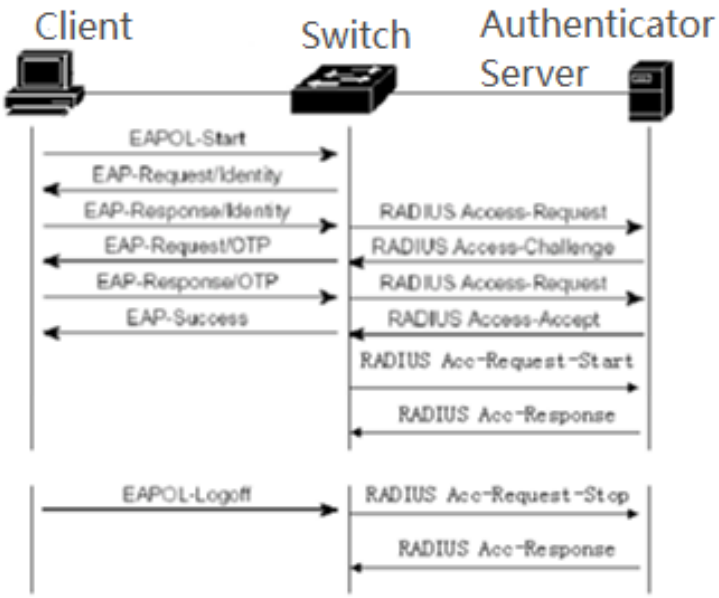
d. **Access-Challenge**: Code value 11, a response packet sent from the authentication server to the authentication system, indicating that the authentication server requires further information from the user, such as a password.

e. **Accounting-Request:** The value of Code is 4. The accounting request packet sent from the authentication system to the authentication server includes the start accounting packet and the end accounting packet. The accounting information is encapsulated in this packet.

f. **Accounting-Response**: a charging response packet sent from the authentication server to the authentication system when the value of the Code is 5, indicating that the charging information has been received.

12.2.2 Protocol flow interaction

When the user initiates authentication, the authentication system interacts with the authentication server through the RADIUS protocol. The protocol flow interaction in which the authentication system does not send RADIUS billing packets is shown in the following figure. In general, after the user is successfully authenticated or when the user is offline, the authentication system needs to send a RADIUS billing packet to the authentication server. The protocol flow interaction is shown in the following figure.



When a user is authenticated, the switch encapsulates the user name in an Access-Request message and sends the Access-Request message to the authentication server, the server responds to the password of the Access-Challenge request user, the switch requests the password of the client user, and the client encapsulates the password in the EAP. After acquiring the EAP, the switch encapsulates the EAP in an Access-Request and sends the Access-Request to an authentication server, the authentication server authenticates the user, if the authentication is successful, an Access-Accept is returned to the switch, and the switch notifies the client that the authentication is successful after receiving the message. At the same time, the Accounting-Request is sent to notify the authentication server to start charging, and the authentication server returns the Accounting-Response.

When the user does not want to use the network, the switch is notified that the user is offline, the switch sends an Accounting-Request to notify the authentication server to end the accounting, the accounting information is encapsulated in the packet, and the authentication server returns an Accounting-Response.

12.2.3 User authentication method

RADIUS has three methods of user authentication, as follows:

- **PAP**（Password Authentication Protocol）The user passes the username and his password to the switch in clear text. The switch passes the user name and password to the RADIUS server through the RADIUS protocol packet. The RADIUS server searches the database. If there is the same user name and password, it indicates that the authentication is passed. Otherwise, it indicates that the authentication is not passed.
- **CHAP**（Challenge Handshake Authentication Protocol）When a user requests to access the Internet, the switch generates a 16-byte random code to the user. The user encrypts the random code, password, and other fields to generate a response, and transmits the user name and response to the switch. The switch passes the username, response, and the original 16-byte random code to the RADIUS server. The RADIU searches the database at the switch side according to the user name to obtain the same password used for encryption at the user side, then encrypts the password according to the transmitted 16-byte random code, and compares the result with the transmitted response. If they are the same, it indicates that the authentication is passed, and if they are not the same, it indicates that the authentication is failed.
- **EAP**（Extensible Authentication Protocol）With this authentication method, the switch does not really participate in the authentication, but only plays the role of forwarding between the user and the RADIUS server. When the user requests to access the network, the switch requests the user name of the user and transfers the user name to the RADIUS server. The RADIUS server generates a random code of 16 bytes for the user and stores the random code.The user encrypts the random code, password, and other fields to generate a response, transmits the user name and response to the switch, and the switch forwards the response to the RADIUS server. The RADIU searches the database at the switch side according to the user name to obtain the same password as that used for encryption at the user side, and then encrypts the password according to the stored 16-byte random code, and compares the result with the transmitted response. If they are the same, it indicates that the authentication is passed, and if they are not the same, it indicates that the authentication is failed. The authentication and accounting solution of the network adopts the EAP user authentication method.

12.3 Configuring 802.1x

This section describes the 802.1x configuration in detail, mainly including the following contents:

- 802.1x Default Configuration
- Turning 802.1x On and Off
- Configure 802.1x port state
- Configure the recertification mechanism
- Configure the maximum number of hosts connected to the port
- Configure the interval time and number of retransmissions
- Configure the port as a transmit port
- Configure 802.1x client version number
- Configure whether to check client version number
- Configure authentication method
- Configure whether to check the timing packet of the client
- Displaying 802.1x information

12.3.1 802.1x Default Configuration

The switch 802.1x configuration defaults as follows:

- 802.1x is off.
- The state of all ports is N/A.
- The recertification mechanism is off and the recertification interval is 3600 seconds.
- The maximum number of access hosts for all ports is 100.
- The timeout interval for resending an EAP-Request is 30 seconds.
- The number of times the EAP-Request is retransmitted after timeout is 3.
- The waiting time for user authentication failure is 60 seconds.
- The timeout retransmission interval of the server is 10 seconds.

The switch provides a command in global CONFIG mode to return all configurations to the default state, as follows:

Switch(config)#dot1x default

12.3.2 Turning 802.1x On and Off

The first step in configuring 802.1x is to enable 802.1x. In global CONFIG mode, enter the following command to enable 802.1x:

Switch(config)#dot1x

When 802.1x is turned off, all ports return to the N/A state. Turn off 802.1x by entering the following command in global CONFIG mode:

Switch(config)#no dot1x

12.3.3 Configure 802.1x port state

Be sure to enable 802.1x before setting the 802.1x port status. If all users under the port must be authenticated before accessing the network, the port must be set to Auto status.

The following command sets port ge1/1 to the Auto state in interface configuration mode and enables anti-ARP spoofing:

Switch(config-ge1/1)dot1x control auto

If the anti-ARP spoofing configuration fails, it may be caused by the following reasons:

1) System CFP resources are exhausted.
2) The current interface is configured with ACL filtering.
3) The current interface has the DHCP SNOOPING feature enabled.
4) The interface being configured is either a Layer 3 interface or a trunk interface.

The following command sets port ge1/1 to the Force-authorized state in interface configuration mode:

Switch(config-ge1/1)dot1x control force-authorized

The following command sets port ge1/1 to the Force-unauthorized state in interface configuration mode:

Switch(config-ge1/1)dot1x control force-unauthorized

The following command sets port ge1/1 to the N/A state in interface configuration mode:

Switch(config-ge1/1)no dot1x control

Note: If a port is bound with a MAC address, the port cannot be set to Auto, Force-authorized, or Force-unauthorized.

12.3.4 Configure the recertification mechanism

In order to prevent the switch and the authentication server from being unable to detect the abnormal offline of the client, the switch provides a re-authentication mechanism, and the switch initiates an authentication every re-authentication interval.

The following command starts the recertification mechanism in global CONFIG mode:

Switch(config)#dot1x reauthenticate

The following command turns off the recertification mechanism in global CONFIG mode:
Switch(config)#no dot1x reauthenticate

The following command sets the recertification interval in global CONFIG mode:

Switch(config)#dot1x timeout re-authperiod <interval>
Note: Do not set the recertification interval too short, otherwise the network bandwidth and the CPU resources of the switch will be consumed too much.

12.3.5 Configure the maximum number of hosts connected to the port

Each port of the switch can control the maximum number of hosts accessed. This function can restrict users from using multiple hosts to access the network illegally. The maximum number of hosts connected to the port is 100 by default, and the maximum number can be set to 100. If the maximum number of hosts accessing a port is set to 0, the port denies any user access.

The following command sets the maximum number of hosts on port ge1/1 in interface configuration mode:

Switch(config-ge1/1)dot1x support-host <number>

12.3.6 Configure the interval time and number of retransmission

The 802.1 X protocol standard specifies some interval times and retransmission times of the protocol interaction and the protocol state machine. The switch uses the standard interval times and retransmission times. It is recommended that the user does not change these interval times or retransmission times when using the switch.

Tx-period represents the interval time for the switch to resend the EAP-Request protocol packet; max-req represents the number of times the switch resends the EAP-Request; quiet-period represents the interval time for waiting for re-authentication when the user authentication fails; Server-timeout

indicates the interval for the switch to retransmit the RADIUS packet to the authentication server; supp-timeout indicates the interval for the switch to retransmit the EAP request packet to the client.

The following command configures these intervals and retransmissions in global CONFIG mode:

Switch(config)#dot1x timeout tx-period <interval>

Switch(config)#dot1x max-req <number>

Switch(config)#dot1x timeout quiet-period <interval>

Switch(config)#dot1x timeout server-timeout <interval>

Switch(config)#dot1x timeout supp-timeout <interval>

12.3.7 Configure the port as a transmit port

When the switch does not enable the 802.1 X authentication, but other switches in the subnet enable the 802.1 X authentication, the port of the switch connecting the client and the authentication switch can be configured as the transmission port, and the eapol authentication packet is forwarded between the client and the 802.1 X authentication switch. O as to realize the 802.1 X authentication of other switches to the client.

The following command sets port ge1/1 as a transmit port in interface configuration mode:

Switch(config-ge1/1)dot1x transmit-port

The following command sets port ge1/1 to be a non-transmitting port in interface configuration mode:

Switch(config-ge1/1)no dot1x transmit-port

12.3.8 Configure 802.1x client version number

Configure the version number of the 802.1x client. Only the client whose version is not lower than the configured version number can be authenticated. Otherwise, the authentication fails. The default client version number for the switch is 2.0.

The following command configures the client version number in global CONFIG mode:

Switch(config)# dot1x client-version <string>

12.3.9 Configure whether to check client version number

Configure whether to check the version number of the 802.1x client. If it is configured to check, the switch will first check the version number of the client when authenticating. The default is configured to check.

The following command configures the checking of the client version number on in global CONFIG mode:

Switch(config)# dot1x check-version open

12.3.10 Configure authentication method

Configure the authentication mode of the switch for the 802.1 X packet. The authentication mode initiated by the client is divided into general authentication and extended authentication. The switch can be configured to authenticate in the first place. If the authentication mode initiated by the client is inconsistent with the authentication mode configured by the switch, the client will switch to another authentication mode to initiate authentication after a certain number of authentication failures.

The following command configures the authentication mode of the switch in global CONFIG mode as extended authentication:

Switch(config)# dot1x extended

12.3.11 Configure whether to check the timing packet of the client

Configure whether the switch checks the timing packet of the client. After successful authentication, the switch will require the client to send 802.1 X packets periodically, but not all clients will send 802.1 X packets periodically after passing the authentication. In this way, configure whether the switch checks the timing packet of the client through the command.

The following command is configured in global CONFIG mode for the switch to check the client's timing packets:

Switch(config)# dot1x check-client

12.3.12 Displaying 802.1x information

The following command displays the information of 802.1 X in normal mode/privileged mode. When the command is show dot1x, all configuration information of 802.1 X is displayed, including the configuration information of all ports; when the command is show dot1x interface, the information of all access users under the port is displayed:

Switch#show dot1x

Switch#show dot1x interface

12.4 Configure RADIUS

This section describes the RADIUS configuration in detail, mainly including the following contents:

RADIUS Default Configuration

- Configure the IP address of the authentication server
- Configure Shared Secret
- Start and stop billing
- Configure RADIUS port and attribute information
- Configure RADIUS roaming
- Display RADIUS information

12.4.1 RADIUS Default Configuration

The switch RADIUS configuration defaults as follows:

2. The IP addresses of the primary and backup authentication servers are not configured, that is, the IP address is 0.0.0.0.
3. There is no shared secret configured, that is, the shared secret string is empty.
4. Billing is enabled by default.
5. The RADIUS authentication UDP port is 1812 and the billing UDP port is 1813.
6. The RADIUS attributes NASPort have a value of 0 xc353, NASPortType has a value of 0x0f, and NASPortServer has a value of 0x02.

12.4.2 Configure the address of the authentication server

For RADIUS communication between the switch and the authentication server, the IP address of the authentication server needs to be configured on the switch. In practical applications, one authentication server or two authentication servers can be used, one as the main authentication server and one as the backup authentication server. If the switch is configured with the IP addresses of two authentication servers, the switch can switch to communicate with the backup authentication server when the communication between the switch and the primary authentication server is interrupted.

The following command configures the IP address of the primary authentication server in global CONFIG mode:

Switch(config)#radius-server host <ip-address>

The following command configures the IP address of the backup authentication server in global CONFIG mode:

Switch(config)#radius-server option-host <ip-address>

12.4.3 Configure Shared Secret

Mutual authentication is required between the switch and the authentication server, and the same shared key needs to be set on both the switch and the authentication server. Note that the shared key on the switch must be the same as the one on the authentication server.

The following command configures the switch's shared secret in global CONFIG mode:

Switch(config)#radius-server key <string>

12.4.4 Start and stop billing

If accounting is turned off by the switch, the switch will not send RADIUS accounting packets to the authentication server after successful authentication or when the user is offline. In general, in the actual application, the billing is turned on.

The following command starts accounting in global CONFIG mode:
Switch(config)#radius-server accounting

The following command turns off billing in global CONFIG mode:
Switch(config)#no radius-server accounting

12.4.5 Configure RADIUS port and attribute information

It is recommended that users do not modify the RADIUS port and attribute information configuration.

The following command modifies the RADIUS authentication UDP port in global CONFIG mode:

Switch(config)#radius-server udp-port <port-number>

The following command modifies RADIUS attribute information in global CONFIG mode:

Switch(config)#radius-server attribute nas-portnum <number>

Switch(config)#radius-server attribute nas-porttype <number>

Switch(config)#radius-server attribute service-type <number>

12.4.6 Configure RADIUS roaming

When MAC, IP, or VLAN binding is performed on the client, and the client is moved to another place, the bound client cannot perform 802.1 X authentication due to the change of the MAC address, IP address, or VLAN. Turning on radius roaming ignores the MAC, IP, or VLAN binding of the client and continues with 802.1 X authentication.

The following command configures RADIUS roaming in global CONFIG mode:

Switch(config)#radius-server roam

The following command turns off RADIUS roaming in global CONFIG mode:

Switch(config)#no radius-server roam

12.4.7 Display RADIUS information

The following command displays RADIUS configuration information in normal/privileged mode:

Switch#show radius-server

12.5 Configuration examples

Turn on the 802.1x protocol, configure the port ge1/1 as Auto, configure the primary authentication server as 198.168.80.111, and configure the shared key of the switch as abcdef.

- Switch#
- Switch# dot1x
- Switch#config t
- Switch(config)#radius-server host 198.168.80.111
- Switch(config)#radius-server key abcdef
- Switch(config)# interface ge1/1
- Switch(config-ge1/1)# dot1x control auto

12.6 TACACS+ Introduction

TACACS + authentication and authorization provides more rigorous user authority management, which can not only verify the legitimacy of users, but also authorize commands. After the TACACS + authentication is enabled, the user needs to verify the user name and password through the TACACS + server when accessing the switch. Only when the user name and password are correct and consistent can they pass the authentication. Users can access the switch after authentication.

TACACS + also divides users' permissions into two levels: ordinary users and privileged users. Ordinary users can only stay in the normal mode of CLI command line interface, and privileged users can access all modes of CLI command line interface. Based on the permission level, the command execution permission is also set. When a user enters a command (except enable, end and exit), he must verify his permission on the TACACS + server. If the verification fails, he will not execute it.

TACACS + authentication and authorization function is only applicable to telnet and SSH terminals, and does not control console terminals. When accessing the switch through telnet or SSH terminal, the user name and password need to be verified. The CLI can be accessed only after the user name and password are verified. During SSH access, only privileged users can pass through. TACACS + authentication is also applied to web login, but only verifies password privileges and permissions without command authorization.

By default, the switch does not turn on the TACACS + function. At this time, Telnet, SSH or web login all use the multi-user management function. After the TACACS + function is turned on, the multi-user management function can continue to be configured, but it is not actually used.

The commands related to TACACS + authentication authorization are shown in the table below：

Command	Description	CLI mode
tacacsplus enable	Turn on the TACACS + function	Global configuration mode
tacacsplus disable	Turn off the TACACS + function	Global configuration mode
tacacsplus host <server-ip>	Configure the primary server address and support IPv4 and IPv6. It is recommended to use ACS of Cisco	Global configuration mode
tacacsplus option-host <server-ip>	Configure the address of the standby server and support IPv4 and IPv6. It is recommended to use ACS of Cisco	Global configuration mode
tacacsplus key WORD	Configure the shared key, which is used to encrypt the transmission data and must be consistent with the configuration on the server	Global configuration mode
tacacsplus auth-type (PAP|CHAP)	Select the authentication method. The supported methods include PAP and chap. PAP is the default mode, and the field encapsulates the secret. Chap encapsulates the MD5 check code of the secret.	Global configuration mode
show tacacsplus	View TACACS + configuration information	Global configuration mode
no tacacsplus host	Clear primary server address	Global configuration mode
no tacacsplus key	Clear shared key	Global configuration mode

13. Configuring GMRP

This chapter includes the following contents:

- Introduction to GMRP
- Configure GMRP
- Show GMRP

13.1 Introduction to GMRP

Currently, GMRP (GARP Multicast Registration Protocol, GARP Multicast Registration Protocol) is a multicast registration protocol based on GARP, which is used to maintain multicast registration information in switches. All switches supporting GMRP can receive the multicast registration information from other switches, dynamically update the local multicast registration information, and propagate the local multicast registration information to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP-supporting devices in the same switching network.

When a host wants to join a multicast group, it sends out a GMRP join message. The switch adds the port receiving the GMRP join message to the multicast group, and broadcasts the GMRP join message in the VLAN where the receiving port is located, so that the multicast source in the VLAN can know the existence of the multicast member. When a multicast source sends a multicast packet to a multicast group, the switch only forwards the multicast packet to a port connected with a member of the multicast group, thereby realizing the layer 2 multicast in the VLAN.

13.2 Configure GMRP

The main configurations of GMRP include:

Open GMRP

View GMRP

In the configuration task, the global GMRP must be enabled before the port GMRP can be enabled.

13.2.1 Turn on GMRP settings

Command	Description	Configuration Mode
set gmrp enable | disable	Enable/disable global all VLAN gmrp	Global Configuration Mode
set gmrp enable vlan <vlan-id>	Nable global-specific VLAN gmrp	Global Configuration Mode
set gmrp registration{fixed | forbidden | normal} <if-name>	Configure interface registration multicast mode	Global Configuration Mode
set gmrp timer {join | leave | nleaveall} <time-value>	Configure the time of various timer	Global Configuration Mode
set port gmrp enable <if-name>	Enable port GMRP function	Global Configuration Mode
set port gmrp disable <if-name>	Disable the port GMRP function	Global Configuration Mode

13.2.2 Viewing GMRP Information

After the above configuration is completed, execute the show command in the privileged mode to display the running status of GMRP after configuration, and verify the effect of configuration by viewing the displayed information

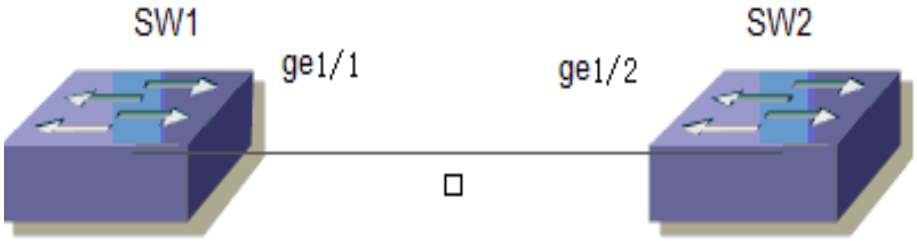
Command	Description	Configuration Mode
show gmrp configuration	Viewing GMRP Configuration Information	Privileged Mode
show gmrp machine	Viewing GMRP State Machine Information	Privileged Mode
show gmrp statistics vlanid	View gmrp statistics for a specific vlanid	Privileged Mode
show gmrp timer <ifname>	View timer information for a specific port	Privileged Mode

13.3 GMRP Typical Configuration Example

(1) Networking requirements

In order to realise the dynamic registration and update of multicast information between switches, GMRP needs to be started on the switch.

(2) Network diagram



GMRP Example Networking Diagram

Configuration steps:

Configure SW1
Start Global GMRP
Switch(config)# set gmrp enable
Start port GMRP on Gigabit Ethernet port ge1/1
Switch(config)# set port gmrp enable ge1/1
Switch(config)#
Configure SW2
Start Global GMRP
Switch(config)# set gmrp enable
Start port GMRP on Gigabit Ethernet port ge1/2
Switch(config)# set port gmrp enable ge1/2
Switch(config)#

14. Configuring IGMP SNOOPING

In man/Internet, when the same data packet is sent to multiple receivers in the network by unicast, the number of packets to be sent will increase linearly with the increase of the number of receivers due to the need to copy the packet to each receiving endpoint, which will increase the overall burden of the host, switching routing equipment and network bandwidth resources. Efficiency is greatly affected. With the increasing demand of multipoint video conference, video on demand and group communication applications, multicast has increasingly become a popular transmission mode in multipoint communication in order to improve resource utilization.

The switch implements the function of IGMP SNOOPING to serve multicast applications. IGMP SNOOPING monitors the IGMP packets on the network to realize the dynamic learning of IP multicast MAC address.

This chapter describes the concept and configuration of IGMP SNOOPING, mainly including the following contents:

- IGMP SNOOPING Introduction
- IGMP SNOOPING Configuration
- IGMP SNOOPING Configuration Example

14.1 IGMP SNOOPING Introduction

In the traditional network, multicast packets are treated as broadcast in a subnet, which is easy to cause network traffic and network congestion. When IGMP SNOOPING is implemented on the switch, IGMP SNOOPING can dynamically learn the IP multicast MAC address and maintain the output port list of the IP multicast MAC address, so that the multicast data stream is only sent to the output port, which can reduce the network traffic.

This section mainly includes the following contents:

IGMP SNOOPING process

- Layer-2 dynamic multicast
- Join a group
- Leave a group

14.1.1 IGMP SNOOPING process

IGMP SNOOPING is a Layer 2 network protocol that monitors IGMP packets passing through the switch, maintains a multicast group according to the receiving port, VLAN ID, and multicast address of these IGMP packets, and then forwards these IGMP packets. Only the ports joined in the multicast group can receive the multicast data stream, thus reducing the network traffic and saving the network bandwidth.

Multicast group includes multicast group address, member port, VLAN ID and Age time.

The formation of IGMP SNOOPING multicast group is a learning process. When a port of the switch receives an IGMP report packet, IGMP SNOOPING generates a new multicast group, and the port receiving the IGMP report packet is added to the multicast group. When the switch receives an IGMP QUERY packet, if the multicast group already exists in the switch, the port that received the IGMP QUERY also joins the multicast group. Otherwise, IGMP QUERY packets are simply forwarded. IGMP SNOOPING also supports the Leave mechanism of IGMP V2. If IGMP SNOOPING is configured with fast-LEAVE as ENABLE, its receiving port can immediately leave the multicast group when receiving

the leave packet of IGMP V2; If the fast-leave-timeout is configured, the multicast group waits for this time to expire before leaving the multicast group.

IGMP SNOOPING has two update mechanisms. One is the leave mechanism described above. In most cases, IGMP SNOOPING uses age time to delete expired multicast groups. When a multicast group joins IGMP SNOOPING, the joining time is recorded. When the multicast group remains in the switch for more than a configured age time, the switch deletes the multicast group.

When a port receives a Leave protocol packet, the port will be immediately deleted from its multicast group, which may affect the continuity of network data streams. Because a HUB or a network device without IGMP SNOOPING function may be connected under the port, and many devices receiving multicast data streams are connected under the device. If one device sends a Leave, it may affect other devices to receive the multicast data stream. The Fast-leave-timeout mechanism can prevent this from happening. A leave-waiting time is configured through the Fast-leave-timeout mechanism. After receiving the leave packet, the port waits for the Fast-leave-timeout long time before deleting it from the multicast group to which it belongs. It is possible to guarantee the continuity of the network multicast stream.

14.1.2 Layer-2 dynamic multicast

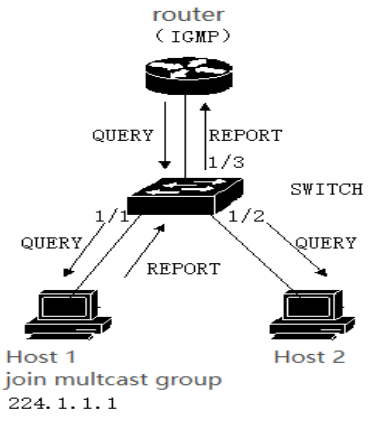
The multicast MAC address entries in the Layer 2 hardware multicast forwarding table can be learned dynamically by IGMP SNOOPING. The IP multicast MAC address is learned dynamically through IGMP SNOOPING.

When the switch closes the IGMP SNOOPING, the Layer 2 hardware multicast forwarding table is in the unregistered forwarding mode, the multicast MAC address cannot be dynamically learned, there is no entry in the Layer 2 hardware multicast forwarding table, and all Layer 2 multicast data streams are treated as broadcasts.

When the network has a multicast environment, in order to effectively control the multicast traffic of the network, the switch can enable the IGMP SNOOPING, at this time, the Layer 2 hardware multicast forwarding table is in the register forwarding mode, and the switch can learn the multicast MAC address by monitoring the IGMP protocol packet on the network. Only the layer 2 multicast flows matching the entries in the layer 2 hardware multicast forwarding table can be forwarded.

14.1.3 Join a group

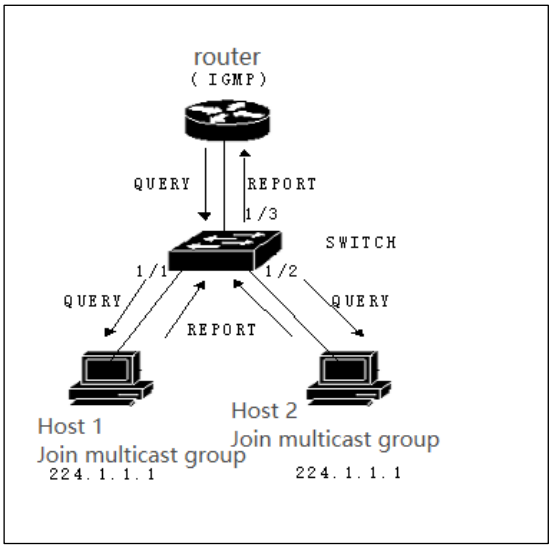
When a host wants to join a multicast group, the host sends an IGMP report packet that specifies the multicast group the host wants to join. When the switch receives an IGMP query packet, the switch forwards the packet to all other ports in the same VLAN..



When the switch receives an IGMP query packet, the switch forwards the packet to all other ports in the same VLAN. When the host under the port that wants to join the multicast group receives the IGMP query packet, it returns an IGMP report packet. When the switch receives an IGMP report packet, a layer 2 multicast entry is created, and the port that receives the IGMP QUERY packet and the port that receives the IGMP report packet are added to the layer 2 multicast entry as its output ports.

As shown in the figure above, all the devices are in a subnet, and the VLAN of the subnet is assumed to be 2. The router runs the IGMPv2 protocol and sends IGMP QUERY packets periodically. Host 1 wants to join a multicast group 224.1. 1.1. When the switch receives an IGMP query packet from port 1/3, it notes this port and forwards the packet to ports 1/1 and 1/2. Host 1 sends back an IGMP report packet after receiving the IGMP query packet, and host 2 does not send the IGMP report packet because it does not want to join the multicast group. When the switch receives an IGMP report packet on port 1/1, it forwards the packet out query port 1/3 and creates a Layer 2 multicast entry (assuming the entry does not exist) that includes the following:

Layer 2 multicast addr	VLAN ID	List of output ports
01:00:5e:01:01:01	2	1/1， 1/3



The condition in the above figure is the same as that in Figure 1. Host 1 has joined the multicast group 224.1. 1.1, and now host 2 wants to join the multicast group 224.1. 1.1. When host 2 receives the IGMP query packet and returns an IGMP report packet, the switch will forward the IGMP report packet from query port 1/3 after receiving it from port 1/2, and add the IGMP report packet from port 1/2 to the Layer 2 multicast entry. The Layer 2 multicast entry becomes

Layer 2 multicast addr	VLAN ID	List of output ports
01:00:5e:01:01:01	2	1/1， 1/2， 1/3

14.1.4 Leave a group

In order to form a stable multicast environment, a device running IGMP (such as a router) will send an IGMP query packet to all hosts at regular intervals. A host that has joined or wants to join a multicast group receives the IGMP QUERY and sends back an IGMP REPORT.

If a host wants to leave a multicast group, there are two ways: active and passive. Active leave means that the host sends an IGMP leave packet to the router. Passive leave means that the host does not return an IGMP REPORT after receiving an IGMP QUERY from the router.

Corresponding to the way the host leaves the multicast group, there are two ways for the port on the switch to leave the layer 2 multicast entry: timeout leaving and receiving IGMP LEAVE packet leaving.

When the switch does not receive an IGMP report packet of a multicast group from a port for a certain time, the port is removed from the corresponding layer 2 multicast entry, and if the layer 2 multicast entry has no port, the layer 2 multicast entry is deleted.

When the fast-leave configuration of the switch is ENABLE, if a port receives an IGMP leave packet of a multicast group, the port is removed from the corresponding layer 2 multicast entry. If the layer 2 multicast entry has no port, the layer 2 multicast entry is deleted.

Fast-leave is generally used when a port is connected to a host. If there is more than one host under a port, the fast-leave-timeout waiting time can be configured to ensure the continuity and reliability of multicast streams in the network.

14.1.5 IGMP Querier

In a network with a three-layer multicast device, the three-layer multicast device acts as an IGMP queryer. The two-layer multicast equipment only needs to monitor the IGMP message, and can establish and maintain the forwarding table item to realize the two-layer multicast. In a network without a Layer 3 multicast device, a Layer 3 multicast device cannot act as an IGMP query. In order to enable the layer 2 multicast device to monitor the IGMP message, the IGMP query function must be configured on the layer 2 device. The layer 2 multicast device not only acts as an IGMP inquirer, but also monitors IGMP messages, so as to establish and maintain forwarding table entries and realize layer 2 multicast.

How it works:

The function of the IGMP query device is that the layer 2 device plays the role of IGMP routing query, sends the IGMP query message at regular time, intercepts and maintains the IGMP Report message answered by the user, and establishes the forwarding table entry of the layer 2 multicast. The relevant parameters of the query message sent by IGMP query can be adjusted by the user through configuration.

① Start the query device: The user can configure to enable the query device function on the specified VLAN.

② Specify the IGMP version used by the query device: Specify the IGMP version used by the query message sent by the query device, which can be configured as v1 or v2 or v3 version.

③ configures the source IP of the inquirer, configures the source IP address carried by the inquiry message sent by the inquirer

④ Configure the query interval of the query device: configure the time interval of the query message sent by the global query device.

14.1.6 IGMP snooping multicast filtering

The device running IGMP Snooping can control the multicast service range and load, and can effectively prevent illegal multicast streams. By configuring the multicast filtering rules globally and applying the rules on the interfaces, it is possible to allow or restrict the joining of specific groups.

14.2 IGMP SNOOPING Configuration

14.2.1 IGMP SNOOPING Default Configuration

IGMP SNOOPING is off by default, and the Layer 2 hardware multicast forwarding table is in unregistered forwarding mode.
Fast-leave is off by default.
Fast-leave-timeout is 300 seconds.
The default age time for the multicast group report port is 400 seconds.
The default age time for the multicast group QUERY port is 300 seconds.

14.2.2 Turn IGMP SNOOPING ON and OFF

The IGMP SNOOPING protocol can be opened globally or separately for some VLANs; only the IGMP SNOOPING protocol can be opened or closed globally for a certain VLAN.

Turn on global IGMP SNOOPING

Switch#configure terminal
Switch(config)#ip igmp snooping

Turn on IGMP SNOOPING for one VLAN

Switch#configure terminal
Switch(config)#ip igmp snooping vlan <vlan-id>

Turn off global IGMP SNOOPING

Switch#configure terminal
Switch(config)#no ip igmp snooping

Turn off IGMP SNOOPING for one VLAN

Switch#configure terminal
Switch(config)#no ip igmp snooping vlan <vlan-id>

14.2.3 Configuration Lifetime

Configure the lifetime of a multicast group
Switch#configure terminal
Switch(config)#ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>
Interval is in milliseconds.

Configuring the Lifetime of a Query Group

Switch#configure terminal

Switch(config)#ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>
Interval is in milliseconds.

14.2.4 Configuring fast-leave

Start fast-leave for one VLAN

Switch#configure terminal
Switch(config)#ip igmp snooping fast-leave vlan <vlan-id>

Close fast-leave

Switch#configure terminal
Switch(config)#no ip igmp snooping fast-leave vlan <vlan-id>

Configure the fast-leave wait times

Switch#configure terminal
Switch(config)# ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>

Restore default fast-leave wait times

Switch#configure terminal
Switch(config)#no ip igmp snooping fast-leave-timeout vlan <vlan-id>

14.2.5 Configure MROUTER

Configure a static query port

Switch#configure terminal
Switch#interface ge1/6
Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

14.2.6 Configure IGMP snooping query port function

Configure a static query port

Switch#configure terminal
Switch(config)#interface ge1/6
Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

14.2.7 Configuring the IGMP snooping query feature

Start the IGMP snooping query function of vlan1

Switch#configure terminal
Switch(config)#ip igmp sno
Switch(config)#ip igmp snooping querier vlan 1

14.2.8 Configure IGMP snooping multicast filtering

Configure the filtering multicast address of port ge1/1 as 235.0.0.1

Switch#configure terminal
Switch(config)#ip igmp snooping filter-rule 1 deny 235.0.0.1
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ip igmp snooping filter-group 1

14.2.9 Display Information

Display IGMP SNOOPING configuration information

Switch#show ip igmp snooping

Displays configuration information for a VLAN

Switch#show ip igmp snooping vlan <vlan-id>

Displays aging information for a report multicast group

Switch#show ip igmp snooping age-table group-membership

Display aging information for QUERY

Switch#show ip igmp snooping age-table query-membership

Displays forwarding information for a multicast group

Switch#show ip igmp snooping forwarding-table

Display MROUTER information

Switch#show ip igmp snooping mrouter

Displays the current configuration of the system, including the configuration of IGMP SNOOPING

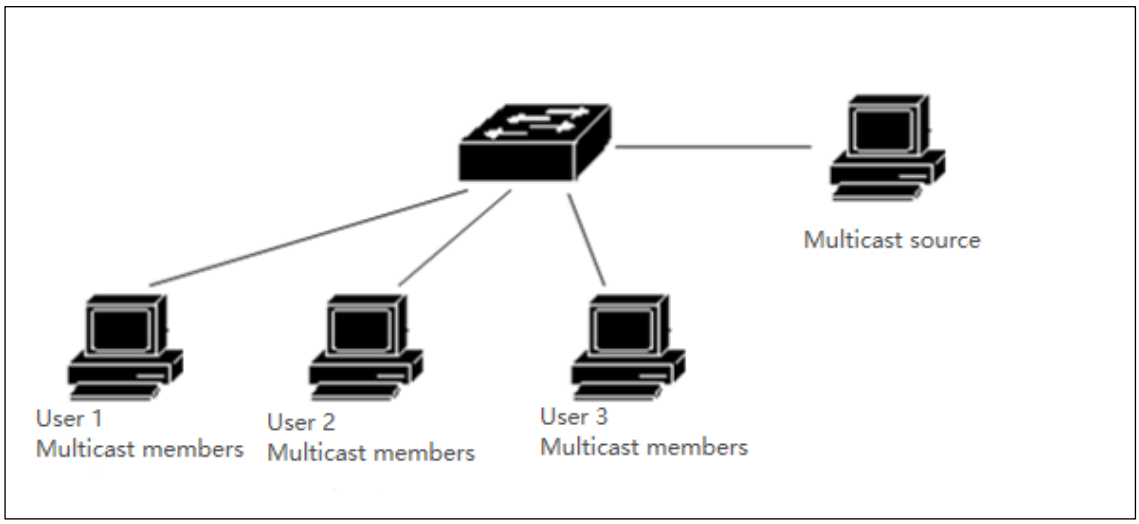
Switch#show running-config

14.3 IGMP SNOOPING Configuration Example

14.3.1 Configuration

Enable the IGMP SNOOPING function on the switch. User 1, User 2, and User 3 can join a specific multicast group.

:



Switch#config t

Switch(config)#ip igmp snooping

Switch(config)#vlan database

Switch(config-vlan)#vlan 200

Switch(config-vlan)#exit

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 200

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 200

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode access

Switch(config-ge1/3)#switchport access vlan 200

Switch(config)#ip igmp snooping vlan 200

Switch(config)#ip igmp snooping group-membership-timeout 60000 vlan 200

15. MVR Configuration

This chapter includes the following contents:

- Introduction to MVR
- Configure MVR

15.1 Introduction to MVR

Multicast VLAN Registration (MVR) for multicast streaming applications in a service provider network, such as video-on-demand. MVR allows subscribers on a port to subscribe to or cancel multicast flows within a multicast VLAN, allowing data flows within one multicast VLAN to be shared by other VLANs. MVR has two objectives: (1) to be able to deliver multicast streams between VLANs efficiently and securely with simple configuration; (2) to support dynamic joining and leaving of multicast groups;

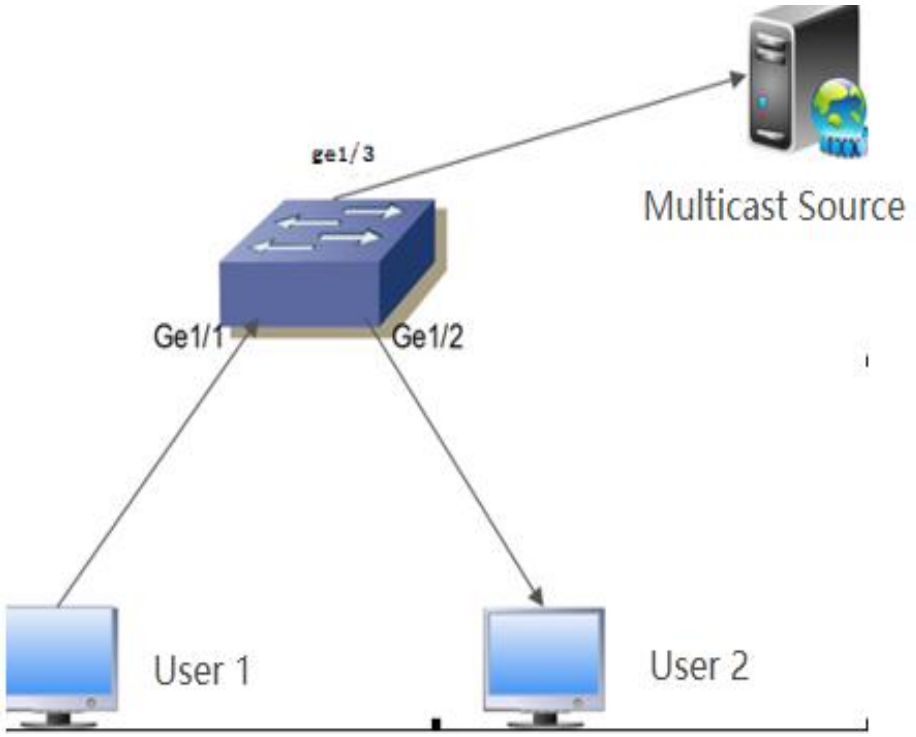
The operation of MVR is similar to IGMP snooping. The two functions can be started at the same time. MVR only handles the joining and leaving of the configured multicast group, and the joining and leaving of other groups are managed by IGMP snooping. The difference between the two is that the multicast stream in IGMP snooping can only be forwarded in one VLAN, while the multicast stream in MVR can be forwarded in different VLANs.

15.2 Configure MVR

Command	Description	CLI Mode
mvr (enable|disable)	Start Global MVR	Global Configuration Mode
no mvr	Clear all MVR configuration	Global Configuration Mode
mvr group A.B.C.D	Configure IP multicast addr	Global Configuration Mode
no mvr group A.B.C.D	Delete IP multicast addr	Global Configuration Mode
mvr group A.B.C.D <1-256>	Configure IP multicast address and c onfigure a continuous MVR group ad dress	Global Configuration Mode
mvr vlan <1-4094>	Specifies the VLAN that receives the multicast data	Global Configuration Mode
no mvr vlan	Restore the default VLAN 1 for receiving multicast data	Global Configuration Mode
mvr-interface (enable|disable)	Start interface MVR	Interface Configuration Mode
show mvr	Display MVR configuration information	Privileged mode

15.3 MVR Configuration Example

The network topology is as shown in the following figure. User 1 and user 2 belong to vlan10 and vlan20 respectively. User 1 and user 2 watch the same program, the program range is 225.1.1.1 ~ 225.1.1.64, and the MVR VLAN is 100:



Configure VLAN, start global IGMP snooping, configure MVR VLAN, MVR program group scope, and globally enable MVR:

Switch#configure terminal

Switch(config)#ip igmp snooping

Switch(config)# mvr enable

Switch(config)#mvr vlan 100

Switch(config)#mvr group 225.1.1.1 64

Switch#

Configure the user port ge1/1, ge1/2, and the uplink port ge1/3 of the switch:

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode hybrid

Switch(config-ge1/1)# switchport hybrid native vlan 10

Switch(config-ge1/1)#switchport hybrid allowed vlan add 100 egress-tagged disable

Switch(config-ge1/1)#mvr enable

Switch(config-ge1/1)#

Switch#configure terminal

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode hybrid

Switch(config-ge1/2)# switchport hybrid native vlan 20

Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged disable

Switch(config-ge1/2)#mvr enable

Switch(config-ge1/2)#

Switch#configure terminal

Switch(config)#interface ge1/3

Switch(config-ge1/3)# switchport access vlan 100

Switch(config-ge1/3)#

16. Configuring DHCP SNOOPING

In a dynamic access network environment, a host acquires an IP address and network parameters through a DHCP server. DHCP SNOOPING is a snooping protocol for ARP attacks. By monitoring the DHCP message, the IP address assigned to the client by the DHCP server and the MAC address of the client are dynamically bound, so as to filter the ARP attack message on the switch.

The switch supports the DHCP SNOOPING function, which can effectively defend against ARP attacks. DHCP SNOOPING intercepts DHCP messages on the network and binds port ARP information.

Four linked DHCP server physical ports can be configured to prevent unknown servers from interfering with the network to some extent.

This chapter describes the concept and configuration of DHCP SNOOPING, mainly including the following contents:

- Introduction to DHCP SNOOPING
- DHCP SNOOPING Configuration
- DHCP SNOOPING Configuration Example

16.1 Introduction to DHCP SNOOPING

Because of the simple trust mechanism, the ARP protocol has caused the loophole to the network security. When an ARP attack packet carrying false MAC information arrives at the host, it will directly overwrite the local ARP cache table without restriction, resulting in normal data flow to the attacker. Therefore, the ARP information binding of the port is implemented on the network layer 2 switch, which can effectively filter the ARP attack packet, so that the attack packet can not reach the attacked host. If an unpredictable DHCP server enters the network, the IP address allocation will be confused. The DHCP SNOOPING protocol provides the physical port of the binding link server. The non-designated physical port cannot forward the DHCP protocol packet sent by the DHCP server, which can reduce the chance of such an unknown server entering the network.

This section mainly includes the following contents:

- DHCP SNOOPING Handling Procedure
- DHCP SNOOPING Binding Table
- DHCP SNOOPING Bind Server's Physical Port

16.1.1 DHCP SNOOPING Handling Procedure

The DHCP SNOOPING protocol only intercepts DHCPrequest, DHCPack, and DHCPrelease messages, and does not receive other types of DHCP messages, and binds the mapping relationship between IP and MAC according to these messages.

The global DHCP SNOOPING switch is responsible for turning on the switch to receive DHCP messages, that is, IP messages with UDP ports 67 and 68.

16.1.2 DHCP SNOOPING Binding Table

The DHCP SNOOPING binding table entry is indexed by MAC address and contains the entry type, IP address, MAC address, interface information, delay timer, and lease timer. There are two types: REQ and ACK. The entry of REQ type indicates that the DHCPrequest message has been received but the DHCPack message has not been received. At this time, the delay timer is started. The default time interval is 10 seconds. If no DHCPack message is received within 10 seconds,The binding table entry of the REQ type is deleted; An entry of ACK type indicates that a DHCPack message is received, the

recorded IP address is the IP address allocated by the server, a lease timer is started at this time, the time interval is the lease value provided by the DHCP server contained in the DHCPack message, the timer is restarted when the lease is renewed, and the binding table entry is deleted when the lease expires. The interface information records the interface where the client is located, that is, the interface corresponding to the binding relationship between the IP address and the MAC address.

When a DHCPrequest message is received, a binding table entry is created, the entry type is REQ, the IP address, the MAC address and the interface information are recorded, and a 10-second delay timer is started.

When the DHCPrequest message is received, the binding table entry of the REQ type already exists, the entry is updated, and the delay timer is restarted.

When a DHCPrequest message is received and an ACK type binding table entry already exists, the interface information is recorded.

When the DHCPack message is received, if the binding table entry of the REQ type exists, the IP address allocated by the server in the DHCPack message is recorded, the delay timer is closed, and the lease timer is started.

When the DHCPack message is received and no binding table entry of the REQ type exists, the message is discarded.

When the DHCPack message is received, the binding table entry of the ACK type already exists, and if the interface is changed, the binding table entry of the original interface is deleted, and the entry is updated.

If the interface is not changed and the IP address assigned by the server is changed, the binding table entry of the original interface is deleted and the entry is updated.

If the interface has not changed and the IP address has not changed, it indicates a renewal process and the lease timer can be restarted.

The delay timer expires and the binding table entry of type REQ is deleted.

The lease timer times out and the ACK type binding table entry is deleted.

16.1.3 DHCP SNOOPING Specifies the physical port of the linked server

DHCP SNOOPING specifies the physical port of the linked server. DHCP messages can be received only on the specified port. If there are multiple DHCP servers in the network, the OFFER provided by the server from a non-designated port will be filtered, and the IP address cannot be assigned to the client. The designated port is conducive to the unified allocation of IP addresses in the network, avoiding that the address pool of unknown servers is not in the IP planning, and some clients can not connect to the network normally. And that probability of network communication abnormity cause by private access to the server is reduce to a certain extent.

16.2 DHCP SNOOPING Configuration

16.2.1 DHCP SNOOPING Default Configuration

DHCP SNOOPING is off by default.

The default delay timer interval for entries of type REQ in the DHCP SNOOPING binding table is 10 seconds.

16.2.2 Turning DHCP SNOOPING on and off globally

DHCP SNOOPING cannot be turned on or off for an interface until DHCP SNOOPING is turned on globally. You must turn off all interfaces before turning off DHCP Snooping globally.

Turn on global DHCP SNOOPING

Switch#configure terminal

Switch(config)#ip dhcp snooping [IF_LIST]

The parameter is the physical port list of the linked DHCP server to be bound. Four ports can be specified in total. The port list is separated by ",", such as ge1/1, ge1/4, ge1/5

Turn off global DHCP SNOOPING

Switch#configure terminal

Switch(config)#no ip dhcp snooping

16.2.3 Interface DHCP SNOOPING ON and OFF

Open DHCP SNOOPING for a port

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#dhcp snooping

Turn off DHCP SNOOPING on one port

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no dhcp snooping

16.2.4 Interface DHCP SNOOPING OPTION8 ON and OFF

DHCP SNOOPING OPTION82 to open an interface

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#dhcp snooping option82

Turn off DHCP SNOOPING OPTION82 on one port

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no dhcp snooping option82

Configure the circuit-id of DHCP SNOOPING OPTION82 for a port

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)# dhcp snooping option82 circuit-id vlan111

Deletes the circuit-id of DHCP SNOOPING OPTION82 for a port

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)# no dhcp snooping option82 circuit-id

16.2.5 Display Information

Display DHCP SNOOPING configuration information

Switch#show dhcp snooping

Displays DHCP SNOOPING binding table information

Switch#show dhcp snooping binding-table

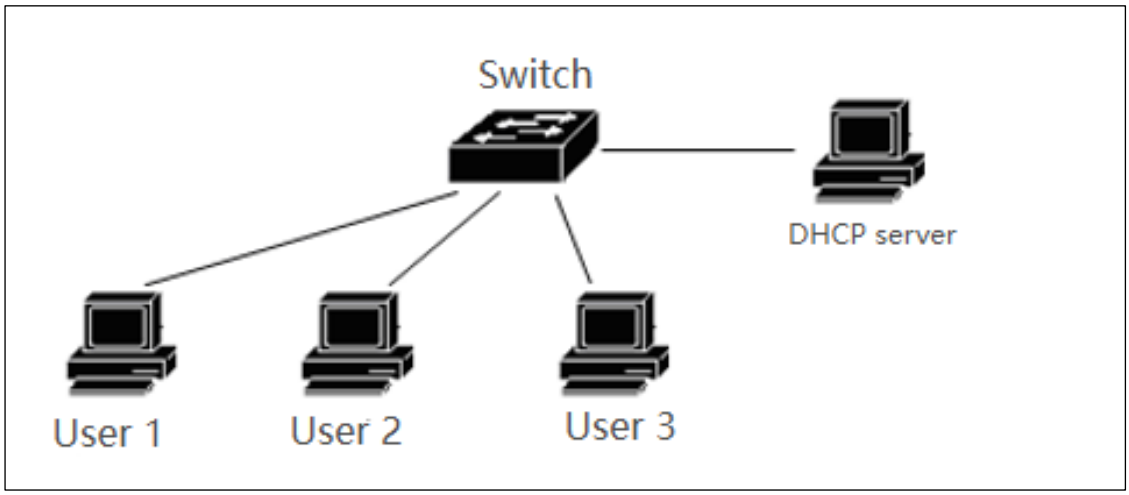
Displays the current configuration of the system, including DHCP SNOOPING configuration.

Switch#show running-config

16.3 DHCP SNOOPING Configuration Example

16.3.1 Configuration

Enable the DHCP SNOOPING function on the layer 2 switch. User 1, User 2, and User 3 dynamically obtain the IP address and network parameters through the DHCP server. DHCP SNOOPING OPTION82 function is enabled on the interfaces of user 1, user 2 and user 3, the circuit-id is AAA, and ARP information is dynamically bound on the interfaces.



Switch#configure terminal
Switch(config)#ip dhcp snooping ge1/5
Switch(config)#interface ge1/1
Switch(config-ge1/1)#dhcp snooping
Switch(config-ge1/1)#dhcp snooping option82
Switch(config-ge1/1)#dhcp snooping option82 circuit-id aaa
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#dhcp snooping
Switch(config-ge1/2)#dhcp snooping option82
Switch(config-ge1/2)#dhcp snooping option82 circuit-id aaa
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#dhcp snooping
Switch(config-ge1/3)#dhcp snooping option82
Switch(config-ge1/3)#dhcp snooping option82 circuit-id aaa
Switch(config-ge1/3)#end

View DHCP snooping information

Switch#show dhcp snooping
DHCP Snooping is enabled globally
DHCP Server interface: ge1/5
Enable interface: ge1/1 ge1/2 ge1/3
Option 82 interface: ge1/1(Circuit ID: aaa) ge1/2(Circuit ID: aaa) ge1/3(Circuit ID: aaa)

Switch#
Switch#show dhcp snooping binding-table

IP	MAC	FLAG	PORT	LEASE
192.168.1.100	00:11:5b:34:42:ad	ACK	ge1/1	23:59:58
192.168.1.101	00:11:64:52:13:5d	ACK	ge1/2	23:50:01
192.168.1.102	00:11:80:4d:a2:46	ACK	ge1/3	20:34:45

16.4 DHCP SNOOPING Configuration Troubleshooting

If the DHCP snooping configuration fails, it may be caused by the following:

① The system CFP resource is exhausted.

② If an interface is configured with ACL filtering function, global opening of DHCP SNOOPING fails.

③ If an interface is configured with IP and MAC binding, global opening of DHCP SNOOPING fails.

④ The current interface is configured with ACL filtering function.

⑤ 802.1 X anti-ARP spoofing enabled on the current interface.

⑥ The configured interface is a three-layer interface or a trunk interface

17. DHCP CLIENT Configuration

17.1 Introduction to DHCP CLIENT

DHCP (Dynamic Host Configuration Protocol) is based on the Client/Server working mode. The function of DHCP CLIENT is that the three-layer interface address of the switch can obtain the address and gateway through the DHCP server.

This section mainly includes the following contents:

Configuration of DHCP CLIENT

17.2 DHCP CLIENT Configuration

Turn on the DHCP client feature for interface vlan1

switch(config)#

Switch(config)#interface vlan1

Switch(config-vlan1)#dhcp client enable

Retrieve the IP address for interface vlan1

switch(config)#

Switch(config)#interface vlan1

Switch(config-vlan1)#dhcp client renew

Turn on the DHCP client feature for interface vlan1

switch(config)#

Switch(config)#interface vlan1

Switch(config-vlan1)#dhcp client release

18. DHCP RELAY

This chapter includes the following contents:

Introduction to DHCP RELAY

- DHCP RELAY Configuration
- DHCP RELAY Configuration Example

18.1 Introduction to DHCP RELAY

DHCP (Dynamic Host Configuration Protocol) is an enhanced version of BOOTP, which dynamically configures the network environment for the hosts on the network. It is divided into server and client. The server centrally manages IP network data and processes client requests, and dynamically configures the TCP/IP environment of the client. When DHCP works, there is at least one server on the network that can listen for DHCP requests from hosts on the network and negotiate TCP/IP parameters. It can be allocated automatically or dynamically. Automatically, once a client obtains an IP address, it uses that address permanently. In the dynamic mode, the IP address obtained by the client has a lease, and once the lease expires, the IP address needs to be released; the lease can also be renewed in advance, or other IP addresses can be leased. Dynamic allocation can effectively solve the problem of insufficient IP.

How DHCP works:

If the client is logging on the network for the first time, it does not have any IP data and will broadcast a Discover message, source address 0.0. 0.0, destination address 255.255. 255.255. If the server does not respond, four Discover requests are issued at regular intervals.

And that serv selects an idle IP to respond to the client Offer message after receiving the Discover.

If there are multiple servers on the network, the client will receive multiple Offer messages. Generally, it will select the offer that arrives first and broadcast the Request message to tell all the servers that it has received the IP address provided by which server.

If the client finds that the IP has been used through ARP, it sends a Decline message to the server, rejects the Offer, and restarts the Discover process.

After receiving the Request message, the server will send an Ack message to the client to confirm that the lease is effective.

If the client has applied for a DHCP lease, there is generally no need to use the Discover process. Before the lease expires, the leased IP is used to send a Request to the server for renewal. The server will try to let the client use the original IP. If there is no problem, the server will respond to the Ack message for confirmation. If the IP has been used by other clients, the server responds to the Nack message to reject the renewal request.

The client can use the Release message to actively release the lease.

The workstation sends a Request request when it is powered on; it will send a Request request again when the lease is half, and the IP can still be used if there is no confirmation; it will send a Request request when the lease is 3/4, and the IP can no longer be used if there is no confirmation.

The Discover message is issued in the form of broadcast, which can only be in the same network segment, and the router will not spread the broadcast message. When the server and the client are not in the same network segment, the client has not obtained the IP environment settings and does not know the location of the router, the Discover message cannot reach the server. In order to solve this problem, the function of DHCP relay can be used to let the router transfer the DHCP protocol message, so that DHCP can operate across network segments.

18.2 DHCP RELAY Configuration

The function of DHCP relay is mostly related to the interface, which realizes the forwarding of DHCP protocol messages across network segments and performs related configuration in the interface mode.
The configuration of DHCP-relay includes:
Start the DHCP-relay function of the interface

18.2.1 Start the DHCP-relay function of the interface

Mode: Interface configuration model

Command: DHCP relay < ip-address-1 > ip-address-2] turns on the DHCP relay protocol on the interface

Command: no DHCP relay close that DHCP relay protocol on the interface

Default: The DHCP relay protocol is not turned on.

18.2.2 Display Information

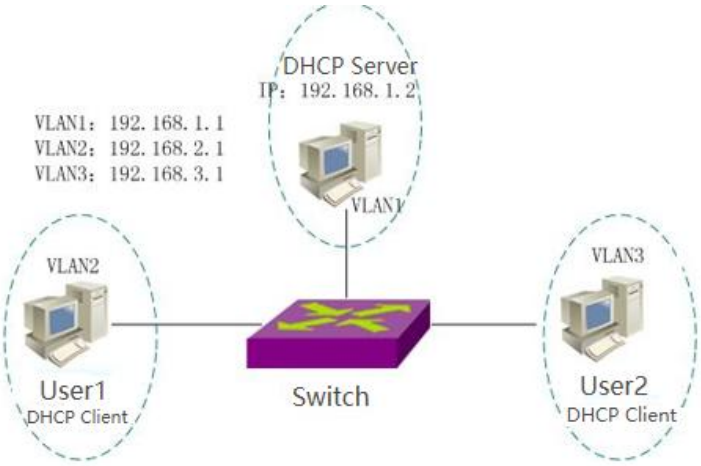
Display DHCP relay configuration information

Switch#show dhcp relay

18.3 DHCP RELAY Configuration Example

(1) Configuration

The switch needs to be configured for DHCP relay forwarding to enable the switch to route and forward DHCP requests from User 1 and User 2 and DHCP reply acknowledgements from the DHCP server. User 1 and user 2 can obtain legal IP addresses through DHCP servers in different network segments to access the network.



Switch>en
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#exit
Switch(config)#ip interface vlan 2
Switch(config)#ip interface vlan 3
Switch(config)#int ge1/2
Switch(config-ge1/2)#sw access vlan 2
Switch(config-ge1/2)#int ge1/3
Switch(config-ge1/3)#sw access vlan 3
Switch(config-ge1/3)# interface vlan2
Switch(config-vlan2)#ip address
192.168.2.1/24
Switch(config-vlan2)#dhcp relay 192.168.1.2
Switch(config-vlan2)#interface vlan3
Switch(config-vlan3)#ip address
192.168.3.1/24
Switch(config-vlan3)#dhcp relay 192.168.1.2

(2) Verification

show running-config Display Configuration Command
show dhcp relay Display DHCP relay configuration information

19. DHCP CLIENT Configuration

19.1 Introduction to DHCP CLIENT

DHCP (Dynamic Host Configuration Protocol) is based on the Client/Server working mode. The function of DHCP CLIENT is that the three-layer interface address of the switch can obtain the address and gateway through the DHCP server.

This section mainly includes the following contents:

Configuration of DHCP CLIENT

19.2. DHCP CLIENT Configuration

Turn on the DHCP client feature for interface vlan1

switch(config)#

Switch(config)#interface vlan1

Switch(config-vlan1)#dhcp client enable

Retrieve the IP address for interface vlan1

switch(config)#

Switch(config)#interface vlan1

Switch(config-vlan1)#dhcp client renew

Turn on the DHCP client feature for interface vlan1

switch(config)#

Switch(config)#interface vlan1

Switch(config-vlan1)#dhcp client release

19. Configuring DHCP SERVER

This chapter mainly includes the following contents:

- Introduction to DHCP SERVER
- DHCP SERVER Configuration
- DHCP SERVER Configuration Example

19.1. Introduction to DHCP SERVER

DHCP (Dynamic Host Configuration Protocol) is an enhanced version of BOOTP, which dynamically configures the network environment for the hosts on the network. It is divided into server and client. The server centrally manages IP network data and processes client requests, and dynamically configures the TCP/IP environment of the client. When DHCP works, there is at least one server on the network that can listen for DHCP requests from hosts on the network and negotiate TCP/IP parameters. It can be allocated automatically or dynamically. Automatically, once a client obtains an IP address, it uses that address permanently. In the dynamic mode, the IP address obtained by the client has a lease, and once the lease expires, the IP address needs to be released; the lease can also be renewed in advance, or other IP addresses can be leased. Dynamic allocation can effectively solve the problem of insufficient IP.

How the DHCP Serve works:

If the client is logging on the network for the first time, it does not have any IP data and will broadcast a Discover message, source address 0.0. 0.0, destination address 255.255. 255.255. If the server does not respond, four Discover requests are issued at regular intervals.

And that server selects an idle IP to respond to the client Offer message after receiving the Discover.

If there are multiple servers on the network, the client will receive multiple Offer messages. Generally, it will select the offer that arrives first and broadcast the Request message to tell all the servers that it has received the IP address provided by which server.

If the client finds that the IP has been used through ARP, it sends a Decline message to the server, rejects the Offer, and restarts the Discover process.

After receiving the Request message, the server will send an Ack message to the client to confirm that the lease is effective.

If the client has applied for a DHCP lease, there is generally no need to use the Discover process. Before the lease expires, the leased IP is used to send a Request to the server for renewal. The server will try to let the client use the original IP. If there is no problem, the server will respond to the Ack message for confirmation. If the IP has been used by other clients, the server responds to the Nack message to reject the renewal request.

The client can use the Release message to actively release the lease.

The workstation sends a Request request when it is powered on; it will send a Request request again when the lease is half, and the IP can still be used if there is no confirmation; it will send a Request request when the lease is 3/4, and the IP can no longer be used if there is no confirmation.

The DHCP server protocol module receives the Discover, Request, Decline, and Release messages, and is used to dynamically allocate IP addresses to clients in the network, and maintain its own address pool information and allocated client information.

19.2 DHCP SERVER Configuration

DHCP server functions need to be configured in global mode, interface mode and address pool mode, including startup commands, address pool configuration, global settings, and tuning switches.

The configuration of the DHCP server includes:

- Start the global DHCP server function
- Start the interface to receive the DHCP server message
- Configure address pool
- Configure address pool ran
- Configure address pool subnet mask
- Configure address pool lease
- Configure the address pool default gateway
- Configure address pool DNS server
- Configure manual exclusion addresses in the address pool

19.2.1 Start the global DHCP server function

Mode: Global Configuration Mode

Command: ip dhcp server starts the global DHCP server protocol

Command: no ip dhcp server turns off the global DHCP server protocol

Default: The DHCP server protocol is not turned on; use this command to start the DHCP server protocol.

19.2.2 Start the interface to receive the DHCP server message

Mode:Interface Configuration Mode

Command:dhcp server listen

Interface starts to receive DHCP server protocol message

Command:no dhcp server listen

The interface is closed and does not receive DHCP server protocol message

Default: The interface is not started and cannot receive DHCP server protocol messages.

19.2.3 Configure address pool

Mode: Global Configuration Mode

Command:dhcp server pool <pool-name>

Create an address pool and enter address pool model

Command:no dhcp server pool <pool-name>

Deletes the specified address pool

Parameter: < pool-name > address pool name, used to distinguish different address pools. Up to 16 characters.

Default:Address pools are not configured. To configure an address pool, just create an address pool name and enter the address pool configuration mode without configuring the actual address.

19.2.4 Configure address pool ran

Mode: Address pool configuration model

Command:no range Delete Address Pool Range

Parameters: < low-address > The starting address of the pool range in dotted-decimal format; < high-address > The ending address of the pool range in dotted-decimal format.

Default:ranges are not configured. When a range is configured in the address pool, an entry is created for each dynamically assignable address within that range in the address pool.

19.2.5 Configure address pool subnet mask

Mode:Address pool configuration model

Command:subnet-mask <address>

Configure address pool subnet mask

Parameters: < address > mask address, in dotted decimal format, is a variable length mask.

Default:255.255.255.0 defaults to a 24-bit mask.

19.2.6 Configure address pool lease

Mode: Address pool configuration model

Command:lease [<days> <hours> <minutes>|infinite]

Configure address pool lease

Parameters: < days > is the number of days, and the range is 0-999; < hours > is the number of hours, and the range is 0-23; < minutes > is a number of minutes, and the ranges are 0-59; all are integers. Infinite is the lease unlimited.

Default: The lease is for 8 days.

19.2.7 Configure the address pool default gateway

Mode: Address pool configuration model

Command:default-router <ip-address>

Configure the address pool default gateway

Command:no default-router Delete Pool Default Gateway

Parameters: < ip-address > The default gateway IP address, in dotted decimal format, should be in the same network segment as the address pool range.

Default: The default gateway is not configured.

19.2.8 Configure address pool DNS server

Mode: Address pool configuration model

Command:dns-server <ip-address1> [ip-address2]

Configure address pool DNS server

Command:no dns-server Remove the address pool DNS server

Parameters: < ip-address1 > and < ip-address2 > are IP addresses of DNS servers in dotted decimal format. Up to two DNS servers or one DNS server can be configured. If two computers are configured, they should be entered in one command, not in two separate commands. If you enter twice, the IP address of the DNS server entered later overrides the previously configured DNS server address, regardless of whether one or two DNS servers were previously configured.

Default: No DNS server is configured.

19.2.9 Configure manual exclusion addresses in address pool

Mode: Address pool configuration model

Command:exclude-address <ip-address>

Configure manual exclusion addresses in the address pool

Command:exclude-address <low-address> <high-address>

Configure Manual Exclusion Address Range

Command:no exclude-address <ip-address>

Restore a manually excluded addr

Command:exclude-address <low-address> <high-address>

Configuring Manual Exclusion Address Range Recovery

Command:no exclude-address all

Restore all manually excluded addresses in the address pool

Parameters: < ip-address > The manually excluded IP address, in dotted-decimal format. One command excludes one available address at a time from the pool. < low-address > and < high-address > are the starting and ending IP addresses of the manually excluded address range, in dotted decimal format. One command can exclude multiple consecutive available addresses in the address pool range at a time. If an address in the range has been manually excluded, it will be skipped without any prompt. Manual exclusion, that is, the address entry within the address pool range will not be dynamically allocatable.

Default: No manual exclusion addresses are configured.

19.2.10 Configure OPTION82

Mode: Address pool configuration model

Command:option82 circuit-id <circuit-id> Configure circuit-id for option82

Parameter: < circuit-id > string, maximum length is 64.

19.2.11 Clear Allocated Address Table Entry

Mode:EXEC Configuration Mode

Command:clear dhcp server address {[ip-address] | [all]}

An address or all address table entry that have been allocated are delete.

19.2.12 Clear address entry with conflict detected

Mode:EXEC Configuration Mode

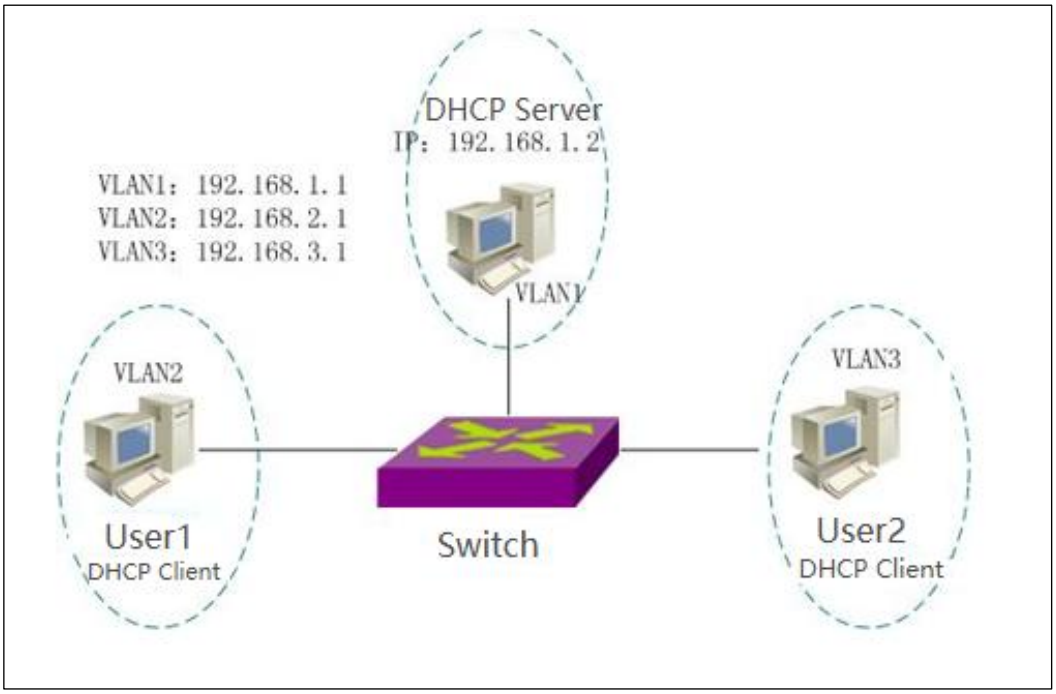
Command:clear dhcp server address conflict {[ip-address] | [all]}

Deleting addresses that are automatically excluded when a conflict is detected. You can delete all conflicting addresses. You can delete a single address that is automatically excluded because of a conflict.

19.3 DHCP SERVER Configuration Example

(1) Configuration

Configure the corresponding address pools for the clients in the three different subnets of vlan1, vlan2, and vlan3, so that the switch as the DHCP server can allocate the IP addresses of the corresponding network segments to the clients in the three subnets.



Switch>en

Switch# configure terminal

Switch(config)#ip dhcp server

Switch(config)# vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Switch(config-vlan)#exit

Switch(config)#ip interface vlan 2

Switch(config)#ip interface vlan 3

Switch(config)#int ge1/2

Switch(config-ge1/2)#sw access vlan 2

Switch(config-ge1/2)#int ge1/3

Switch(config-ge1/3)#sw access vlan 3

Switch(config-ge1/3)#interface vlan2

Switch(config-vlan2)#ip address 192.168.2.1/24

Switch(config-vlan2)#dhcp server listen

Switch(config-vlan2)#interface vlan3

Switch(config-vlan3)#ip address 192.168.3.1/24

Switch(config-vlan3)#dhcp server listen

Switch(config-vlan3)#interface vlan1

Switch(config-vlan1)#dhcp server listen

Switch(config)#dhcp server pool a

Switch(config-dhcp)#range 192.168.2.1 192.168.2.20

```
Switch(config-dhcp)#lease 2 0 0
Switch(config-dhcp)#default-router 192.168.2.1
Switch(config-dhcp)#dns-server 1.1.1.1 2.2.2.2
Switch(config-dhcp)#exclude-address 192.168.2.10
Switch(config-dhcp)#exit
Switch(config)# dhcp server pool b
Switch(config-dhcp)#range 192.168.3.2 192.168.3.20
Switch(config-dhcp)#default-router 192.168.3.1
Switch(config-dhcp)#exit
Switch(config)# dhcp server pool c
Switch(config-dhcp)#range 192.168.1.2 192.168.1.20
Switch(config-dhcp)#default-router 192.168.1.1
Switch(config-dhcp)#exit
```

(2) Verification

show running-config Display Configuration Command

show dhcp server Display global configuration information

show dhcp server pool [pool-name]

Displays the address pool configuration information. Individual address pool information can be displayed.

show dhcp server address Displays the assigned address table entry information.

20. Configuring ACL

In the actual network, the administrator is very concerned about the security of network access. The switch supports ACL filtering to provide network access security. Through the configuration of ACL rules, the switch filters the input data flow according to these rules to realize the network access security.

This chapter describes how to configure ACLs, including the following:

- ACL Resource Library Introduction
- ACL Filtering Introduction
- ACL Resource Pool Configuration
- ACL filtering configuration
- ACL Configuration Example

20.1 ACL Resource Library Introduction

ACL (Access list control) resource library is a collection of multiple groups of access rules. ACL resource library has no function of controlling data forwarding, but is a collection of rules with conflict sorting. After the ACL resource pool is referenced by applications, these applications control the forwarding of data according to the rules provided by the ACL resource. ACLs can be applied to port access filtering, service access filtering, QoS, and so on.

ACL resource library has standard IP rule group (group number 1 ~ 99, 1300 ~ 1999), extended IP rule group (group number 100 ~ 199, 2000 ~ 2699), IP MAC group < group number 700 ~ 799 >, and ARP group (number 1100 ~ 1199); Prioritization of conflicting rules is automatically performed within each set of rules. When a user configures an ACL rule, the system inserts the rule in the appropriate location based on the collation.

During application, when a data packet passes through a port, the switch compares the field in each rule with all corresponding fields in the data packet; when a plurality of rules are completely matched at the same time, the first completely matched rule takes effect; and the matched rule determines whether the data packet is forwarded or discarded. An exact match is one in which the value of a field in the rule is exactly equal to the value of the corresponding field in the packet. A rule will not take the corresponding deny or permit action unless it exactly matches one of the ACL rules.

In a switch, rules within the same group are automatically ordered. The automatic sorting of rules is relatively complex. In the sorting process, the rules with a large range are arranged in the back, and the rules with a small range are arranged in the front. The size of the range is determined by the constraints of the rule; the fewer the constraints of a rule, the larger the range of rule matches, and the more the constraints of a rule, the smaller the range of rule matches. The constraints of the rules are mainly embodied in the wildcard of the address and the number of some non-address fields.Wildcard is a bit string. The IP address is four bytes and the MAC address is six bytes. A bits of '1' means no match is required, and a bits of' 0 'means match is required. Non-address fields refer to protocol type, IP protocol type, and protocol port. These fields also hide a wildcard. Their length is the byte length of the corresponding field, so the length of the same field is uniform, and only the number of fields needs to be calculated. The more bits of Wildcard = '0', the more constraints.

Take port access filtering as an example to illustrate the necessity of rule sorting and the advantages of automatic sorting. If the user needs to refuse the address forwarding with the source address as 10.10, 10.0/16 network segment, and allow the address forwarding with the source address as 192.168, 1.0/24 network segment, the following two rules can be configured:

access-list 1 permit 192.168.1.0 0.0.0.255－Rule 1

access-list 1 deny 10.10.10.0 0.0.255.255 －Rule 2

Rule 1 and Rule 2 for short.

These two rules are in conflict; because the address of rule 1 is contained in the address of rule 2, and one is deny and the other is permit; according to the filtering principle of ACL, different orders have different results. If the above requirement is to be fulfilled, the order of the two rules above must be: Rule 1 comes first and Rule 2 comes last. The switch automatically implements the above sorting function. No matter what order the user configures the above rules, the last order is that rule 1 is in front of rule 2. When a packet with a source address of 192.168 and a 1.1 address is forwarded, the first rule is compared first, and then the second rule is compared. If both rules match, the former rule takes effect (forwarding). If the source address is 10.10 and 10.1, only the first rule matches, then it is discarded (not forwarded).

If there is no sorting, the user may configure Rule 2 first, then Rule 1; Rule 1 is sorted later, and Rule 2 is sorted first.

access-list 1 deny 10.10.10.0 0.0.255.255－Rule 2

access-list 1 permit 192.168.1.0 0.0.0.255－Rule 1

Because the former rule 2 contains the latter rule 1, it is possible that a packet that exactly matches rule 1 will also exactly match rule 2, and rule 2 will take effect every time; it will not meet the requirements of the application.

In the switch, '0.0. 255.255' is wildcard bits, where a bits of '1' means no match is required, and a bits of' 0 'means match is required. It can be seen that the wildcard bits in Rule 2 is' 0.0. 255.255 ', which needs to match two bytes (16 bits); the wildcard bits in Rule 1 is' 0 0.0. 255', which needs to match three bytes (24 bits); So the rule'scope 'of rule 2 is larger, so it's behind. In extended IP, more rule fields need to be considered for sorting, such as IP protocol type, communication port, and so on. Their ordering rules are the same, that is, the more configuration restrictions, the smaller the'scope 'of the rule, and vice versa. The sorting of rules is implemented in the background, and user commands can only be displayed in the order configured by the user.

The filtering fields supported by ACL include source IP, destination IP, IP protocol type (such as TCP, UDP, OSPF), source port (such as 161), and destination port. Users can configure different rules for access control according to different needs.

In a switch, a set of rules can be applied by multiple applications; e.g., a set of rules is referenced by both port access filtering and service access filtering or by both port access filtering.

20.2 ACL Filtering Introduction

ACL filtering is carried out at the input port of the switch, and the filtering of the port is realized by performing rule matching on the data flow input to the port. ACL filtering is handled at the line speed of the switch and does not affect the forwarding efficiency of the data flow.

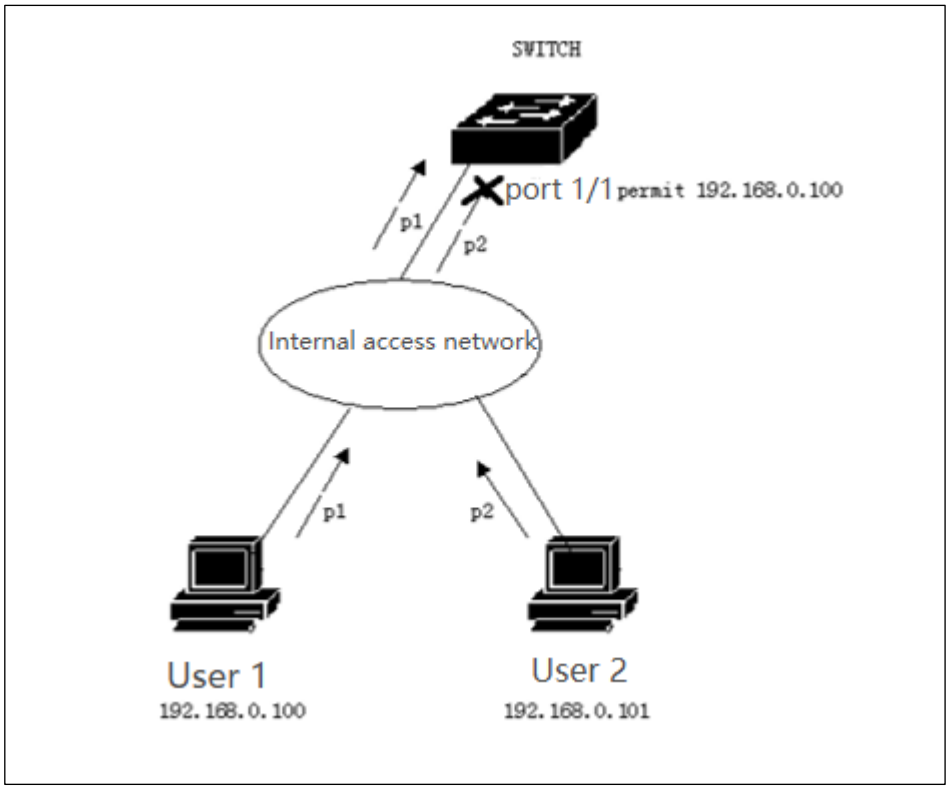
When a port of a switch is not configured with ACL filtering, all incoming traffic through the port will not match the rules and can be forwarded through the port. When a port of a switch is configured with ACL filtering, all input data flows passing through the port will be matched by rules. If the action of the matched rule is permit, the data flow is allowed to be forwarded. If it is deny, the data flow is not allowed to be forwarded and is discarded.

When configuring the ACL filtering of a port, multiple ACL rule groups can be selected for a port. After selection, the group of rules is imported into the CFP of the port. If there is no rule that denies or allows all IP protocol packets in the group of rules, a rule that denies all IP protocols will be added when writing the CFP. When the rules in the ACL repository change, the rules written to the CFP will also change automatically.

For example, if there is only one rule in a set of rules: access-list 1 permit 192.168. 1.0 0.0. 0.255, a rule that denies all IP protocol packets will be hidden by default, and there will actually be two rules imported to the CFP of the port. In traffic filtering, only traffic with a source address from the 192.168, 1.0, to the 192.168 and 1.255 can be forwarded through that port, and all other traffic is filtered out.

For example, there are two rules in the set: access-list 1 deny 192.168. 1.0 0.0. 0.255 and access-list 1 permit any. There is one rule that allows all IP protocol packets, there are no hidden rules, and there are actually two rules that are imported to the CFP of the port. In traffic filtering, only traffic with a source address from the 192.168, the 1.0, to the 192.168, and the 1.255 is filtered out, and all other traffic is allowed to be forwarded.

The following figure shows an example of ACL filtering. Port 1/1 of the switch selects an ACL rule group 1 with only one rule access-list 1 permit 10.10. 10.100. Two users under port 1/1 on the switch want to access the network from that port. The IP address of user 1 is 10.10. 10.100 and the IP address of user 2 is 10.10. 10.101. Only user 1 can access the network through port 1/1 of the switch. User 2 cannot access the network through port 1/1 of the switch. Data flow P1 from user 1 can be forwarded through port 1/1 of the switch, while data flow P2 from user 2 is dropped at port 1/1 of the switch.



When multiple ports are used for ACL filtering, the same ACL rule group can be selected and the same filtering rule can be used.

Whether a set of rules or multiple sets of rules are referenced by a port, they are automatically sorted, even if the sorting between two sets of rules is crossed.

After a user references a set of rules, if the set of rules changes, the port that references the set of rules will automatically respond to the user's configuration; there is no need to reconfigure the reference of the port.

20.3 ACL Resource Pool Configuration

The switch defaults without any rules.

The resource pool in the switch supports four types of ACL rules: standard IP rules, extended IP rules, IP MAC groups, and ARP groups. ACL configuration is described in four categories of rules.

Standard IP rules: Standard IP rules control packet forwarding by source IP address.

Command form:access-list <groupId> {deny | permit} <source>

Parameter description:

groupId: The access control list group numb. Standard IP ACLs support group from 1 to 99 or 1300 to 1999. Deny/permit: If there is an exact match, the packet is denied or allowed to be forwarded.

Deny/permit:If there is an exact match, the packet is denied or allowed to be forwarded.

source：The source IP can be entered in three ways:

1) A. B. C. D wildcard can control IP addresses from one network segment;

2) any equals A. B. C. D 255.255.255.255

3) host A. B. C. D equivalent to A. B. C. D 0.0.0.0

Wildcard: Determines which bits need to be matched. '0' means match is required and' 1 'means no match is required.

Extended IP rules: Extended IP rules are extensions to standard IP rules that control packet forwarding by source IP, destination IP, IP protocol type, and service port.

Command form :access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort] <tcp-flag>

Parameter description:

groupId:Access control list group number. Extended IP ACLs support groups from 100 to 199 or 2000 to 2699.

Deny/permit: If there is an exact match, the packet is denied or allowed to be forwarded.

Protocol:For protocol types above the IP layer, such as TCP, UDP, etc., the corresponding number 6 (TCP) can also be entered. If you do not want to control these protocols, you can enter IP or 0.

Source：The source IP can be entered in three ways:

1) A. B. C. D wildcard can control IP addresses from one network segment;

2) any equals A. B. C. D 255.255.255.255

3) host A. B. C. D equivalent to A. B. C. D 0.0.0.0

srcPort:If the protocol is TCP or UDP, the source port of the data packet can be controlled. The input mode can be some familiar port service names, such as www, or numbers, such as 80.

There are three ways to input the destination IP:

1) A. B. C. D wildcard can control IP addresses from one network segment;

2) any equals A. B. C. D 255.255.255.255

3) host A. B. C. D equivalent to A. B. C. D 0.0.0.0

destPort:If the protocol is TCP or UDP, the destination port of the data packet can be controlled. The input method is the same as that of srcPort.

tcp-flag:For the case where the protocol is TCP. You can control the TCP field matching of the packet. The optional parameters are ack, fin, psh, rst, syn, urg.

IP MAC rules: IP MAC groups can control the source and destination MAC addresses and source and destination IP addresses of IP packets.
Command form:access-list <groupid> {deny | permit} <src-mac> ip <src-ip> <dst-ip>
Parameter description:
groupId:Access control list group number. Extended IP ACLs support groups from 700 to 799.
deny/permit:If there is an exact match, the packet is denied or allowed to be forwarded.
src-mac：Source MAC address.
There are three ways to enter a MAC address:
1) The HHHH. HHHH. HHHH wildcard can control the MAC address from one segment;
2) any is equivalent to HHHH. HHHH. HHHH FFFF. FFFF. FFFF.
3) host A. B. C. D is equivalent to HHHH. HHHH. HHHH 0000.0000.0000
src-ip：Source IP address.
dst-ip：Destination IP address.
There are three ways to enter an IP address:
1) A. B. C. D wildcard can control IP addresses from one network segme nt;
2) any equals A. B. C. D 255.255.255.255
3) 0host A. B. C. D equivalent to A. B. C. D 0.0.0.0
ARP rules: The ARP group can control the operation type, sender MAC and sender IP of the ARP packet.
Command form:access-list <groupid> {deny | permit} arp {arp-type} <sender-mac> <sender-ip>
Parameter description:
groupId:The access control list group numb. Extended IP ACL support groups from 1100 to 1199.
deny/permit:If there is an exact match, the packet is denied or allowed to be forwarded.
arp-type:Refers to any reply request, where any is the type that does not control the ARP packet, reply is the response packet that controls the ARP, and request is the request packet that controls the ARP packet.

The MAC address of the sender of the ARP packet.

There are three ways to enter a MAC address:

1) The HHHH. HHHH. HHHH wildcard can control the MAC address from one segment;

2) any is equivalent to HHHH. HHHH. HHHH FFFF. FFFF. FFFF.

3) host A. B. C. D is equivalent to HHHH. HHHH. HHHH 0000.0000.0000

IP address of the sender of the ARP packet.

There are three ways to enter an IP address:

1) A. B. C. D wildcard can control IP addresses from one network segment;

2) any equals A. B. C. D 255.255.255.255

3) host A. B. C. D equivalent to A. B. C. D 0.0.0.0

List of additional commands:

show access-list [groupId]

Displays a list of the rules configured in the current ACL. If groupId is entered, a list of rules for the current group is displayed; otherwise, a list of all rules is displayed.

no access-list <groupId>

Deletes the specified rule list. All rules for the groupId group.

20.4 ACLTime-based ACL

A time period is used to describe a particular time range. Users may have a need for some ACL rules to take effect at one or more specific times and not be used for message filtering at other times, commonly known as filtering by time period. At this time, the user can configure one or more time periods first, and then refer to the time period by the time period name under the corresponding rule. This rule only takes effect in the specified time period, so as to realize ACL filtering based on time period.

If the time period referenced by the rule is not configured, the system will give a prompt and allow the rule to be created successfully. However, the rule cannot take effect immediately until the user configures the referenced time period and the system time is within the specified time period.

There are two ways to configure the time period:

(1) Configure the relative time period: from a certain hour and a certain minute of a certain day to a certain hour and a certain minute;

(2) Configuration of absolute time period: from a certain hour and a certain minute on a certain day of a certain month in a certain year to a certain hour and a certain minute on a certain day of a certain month in a certain year.

To configure a time-based ACL:

Command	Description	CLI Mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59>	Configure a relative time period containing only time division for the time period	Global Configuration Mode
time-range WORD cycle-time days from <0-6> to <0-6>	Configure a relative time period containing only the day of the week for the time period X	Global Configuration Mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59> days from <0-6> to <0-6>	Configure a relative time period including time division and week for time period X	Global Configuration Mode
time-range WORD utter-time from <2000-2100> <1-12> <1-31> <0-23> <0-59> to <2000-2100> <1-12> <1-31> <0-23> <0-59>	Configure an absolute time period containing year, month, day, and hour for time period X	Global Configuration Mode
no time-range WORD cycle-time	Delete all relative time periods of a certain time period	Global Configuration Mode
no time-range WORD utter-time	Delete all absolute time periods for a certain time period	Global Configuration Mode
no time-range WORD	Delete a time period (including deleting all relative and absolute time periods)	Global Configuration Mode
no time-range	Delete all time period	Global Configuration Mode
show time-range WORD utter-time	Display all absolute time periods for a certain time period	Privileged Mode
show time-range WORD	Display a time period (including all absolute and relative time periods)	Privileged Mode
show time-range	Show all time periods	Privileged Mode
time-acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range WORD	The so-and-so ACL rule applies for a certain time period and takes effect when the ACL is applied on the interface	Global Configuration Mode
no time-acl (<1-99>|<100-199>|<1300-1999>|<2000-	Unapply an ACL rule to a time period or all time period	Global Configuration Mode

2699>|<700-799>|<1100-1199>) time-range (WORD|)		
show time-acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range	Displays all time periods to which the specified ACL rule applies	Privileged Mode
show time-acl all time-range	Displays the time period to which all ACL rules apply	Privileged Mode

It should be noted that:
(1) a plurality of relative time periods are configured for a certain time period, the relationship between the relative time periods is or, and the time period is in an active state when the system time is in any relative time period;
(2) a plurality of absolute time periods are configured for a certain time period, the absolute time periods are in an or relationship, and the time period is in an active state when the system time is in any absolute time period;
(3) If a relative time period and an absolute time period are configured for a certain time period at the same time, the relative time period and the absolute time period are in a relationship of and, and the time period is in an active state only when the system time is in both the relative and absolute time periods;
(4) a maximum of 256 time periods can be defined; a maximum of 256 relative and absolute time periods can be configured for a time period; an ACL rule can apply up to 256 time periods; when an ACL rule associated with a time period is applied to an interface, the time period takes effect.

20.5 ACL filtering configuration

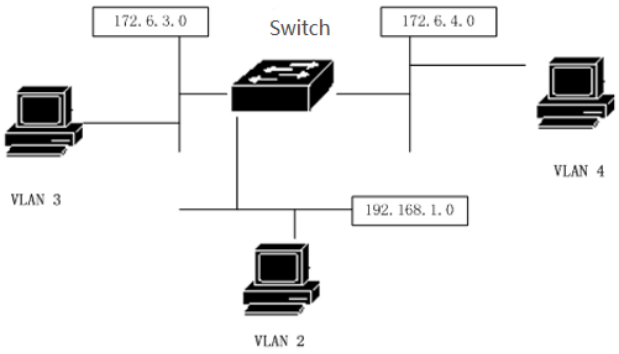
By default, all ports on the switch do not have ACL filtering.
Command list:
access-group <groupId>
Mode: Layer 2 interface configuration mode
Parameters:
GroupId: ACL group number bound to the port
Function: Configure ACL port filtering.

Note: If the above command configuration fails or is not valid, there may be the following reasons: There are too many rules in the ACL group or the hardware resources are exhausted or occupied by other applications.
Displays the ACL port filtering configuration
show acccess-group
Deletes the current port and ACL port filtering related configuration
no acl- group <groupId>

20.6 ACL Configuration Example

A switch is connected to three subnets, ACL is designed, and the blocking source address is the 192.168. The 1.0 network address. While traffic from other network addresses is allowed. 192.168. The 1.0 segment is connected to port 1/1 of the switch.

Configure the following on the switch:




```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config)#interface ge1/1
Switch(config-ge1/1)# switchport mode access
Switch(config-ge1/1)#switchport access vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 3
Switch(config)#interface vlan3
Switch(config-vlan2)#ip add 172.16.3.1/24
Switch(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Switch(config)#access-list 10 permit any
Switch(config)#interface ge1/1
Switch(config-ge1/1)#access-group 10
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#access-group 10
```

20.7 ACL Configuration Troubleshooting

If the ACL configuration fails, there may be the following reasons:

(1) Make sure that all IPs are connected before configuring the access control list, and then add the access control list. This access list blocks IP traffic with a source address of the 192.168. IP traffic with a source address of the 1.0 segment passes through the switch. Note how the subnet complement is written. Use the show access-list command to list the access control list for viewing, and be sure that the source and destination addresses are not written backwards. And then view the access control list. And the default access control list has an implicit deny any statement at the end. If you want the others to pass, you need to add a permit any statement, otherwise they will not pass.

(2) The system is configured with static IP MAC binding.

(3) DHCP SNOOPING protocol is enabled on the current interface.

(4) The system CFP resource is exhausted.

21. Basic TCP/IP Configuration

For a layer 2 switch with network management function, it is necessary to provide basic network configuration for TCP/IP protocol to realize the communication function with other devices.

This chapter mainly includes the following contents:

- Configure VLAN interface
- Configure ARP
- Configure Static Routine
- IP Routing Configuration Example

21.1 Configure VLAN interface

In a switch, each Layer 3 interface is attached to a VLAN, so Layer 3 interfaces are also called VLAN interfaces. The creation and deletion of VLAN interfaces is done manually, and up to 4094 VLANs can be created on the switch, but only up to 32 subnets can be established. The subnet interface can be created according to the user's requirements; the subnet interface can be deleted manually by the user, and can also be deleted along with the deletion of the VLAN where the subnet is located.

Each VLAN interface has a name. The name of a VLAN interface is the string "VLAN" followed by the VLAN ID number. For example, the name of the three-layer interface of VLAN 1 is "vlan1", and the name of the three-layer interface of VLAN 4094 is "vlan4094".

Like ports, VLAN interfaces have administrative and link status. At present, the switch does not provide the configuration of the management state of the VLAN interface. As long as the VLAN interface is created, the management state of the VLAN interface is always UP. The link state of a VLAN interface is related to the port included in the VLAN corresponding to the interface. As long as the link state of a port in the VLAN is RUNNING, the link state of the VLAN interface is RUNNING. If all ports in the VLAN are not RUNNINGing, The link state for that VLAN interface is also not RUNNING.

On a VLAN interface, you can configure an IP address and indicate the network prefix (which can be translated to a netmask) for the segment connected to this interface. Currently, the switch supports only one IP address on one VLAN interface. Before configuring the IP address, the user needs to create a VLAN and add the relevant port to the VLAN. By default, the switch has a VLAN1 interface, and the IP address 10.10 is set on this interface. 10.1/24, the user can also modify the IP address of the VLAN1 interface. Interfaces for VLANs other than VLAN 1 do not have IP addresses set by default.

The commands to configure the IP address of a VLAN interface are shown in the following table:

Command	Description	CLI Mode
Ip interface vlan <2-4094>	Create a VLAN interface	Global Configuration Mode
No Ip interface vlan <2-4094>	Delete a VLAN interface	Global Configuration Mode
ip address <ip-prefix>	Set the IP address on the VLAN interface. The parameters include the IP address of the interface and the network prefix of the connected network segment. If the VLAN interface originally has an IP address, delete the original IP address first, and then set the specified IP address. The format of the parameter is A. B. C. D/M.	Interface Configuration Mode
no ip address [ip-prefix]	Delete the IP address of the VLAN interface. If a parameter is specified, it must be the same as the parameter given during setup or the command is invalid. The format of the parameter is A. B. C. D/M.	Interface Configuration Mode

The commands for viewing the VLAN interface are shown in the following table:

Command	Description	CLI Mode
show interface [if-name]	View the information of VLAN interface, including IP address, MAC address, management status, link status, etc. The parameter is the interface name of the VLAN interface. If no parameter is specified, the information of all ports and VLAN interfaces will be viewed.	Normal mode, privileged mode
show running-config	To view the current configuration of the system, you can view the configuration to the VLAN interface.	Privileged Mode

21.2 Configure ARP

ARP (Address Resolution Protocol) is a protocol that provides a mapping from an IP address to a corresponding MAC address. When a source sends an Ethernet data frame to a destination in the same VLAN, the destination is determined based on the 48-bit Ethernet MAC address, and the destination determines whether to receive the packet based on the destination MAC address of the packet.

It is assumed that hosts A and B in two adjacent network segments communicate through a switch. Before sending data to host B, host A first sends an ARP request message to the interface of the switch directly connected to host A, and then sends a data packet to the interface after receiving an ARP response. After receiving the data packet, the switch first broadcasts an ARP request message to the host B. After receiving the ARP response message from the host B, the switch sends the data packet to the host B.

The switch has an ARP cache, called an ARP table, that holds a record of the mapping of IP addresses to MAC addresses on directly connected networks. Each entry in the ARP table has a lifetime, which is 20 minutes by default. When the switch does not receive an ARP request or response message from the IP address during the lifetime, the ARP entry corresponding to the IP address will be deleted.

This section mainly includes the following contents:

- Configure static ARP
- Configure ARP Binding
- View ARP information

21.2.1 Configure static ARP

There are two different ARP entries in the ARP table, one is static ARP and the other is dynamic ARP. Static ARP is an ARP table entry configured by the user through commands. The system will not automatically refresh and delete it, and the user needs to complete it manually. Dynamic ARP refers to the ARP automatically learned by the system according to the received ARP request or response packet. The system automatically creates and deletes the ARP, and updates and maintains it in real time without user intervention, but the user can manually delete the dynamic ARP table entry.

The switch is not configured with a static ARP entry by default. It should be noted that when a VLAN interface is deleted or the IP of the subnet segment of the interface is changed, the static and dynamic ARP entries in the original subnet segment are deleted.

The commands for configuring static ARP are shown in the following table:

Command	Description	CLI Mode
arp <ip-address> <mac-address>	Configure a static ARP entry. The first parameter is the IP address, which must be within a subnet segment. The second parameter is the MAC address. The MAC address must be a unicast MAC address. The format of the MAC address is a HHHH. HHHH. HHHH, such as 0010.5 CB 1.7825.	Global Configuration Mode
no arp <ip-address>	Deletes the ARP entry. Includes deleting an ARP entry for an IP	Global Configuration Mode

21.2.2 View ARP information

The commands for viewing ARP information are shown in the following table:

Command	Description	CLI Mode
show arp	View the ARP table entry information in the A RP table, including all ARP table entries.	Normal mode, privileg ed mode
show running-config	To view the current configuration of the system, you can view the ARP configuration.	Privileged Mode

21.3 Configure Static Routine

A static route is a user-defined route that causes a packet to traverse a specified path from a source address to a destination address. Packets that cannot be routed can be sent to the default gateway by configuring a static route as the default route.

Static routes are manually configured by an administrator. It is suitable for the network with simple networking structure, and the administrator only needs to configure the static route to make the switch work normally. Static routes do not consume valuable network bandwidth because there are no routing updates.

The default route is also a static route. Simply put, a default route is a route that is used only when no matching route entry is found. That is, the default route is used only when there is no suitable route. In the routing table, the default route appears as a route to the network 00.0.0/0 with a mask of 00.0.0. If the destination of the message is not in the routing table and there is no default route in the routing table, the message is discarded and an ICMP message indicating that the destination address or network is unreachable is returned to the source. A default route is very useful in a network. In a typical network with hundreds of switches, running a dynamic routing protocol may consume a large amount of bandwidth resources. Using default routing can save the time occupied by routing and the bandwidth resources occupied by packet forwarding, which can meet the needs of a large number of users communicating at the same time to a certain extent.

A switch can be configured with multiple static routes to the same destination, but only one of these routes is activated for actual data forwarding. The switch is not configured with static routes by default.

The commands for configuring a static route are shown in the following table:

Command	Description	CLI Mode
ip route <ip-prefix> <nexthop-address>	Set up a static route. The first parameter specifies the segment IP and network prefix length, and the second parameter specifies the next-hop IP address.	Global Configuration Mode
ip route <ip-address> <mask-address> <nexthop-address>	The function is the same as the previous command. The first parameter specifies the IP address of the network se gment, the second parameter specifies the mask of the ne twork segment, and the third parameter specifies a next-hop IP address.	Global Configuration Mode
no ip route <ip-prefix> [nexthop-address]	emoves a static route. The first parameter specifies the network segment IP and network prefix length, and the second parameter specifies the next-hop IP address. Without the second parameter, all routes matching the specified network segment are removed. If there is a second parameter, the route that matches both the specified network segment and the next hop is removed.	Global Configuration Mode
no ip route <ip-address> <mask-address> [nexthop-address]	The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the next-hop IP address. Without the third parameter, all routes matching the specified network segment are removed. If there is a third parameter, the route that matches both the specified network segment and the next hop is removed.	Global Configuration Mode

The commands for viewing the route are shown in the following table:

Command	Description	CLI Mode
show ip route [<ip-address> | <ip-prefix>	To view the information of the activated route, you can select to view all routes, a route, a route of a net work segment, or a static route.	Normal mode, pr ivileged mode
show ip route database	To view information about all routes (both active a nd inactive), select View All Routes.	Normal mode, pr ivileged mode
show running-config	View the current configuration of the system to see the configuration of the static route.	Privileged Mode

instance:

Set the destination network to 200.1.1.0, subnet mask to 255.255.255.0, and next hop to 10.1.1.2. The configuration commands are:

Switch(config)#ip route 200.1.1.0 255.255.255.0 10.1.1.2

or Switch(config)#ip route 200.1.1.0/24 10.1.1.2

Delete a static route with a destination IP address of 200.1.1.0, a subnet mask of 255.255.255.0, and a next hop of 10.1.1.2. The configuration commands are:

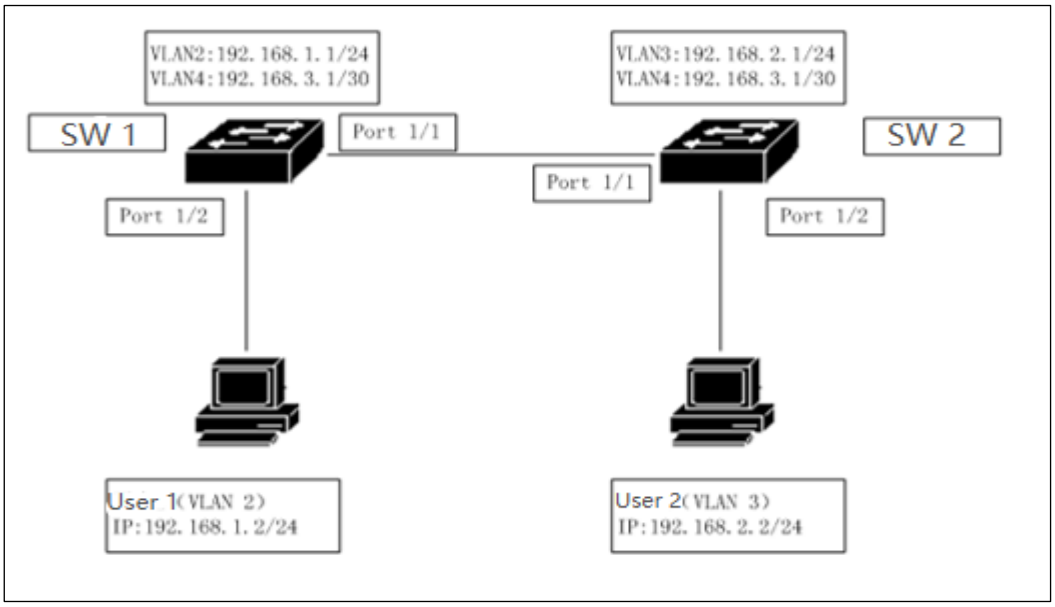
Switch(config)#no ip route 200.1.1.0/24

Or Switch(config)#no ip route 2001.1.0/24 10.1.1.2

Or Switch(config)#no ip route 200.1.1.0 255.255.255.0

Or Switch(config)#no ip route 200.1.1.0 255.255.255.0 10.1.1.2

21.4 TCP/IP Basic Configuration Example



In the figure, Switch 1 is a Layer 2 switch and Switch 2 is a Layer 3 switch

21.4.1 Layer Three interface

Configure the Layer 3 interface for VLAN2 on switch 1 and assign an IP address of 192.168.1.1/24.

The configuration is as follows:

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switch access vlan 2

Switch(config)#ip interface vlan 2

Switch(config)#interface vlan2

Switch(config-vlan2)#ip add 192.168.1.1/24

Verify that User1 is able to ping the Layer 3 interface IP address for VLAN 2 on switch 1.

21.4.2 Static Route

If user 2 wants to access switch 1, it must go through the routing function of switch 2 to access switch 1.

The configuration on switch 1 is as follows:

Switch#config t

Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

The configuration on switch 2 is as follows:

Switch#config t

Switch(config)#ip route 192.168.1.0/24 192.168.3.1

Verify that user 2 can ping generic switch 1.

21.4.3 ARP

Configure static ARP for user 1 to allow only user 1 to access from VLAN 2. Assume that the MAC address of user 1 is 00:00:00:01.

Switch 1 is configured as follows:

Switch#config t

Switch(config)#arp 192.168.1.2 0000.0000.0001

Verify that User1 is able to ping the Layer 3 interface IP address for VLAN 2 on switch 1.

22. Configuring SNMP

The PIXE L3 8T 4XR switch provides SNMP for remote management.. This chapter describes how to configure SNMP, including the following:

This chapter includes the following contents:

- Introduction to SNMP SNMP Configuration SNMP Configuration Example

22.1 Introduction to SNMP

SNMP is a simple network management protocol, which is the most widely used network management protocol. It has five functions: fault management, accounting management, configuration management, performance management, security management. It provides the information format for the communication between the network management application software and the network management agent.

SNMP network management protocol has four elements: management station, management agent, management information base, network management protocol. On the switch, the management agent is the server for the management workstation to access the switch. The information of the management workstation accessing the network management agent is organized in the form of MIB to form a management information base.

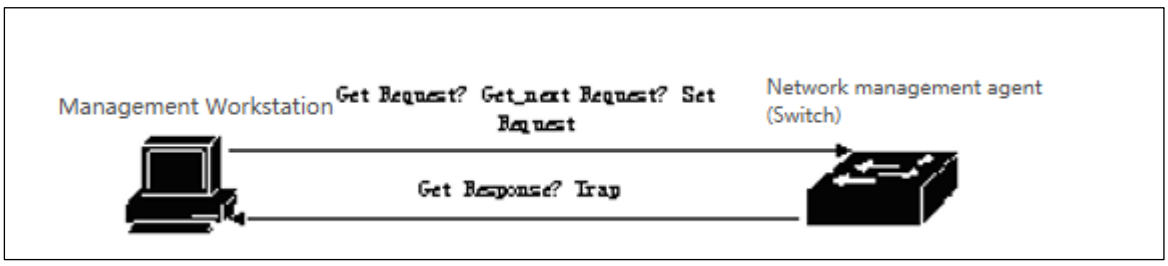
SNMP has three operations: GET, SET, and TRAP. The GET operation enables the management station to get the value of an object in the agent. The SET action enables the management station to set the value of an object in the agent. The TRAP action enables the agent to advertise events to the management station.

TRAP messages are actively sent to the management workstation when an event occurs on the switch. These messages include cold start, warm start, link up and link down of the port, authentication failure of the common entity name, status switching of STP, etc.

At present, there are three versions of SNMP: SNMPV1, SNMPV2 and SNMPV3. The latter version is the upgraded version of the former, with enhanced functions and improved security. The switch supports all three versions of SNMP and can parse all three versions of SNMP protocol packets. When a TRAP message is sent, it may be sent using any one of SNMPV1, SNMPV2, and SNMPV3.

The switch supports RFC, BRIDGE, and proprietary MIB objects, and can be fully managed via SNMP. Some of the MIBs supported by the switch are listed below: RFC 1213, RFC 1493, RFC 1724, RFC 1850, RFC 1907, RFC 2233, RFC 2571, RFC 2572, RFC 2573, RFC 2574, MIBs common to RFC 2575, RFC 2674, etc.

The figure is an example of SNMP protocol interaction between a management workstation and a management agent. The management station can access the switch management agent by sending SNMP messages for Get Request, GetNext Request, GetBulk Request, and Set Request to obtain or set the values of the MIB objects of the switch. The switch management agent sends back an SNMP message of Get Response to the management workstation. When some events occur on the switch, the management agent of the switch actively sends SNMP TRAP messages to the management station.



22.2 SNMP Configuration

SNMP configuration includes community configuration of switch, TRAP workstation, and SNMP system information configuration. By default, the switch has a read-only community named public. The switch can be configured with up to eight communities. The switch is not configured with a TRAP workstation by default.

SNMP commands are shown in the following table:

Command	Description	CLI Mode
snmp community <community-name> {ro | rw}	Configure the community name to access the network management. This is an interactive command. During configuration, the user can input the name of the created community and the read/write permission according to the prompt.	Global Configuration Mode
no snmp community <community-name>	Deletes the specified SNMP community na me.	Global Configuration Mode
snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}	Add or modify the destination to which the SNMP trap is sent. This is an interactive command. The notify name is unique. If the existing name is modified, the trap sending target item can be modified. The host is the destination address for sending trap; the version is sent in the form of snmpV1, snmpV2c or snmpV3. This command is configured with a target port of 162 by default.	Global Configuration Mode
no snmp trap <notify-name>	Deletes the specified SNMP trap.	Global Configuration Mode
snmp system information <contact | location | name> <information-string>	Configure the system information. The configurable system information includes contact, location and name.	Global Configuration Mode
no snmp system information <contact | location | name >	Deletes certain system configuration information.	Global Configuration Mode
show snmp community	Displays all current common body names and the corresponding read and write permission information.	Normal Mode/Privileged Mode
show snmp trap	Displays all the current trap names and the corresponding destination IP addresses and version information sent by trap.	Normal Mode/Privileged Mode
show snmp system information	Displays system information for SNMP settings.	Normal Mode/Privileged Mode

22.3 SNMP Configuration Example

22.3.1 Configuration

Configure a community name named private with read and write permissions.

Configure an SNMP trap named test and send the destination IP as the 10.10. 10.10; the SNMP version used is 1.

The specific content of the contact of the configuration system is: E-mail: networks@acb.com.

The location of the configuration system is Shenzhen.

The name of the configuration system is switch.

The switch is configured as follows:

Switch#config t

Switch(config)#snmp community private rw

Switch(config)#snmp system information contact E-mail:networks@abc.com

Switch(config)#snmp system information location Shenzhen

Switch(config)#snmp system information name switch

23. RMON Configuration

This chapter mainly includes the following contents:

- RMON Introduction
- RMON Configuration
- RMON Configuration Example

23.1 RMON Introduction

RMON (Remote Monitoring) is a standard monitoring specification, which is mainly used to monitor the data traffic in a network segment or even the whole network. It is one of the most widely used network management standards at present. The RMON specification is an extension of the SNMP MIB, so it is also a MIB, the most important enhancement to the MIB II standard. RMON enables SNMP to monitor remote devices more effectively and proactively.

The RMON monitoring system consists of two parts: a probe (agent or monitor) and a management station. RMON agents store network information in RMON MIBs, which are directly implanted in network devices (such as routers, switches, etc.). The management station uses SNMP to obtain RMON data information.

The appliance supports the four most commonly used groups in RMON:

(1)Statistics: Provides statistics for each interface. Most of these objects are counters, which record the information that the monitor collects from the interface.

(2)History group (history): save the data sampled from the specified interface at a fixed time interval.

(3)Alarm group (alarm): sample the specified data of all interfaces at a fixed time interval, compare it with the set threshold, and trigger the corresponding event when the condition is met.

(4)Event group (event): Set the event, and you can choose to log or issue Trap.

RMON Configuration

The RMON command includes the configuration of four groups, View Configuration, and View Data:

Command	Description	CLI Mode
rmon statistics <1-100> (owner WORD|)	Configure the event group parameters for the specified sequence number. This is an interactive command. The configuration user is prompted to enter a sequence number, event type, community name, description, and owner. SN is the number of the event group configuration, and the value range is 1 to 60; The event type can be selected from log, log-trap, none, and trap. When log-trap or trap is selected, the community name must also be specified (the community name configuration is ignored in this dev	Port Configuration Mode
no rmon statistics <1-100>	Cancels the event group configuration for the specified sequence number.	Port Configuration Mode
rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD|)	Configure the history group parameter with the specif ied sequence number for this port. This is an interacti ve command. The configuration user can enter the se quence number, the number of requested buckets, the time interval, and the owner as prompted. SN is the n umber of history group configuration, and the value r ange is 1 to 100; Request Bucket Quantity is the maxi mum number of saved data, and the value range is 1 t o 100; Sampling Interval is in seconds, and the value range is 1 to 3600.	Port Port Configuration Mode

no rmon history <1-100>	Cancels the history group configuration for the specified sequence number.	Port Configuration Mode
rmon alarm <1-60> WORD <1-3600> (absolute|delta) rising-threshold <1-2147483647> <1-60> falling-threshold <1-2147483647> <1-60> (owner WORD|)	Global Configuration Mode	Global Configuration Mode
no rmon alarm <1-60>	Cancels the alarm group configuration for the specified sequence number.	Global Configuration Mode
rmon event <1-60> (log|log-trap WORD|none|trap WORD) (description WORD|) (owner WORD|)	Configure the event group parameters for the specified sequence number. This is an interactive command. The configuration user is prompted to enter a sequence number, event type, community name, description, and owner. SN is the number of the event group configuration, and the value range is 1 to 60; The event type can be selected from log, log-trap, none, and trap. When log-trap or trap is selected, the community name must also be specified (the community name configuration is ignored in this device).	Global Configuration Mode
no rmon event <1-60>	Cancels the event group configuration for the specified sequence number.	Global Configuration Mode
show rmon (statistics|history-control|alarm|event) config	View RMON configuration information. This is an interactive command. Configure users to view objects based on input prompts.	Global Configuration Mode
show rmon statistics-data interface IFNAME|	To view the RMON statistics group data, the configuration user must enter the interface name.	Global Configuration Mode
show rmon history-data interface IFNAME|	To view RMON historical group data, the configuration user must enter an interface name.	Global Configuration Mode

23.2 RMON Configuration Example

Enable statistics group configuration on port ge1/1, sequence number 10, owner tereco.

Enable the collection of historical group data of port ge1/8. The serial number is 2. 80 pieces of data can be saved at most. The sampling interval is 1 minute. There is no owner.

Event with configuration sequence number 1 is logged and has no owner.

Configure the event with sequence number 3 to send Trap. The community name is public and there is no owner.

Enable the alarm group numbered 5 to monitor the number of bytes received by each port. When the number of bytes per half minute is greater than 1000, the Trap alarm will be sent out, and when it is less than 10, the log will be recorded. No owner.

The switch is configured as follows:

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#rmon statistics 10 owner tereco

Switch(config-ge1/1)#exit

Switch(config)#interface ge1/8

Switch(config-ge1/8)#rmon history 2 buckets 80 interval 60

Switch(config-ge1/8)#exit

Switch(config)#rmon event 1 log

Switch(config)#rmon event 3 trap public

Switch(config)#rmon alarm 5 1.3.6.1.2.1.2.2.1.10 30 delta rising-threshold 1000 3 falling-threshold 10 1

24. Cluster Configuration

Switches provide a cluster management feature that enables a single device to manage a group of network devices. This chapter describes how to configure cluster management, including the following:

Introduction to Cluster Management

- Configuration management device
- Configure Member Device
- Cluster Management Display and Maintenance
- Typical Configuration Example of Cluster Management

24.1 Introduction to Cluster Management

24.1.1 Cluster Definition

A cluster is a collection of network devices that can be managed as a single device.

The purpose of cluster management is to solve the problem of centralized management of a large number of scattered network devices.

Advantages of cluster: save public network IP address; simplify configuration and management tasks. The network manager only needs to configure the public network IP address on one switch in the cluster to realize the management and maintenance of other switches in the cluster.

The switch that configures the public network IP address and performs the management function is the command switch, and the other managed switches are the member switches. The command switch and the member switches form a "cluster".

The cluster configures and manages the switches in the cluster through the following three protocols.

- NDP（Neighbour Discovery Protocol）
- NTDP（Neighbour Topology Discovery Protocol）
- Cluster （Cluster Management Protocol）

The working process of the cluster includes the topology collection and the establishment and maintenance of the cluster. The topology collection process and the cluster maintenance process are relatively independent. The topology collection process is started before the cluster is established. The working principle is as follows:

- All devices obtain the information of neighbouring devices through NDP, including the software version, host name, MAC address, port name and other information of the neighbour ing devices.
- The management device collects the device information within the hop count range specified by the user and the connection information of each device through NTDP, and determines the candidate devices of the cluster from the collected topology information.
- According to the candidate device information collected by the NTDP, the management device completes the operation of adding the candidate device to the cluster and removing the member device from the cluster.

The messages of the cluster are all Layer 2 Ethernet messages. See the national standard YDT 1692-2007 Technical Requirements for Cluster Management of Ethernet Switches for the specific format and interaction process.

24.1.2 Cluster Role

According to the different positions and functions of each device in the cluster, different roles are formed. The user can specify the roles through configuration. All the roles are as follows:

1） Command switch:

In a cluster, the only switch that can configure and manage the entire cluster is also the only switch with a public IP address in the cluster.

- Command the switch to create a cluster;
- The command switch discovers and determines a candidate switch by collecting NDP (Neighbour Discovery Protocol, Neighbour Discovery Protocol) and NTDP (Neighbour Topology Discovery Protocol, Neighbour Topology Discovery Protocol) information;
- The command switch controls the maintenance of the cluster and can add a candidate switch to the cluster or delete a member switch from the cluster;
- After the cluster is established, the command switch provides a management channel to the cluster.

2）Member switch：

The managed switch in the cluster.

Member switches are candidates before they join the cluster.

The member switch is not provided with a public network IP;

Management of member switches is done through the command switch agent.

3）Candidate switch：

A switch that has the ability to join a cluster, but has not yet joined any cluster.

A switch must be a candidate before it can become a member.

4）Independent switch：

Switches that are not cluster-capable.

The various roles can be switched according to certain rules:

- When creating a cluster on a candidate device, the user designates the current candidate device as a cluster management device. Each cluster must specify one and only one management device. After the management device is designated, the management device discovers and determines the candidate device by collecting the relevant information. The user can add the candidate device to the cluster through the corresponding configuration.
- After joining the cluster, the candidate device becomes a member device.
- When a member device in a cluster is deleted, it is restored as a candidate device.
- A managed device can only be restored as a candidate when the cluster is deleted.

24.1.3 NDP Introduction

NDP is used to obtain the information of directly connected neighbour devices, including connection port, device name, software version, etc. The working principle is as follows:

- A device running NDP periodically sends NDP messages to its neighbours. The NDP messages contain NDP information (including the device name, software version, connection port, etc. Of the current device) and the aging time of the NDP information on the receiving device. It also receives but does not forward the NDP message sent by the neighbour device.
- The device running NDP will store and maintain the NDP neighbour information table, and create an entry for each neighbour device in the NDP neighbour information table. If a

neighbour is newly found, that is, the NDP message sent by the neighbour is received for the first time, a new entry is added to the NDP neighbour information table; If the NDP information received from the neighbour equipment is different from the old information, the corresponding data item in the NDP table is updated, if the NDP information is the same as the old information, only the aging time is updated, and if the NDP information sent by the neighbour is not received beyond the aging time, the corresponding neighbour table item is automatically deleted.

24.1.4 NTDP Introduction

NTDP is used to collect information about each device and the connections between devices within a network. NTDP provides management devices with information about devices that can be added to the cluster and collects topology information about devices within a specified hop count.

NDP provides adjacency table information for NTDP, and NTDP sends and forwards NTDP topology collection request according to adjacency information and collects NDP information of each device in a certain network range and connection information between each device and all neighbours. After the information is collected, the management device or the network manager can use the information as needed to complete the required functions. When the NDP on the member device finds that the neighbour has changed, it notifies the management device of the change of the neighbour through the handshake message, and the management device can start the NTDP to collect the specified topology, so that the NTDP can reflect the change of the network topology in time.

The management device can collect the topology in the network at regular time, and the user can also start the topology collection once through the manual configuration command. The process for the management device to collect the topology information is as follows:

- The management device sends the NTDP topology collection request message at regular time from the port enabling the NTDP function.
- The device that receives the request message immediately sends a topology response message to the management device, and copies the request message at the port where the NTDP function has been enabled and sends it to the adjacent device; the topology response message contains the basic information of the device and the NDP information of all adjacent devices.
- After receiving the request message, the adjacent device will execute the same operation until the topology collection request message spreads to all devices within the specified hop range.
- When the topology collection request message spreads in the network, a large number of network devices receive the topology collection request and send the topology response message at the same time. In order to avoid network congestion and busy management device tasks, the following measures can be taken to control the spread speed of the topology collection request message.
- After receiving the topology collection request, the device does not immediately forward the topology collection request message, but delays for a certain period of time before forwarding the topology collection request message at the port enabling the NTDP function.
- On the same device, except for the first port, each port that enables the NTDP function will delay a certain time before forwarding the topology collection request message after the previous port sends the topology collection request message.

24.1.5 Cluster management and maintenance

(1) The candidate device joins the cluster

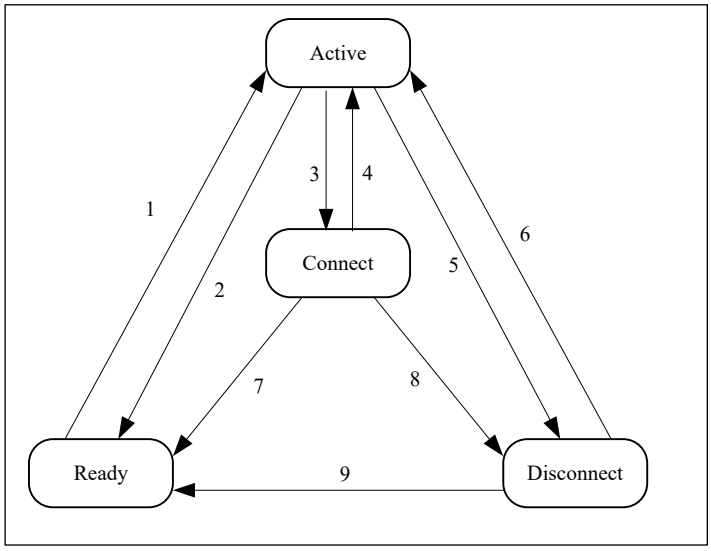
Before establishing a cluster, the user shall first designate a management device. The management device discovers and determines a candidate device through NDP and NTDP protocols, and

automatically adds the candidate device to the cluster. Alternatively, the candidate device can be added to the cluster through manual configuration.

Before establishing a cluster, the user shall first designate a management device. The management device discovers and determines a candidate device through NDP and NTDP protocols, and automatically adds the candidate device to the cluster. Alternatively, the candidate device can be added to the cluster through manual configuration.

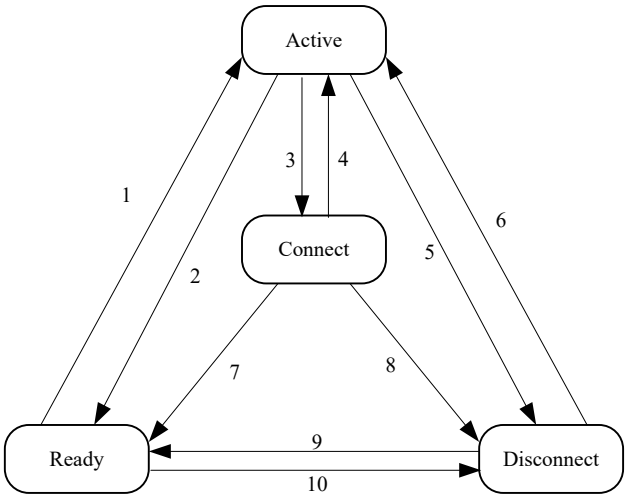
(2) Cluster internal communication

Within the cluster, the management device communicates with the member devices in real time through handshake messages to maintain the connection status between them. The connection status between the management device and the member devices is shown in the following figure.



Command Switch State Transition Diagram

1.Member addition	2、Member deletion	3 No handshake signal is received for three consecutive times
4. Handshake signal is received	5. Recovery request is received	6. Interrupt recovery. Re-registration is passed
7. Member deletion	8. Status maintained beyond the specified time	9. Member deletion



1. Join the cluster	2. Exit the cluster	3. The handshake message is not received for three consecutive times
4.Receive the handshake message	5. Receive the join request	6. Interrupt recovery， Re-registration is passed
7. Quit the cluster	8. Keep the status for more than the specified time or receive the join request message	9. Quit the cluster
10. Restore the configuration		

The command switch collects the basic information of the device and identifies a device as a candidate switch, which is initially in the Ready state.

The operation of remove a member in any state will transition that member switch back to the Ready state and identify it as a candidate switch.

- After a cluster is established successfully and a candidate device joins the cluster to become a member device, the management device saves the state information of the member device locally and identifies the member state as Active, and the member device also saves its own state information locally and identifies its own state as Active.
- The management device and the member device send a handshake message to each other at regular time. After receiving the handshake message from the member device, the management device does not respond and keeps the member device in the Active state; The member device also does not respond and keeps its own state as Active.
- after sending that handshake message to the memb device, if the management device does not receive the handshake message sent by the member device within three times of the time interval for sen the handshake message, transferring the state of the member device stored locally from Active to Connect; Similarly, if the member device does not receive the handshake message sent by the management device within three times of the handshake message sending time interval after sending the handshake message to the management device, its own state will also be transferred from Active to Connect.
- if the management device receives a handshake message or a management message sent by the member device in the Connect state within the valid retention time, the state of the member device is transferred back to Active, otherwise, the state of the member device is

transferred to Disconnect, and at this time, the management device considers that the member is disconnected; If the member device in the Connect state receives the handshake message or management message sent by the management device within the valid retention time, it will migrate its own state to Active, otherwise it will migrate to Disconnect.

- When the interrupted communication between the management device and the member device is restored, the member device in the Disconnect state will rejoin the cluster. After the join is successful, the state of the member device in the management device and the local state will be restored to Active.

If a topology change is found, the member device also transmits the change information to the management device through a handshake message.

24.1.6 Management VLAN

The management VLAN limits the scope of cluster management. By configuring the management VLAN, the following functions can be realized:

- The management messages of the cluster (including NDP, NTDP and handshake messages) will be confined in the management VLAN and isolated from other messages, which increases the security.
- The internal communication between the management device and the member device is realized through the management VLAN.

Cluster management requires that the ports connected between the management device and the member/candidate device, including the cascade ports (when the candidate device is connected to the management device through another candidate device, the ports connected between the candidate devices are called cascade ports), must allow the management VLAN to pass through. Therefore:

- If the port does not allow the management VLAN to pass through, the device connected to the port cannot join the cluster. Therefore, before the cluster, it should be determined that the port connecting the candidate device and the management device, including the cascade port, allows the management VLAN to pass through.
- Only when the default VLAN ID of the port where the management device and the member/candidate device are connected and the default VLAN ID of the cascade port are the management VLAN, the message of the configuration management VLAN is allowed to pass without a tag, otherwise the message of the management VLAN must pass with a tag.

For information about VLANs, see Configuring VLANs.

24.2 Introduction to Cluster Configuration

Before configuring the cluster, users need to define the roles and functions of each device in the cluster, configure relevant functions, and plan the communication with the devices in the cluster.

Configuration Task	
Configuration management device	Enables NDP functionality for the system and port
	Configure NDP parameter
	Enables NTDP functionality for the system and port
	Configuring NTDP Parameters
	Configure manual collection of NTDP information
	Enable the cluster function
	Establish cluster
	Configure the interaction of members within the cluster
	Configure cluster member management
Configure Member Device	Enable NDP function of system and port
	Enable NTDP function of system and port
	Configure manual collection of NTDP information
	Enable the cluster function
Configure cluster members to access each other	

Notice:

After the cluster is established, after the NDP or NTDP function is turned off on the management device and the member device, the cluster will not be dissolved, but the normal operation of the established cluster will be affected.

24.3 Configuration management device

24.3.1 Enables NDP functionality for the system and port

Command	Description	CLI Mode
ndp global enable	Enable the global NDP function. Global shutdown by default.	Configuration Mode
ndp enable	Enables the NDP function of the port. All ports are closed by default.	Interface Configuration Mode

Notice:

- NDP must be enabled for both the global and port functions for NDP to function properly.
- The NDP feature does not support aggregated ports.
- In order to prevent the management device from collecting the topology information of the device that does not need to join the cluster during topology collection and adding it to the cluster, it is recommended to disable the NDP function on the port connected to the device that does not need to join the cluster.

24.3.2 Configure NDP parameter

Command	Description	CLI Mode
Ndp aging-timer <aging-time>	Configure the aging time of the NDP message sent by the device on the receiving device. The default is 180 seconds	Configuration Mode
ndp hello-timer <hello-time>	Configure the time interval for sending N DP message. Default is 60 seconds.	Configuration Mode

Notice:
Generally, the aging time of the NDP message on the receiving device cannot be less than the NDP sending time interval, otherwise it will cause the instability of the NDP port neighbour information table.

24.3.3 Enable NTDP functionality for system and interface

Command	Description	CLI Mode
ntdp global enable	Enables global NTDP functionality. Globally off by default.	Configuration Mode
ntdp enable	Enables the NTDP function of the port. All ports are closed by default.	Interface Configuration Mode

Notice:

- Both global and port NTDP functions must be enabled for NTDP to work.
- NTDP feature does not support aggregated ports.
- In order to prevent the management device from collecting the topology information of the device that does not need to join the cluster during topology collection and adding it to the cluster, it is recommended to disable the NTDP function on the port connected to the device that does not need to join the cluster.

24.3.4 Configuring NTDP Parameters

Command	Description	CLI Mode
ntdp hop <hop-value>	Configures the scope of the topology collection. By default, the farthest device in the collected topology has a maximum hop count of 3 from the topology collection device.	Configuration Mode
ntdp timer <interval-time>	Configure the time interval for the scheduled topology collection. The default is 1 minute.	Configuration Mode
ntdp timer hop-delay <time>	Configure the waiting time of the device to be collected before the first port forwards the topology collection request message. The default is 200 milliseconds.	Configuration Mode
ntdp timer port-delay <time>	Configure the port delay time for the curre nt device to forward topology collection re quests. The default is 20 milliseconds.	Configuration Mode

24.3.5 Configure manual collection of NTDP information

After the cluster is established, the management device will periodically collect the topology information. In addition, users can manually collect NTDP information through configuration at any time (regardless of whether the cluster is established or not), and initiate a NTDP information collection process, so as to more effectively manage and monitor devices in real time.

Command	Description	CLI Mode
ntdp explore	Collect topology information manually once.	Normal mode, privileged mode

24.3.6 Enable cluster function

Command	Description	CLI Mode
cluster enable	Enable the cluster function. The default clustering feature is turned off.	Configuration Mode

24.3.7 Set up a cluster

The management VLAN limits the scope of cluster management. By configuring the management VLAN, the following functions can be realized:

- The management messages of the cluster (including NDP, NTDP and handshake messages) will be confined to the management VLAN and isolated from other messages, which increases the security.
- The internal communication between the management device and the member device is realized through the management VLAN.

Command	Description	CLI Mode
cluster management-vlan <vlan-id>	Specifies the management VLAN . The default management VLAN is VLAN1.	Configuration Mode

Notice:

If the current device is in the cluster, it is not allowed to modify the management VLAN.

Not in cluster:

1) Check whether the VLAN exists. If there is no direct failure, proceed to the next step.

2) Check all the interfaces again. If the VLAN where the interface is located and the management VLAN are not the same VLAN, turn on the global switches of NDP and ntdp, turn off and clear them, and then turn them on again.

3) Find the three-layer interface of the VLAN to be configured. If it is not found, create a new three-layer interface corresponding to the VLAN. If the new creation fails, the management VLAN is configured successfully. You can NDP and ntdp, but you cannot join the cluster.

4) Set the mac of the current three-layer interface as dev _ ID. If the VLAN is set successfully but the new three-layer interface fails, use the mac of vlan1 as dev _ ID.

If the management VLAN has been configured, but the user directly deletes the VLAN in the VLAN database, the management VLAN will be automatically set to vlan1, and the global switches of NDP, ntdp and cluster that have been turned on will be turned off and cleared accordingly.

Before establishing the cluster, the user must first set the private IP address range used by the member devices in the cluster. When a candidate device is added, the management device dynamically allocates a private IP address that can be used within the cluster range and sends it to the candidate device for communication within the cluster, so as to realize the management and maintenance of the member devices by the management device

Command	Description	CLI Mode
cluster ip-pool <IP/MASK>	Configure the private IP address range used by the member devices in the cluster on the device to be set as the management device.	Configuration Mode

Notice:

- The IP address of the VLAN interface of the management device and the member device and the cluster address pool cannot be configured in the same network segment, otherwise the cluster will not work properly.
- It can be configured only when the device is not in the cluster.
- searching whether a corresponding three-layer port exists by using the management VLAN, and directly returning failure if the corresponding three-layer port does not exist. (The device cannot be used as a cluster command switch.) If there is a three-layer interface, configure the base address of IP-POol to the three-layer interface. If the configuration fails, the IP-POol configuration also fails.

By default, the device is not a management device, and the cluster is established:

Command	Descriptian	CLI Mode
cluster build <name>	Manually create a cluster, configure the curren t device as a management device, and assign a cluster name.	Configuration Mode
cluster auto-build <name>	Cluster is automatically established. The auto-clustering feature automatically joins all candi date devices discovered within a specified hop count to the cluster created.	Configuration Mode
cluster delete <name>	Delete the cluster.	Configuration Mode
cluster stop auto-add member	In the automatic cluster configuration, stop automatically joining the member switches. This action will only stop new devices from joining. Devices that have already joined the cluster will remain in the cluster.	Configuration Mode

Notice:

- The user can only specify the management VLAN before establishing the cluster. After the device has joined the cluster, the user cannot modify the management VLAN. If the management VLAN needs to be changed after the cluster is established, it is necessary to delete the cluster on the management device, re-designate the management VLAN, and finally re-establish the cluster.
- For security reasons, it is recommended that you do not configure the management VLAN as the default VLAN ID for the port where the management device connects to the member device and for the cascade port.
- only when the default VLAN IDs of the ports connected with the management device and the member device and all the cascaded ports are the management VLAN, the message of the management VLAN can be allowed to pass without a label, otherwise, the ports connected with the management device and the member device and all the cascaded ports must be configured to allow the message of the management VLAN to pass with a label, Refer to VLAN for specific configuration.
- The private IP address range of member devices in the cluster can be configured only when the cluster has not been established, and can only be configured on the management device. If the cluster is already established, the system does not allow the IP address range to be modified.

24.3.8 Configure intra-cluster member interaction

Within the cluster, the management device communicates with the member devices in real time through the handshake message to maintain the connection status between them. The time interval for sending the handshake message and the effective retention time of the device can be configured on the management device. The configuration will take effect for all member devices in the cluster at the same time.

Command	Description	CLI Mode
cluster timer <interval-time>	Configure the time interval for sending the handshake message. Default is 10 seconds	Configuration Mode
cluster holdtime <hold-time>	Configure the effective retention time for the device. Default 60 second	Configuration Mode

24.3.9 Configure cluster member management

The user can manually specify the candidate device to be added to the cluster on the management device, or manually delete the specified member device in the cluster. The cluster member join/delete operation must be performed on the management device, otherwise an error message will be returned

Command	Description	CLI Mode
cluster add member mac-address <mac-address>	The candidate device is added to the cluster.	Configuration Mode
cluster delete member mac-address <mac-address>	Remove the member device from the cluster.	Configuration Mode

24.4 Configure Member Device

24.4.1 Enables NDP functionality for the system and port

See Enabling NDP Functions for Systems and Port

24.4.2 Enables NTDP functionality for the system and port

See Enabling NTDP Functions for Systems and Port

24.4.3 Configure manual collection of NTDP information

See Configuring manual collection of NTDP information

24.4.4 Enable cluster function

See Enabling Cluster Features

24.5 Configure access to cluster member

After NDP, NTDP and cluster functions are configured correctly, the member devices in the cluster can be configured, managed and monitored through the management device. You can switch to the specified member device operation interface on the management device to perform configuration management on the member device.

Command	Description	CLI Mode
cluster switch-to member <member-number>	Switch from the management device operation interface to the member device operation interface	Normal mode, privileged mode

Notice:

Switching between the cluster management device and the member device uses the Telnet connection. Please pay attention to the following during the switching:

- Before executing the handover, the peer device needs to execute the "telnet server enable" "command to enable the telnet function, or the handover will fail.
- Switch from the management device to the member device. If the member number n does not exist, an error message will be displayed.
- If the Telnet user of the device requested to log in is full, the switchover will fail.

24.6 Cluster Management Display and Maintenance

Command	Description	CLI Mode
show ndp[interface <ifname>]	Display NDP configuration information	Normal mode, privileged mode
reset ndp statistics [interface <ifname>]	Clear NDP Statistics	Configuration View
show ntdp	Display system NTDP information	Normal mode, privileged mode
show ntdp device-list	Display device information collected by NTDP	Normal mode, privileged mode
show ntdp single-device mac-address <mac-address>	Displays NTDP details for the specified device	Normal mode, privileged mode
show cluster	Displays the status and statistics of the cluster to which the device belon	Normal mode, privileged mode
show cluster topology	Display cluster topology information	Normal mode, privileged mode
show cluster candidates [mac-address <mac-address>]	Display candidate device information	Normal mode, privileged mode
show cluster members [<member-number>]	Displays cluster member information	Normal mode, privileged mode

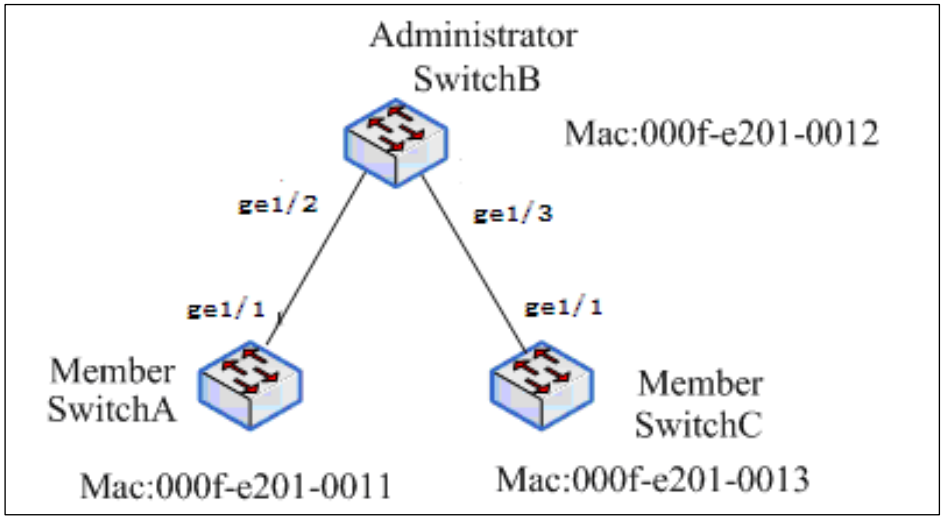
24.7 Typical Configuration Example of Cluster Management

(1) Networking requirements

A clust of three switches, ABC, has a management VLAN of VLAN 10. Switch B is the Administrator; Switch A and Switch C are the Members.

The base address IP of the entire cluster address pool is a 10.0. The 0.1 supports 8 devices.

(2) Networking diagram



(3) Configuration steps:

Configure member device Switch A

Configure the management VLAN.

[SwitchA] cluster management-vlan 10

[SwitchA] interface ge1/1

[SwitchA-ge1/1] switch access vlan 10

Enable the global NDP function and the NDP function on port ge1/1.

[SwitchA] ndp global enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ndp enable

Enable global NTDP function and NTDP function on port ge1/1.

[SwitchA] ntdp global enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ntdp enable

。# Enable the cluster function.

[SwitchA] cluster enable

Configure member device Switch C

Since the member devices have the same configuration, the configuration of Switch C is similar to that of Switch A, and the configuration process is omitted.

Configure member device Switch B

Configure the management VLAN.

[SwitchB] cluster management-vlan 10

[SwitchB] interface ge1/2

[SwitchB-ge1/2] switch access vlan 10

[SwitchB] interface ge1/3

[SwitchB-ge1/3] switch access vlan 10

 # Enable global NDP and NTDP functions, and respectively enable NDP and NTDP functions on ports ge1/2 and ge1/3.

[SwitchB] ndp global enable

[SwitchB] ntdp global enable

[SwitchB] interface ge1/1

[SwitchB-ge1/2] ndp enable

[SwitchB-ge1/2] ntdp enable

[SwitchB] interface ge1/3

[SwitchB-ge1/3] ndp enable

[SwitchB-ge1/3] ntdp enable

Configure the aging time of the NDP message sent by the device on the receiving device to be 200 seconds.

[SwitchB] ndp timer aging 200

Configure the time interval for sending NDP message as 70 seconds.

[SwitchB] ndp timer hello 70

The maximum number of hops collected by the configuration topology is 2 hops.

[SwitchB] ntdp hop 2

Configure the delay time for the first port of the collected device to forward the topology collection request message to be 150ms.

[SwitchB] ntdp timer hop-delay 150

Configure the delay time of forwarding the topology collection request message on other ports of the collected device to be 15ms.

[SwitchB] ntdp timer port-delay 15

Configure the time interval for topology collection to be 3 minutes.

[SwitchB] ntdp timer 3

 # Enable the cluster function.

[SwitchB] cluster enable

Configure the private IP address range of member devices as 10.0 0.1 ~ 10.0 0.9.

[SwitchB] cluster ip-pool 10.0.0.1 8

Configure the current device as a management device and establish a cluster named ABC. Members automatically join the cluster.

[SwitchB] cluster autobuild abc

When you have joined all the switches you want to join, you can turn off the automatic joining cluster function.

[SwitchB]cluster stop auto-add member

25. SNTP Configuration

This chapter includes the following contents:

- Introduction
- Configuring SNTP
- Show SNTP

25.1 Introduction to SNTP

At present, the Internet generally adopts a communication protocol to realize network time synchronization, namely NTP (Network Time Protocol), and another protocol is a simplified version of the NTP protocol. SNTP (Simple Network Time Protocol).

NTP protocol can span a variety of platforms and operating systems, with very sophisticated algorithms, so it is almost not affected by network latency and jitter, and can provide 1-50ms accuracy. NTP also provides an authentication mechanism with a high level of security. However, the NTP algorithm is complex and has high requirements for the system.

SNTP (Simple Network Time Protocol) is a simplified version of NTP. When it is implemented, a simple algorithm is used to calculate the time, and the performance is high. And the accuracy can generally reach about 1 second, which can basically meet the needs of most occasions.

Since the SNTP message is completely consistent with the NTP message, the SNTP Client implemented by the switch is fully compatible with the NTP Server.

25.2 Configuring SNTP

25.2.1 Default SNTP settings

Item	Default Value
SNTP Status	Disable turns off the SNTP service
NTP Server	nothing
Interval of synchronization time of SNTP	1800 second
Local Time Zone	GMT

Turning SNTP on and off

The configuration is as follows:

Switch# configure terminal

Enter global configuration model

Switch(config)# sntp enable

Open SNTP

Switch(config)# sntp disable

SNTP off

25.2.2 Configure SNTP Server Address

Since the SNTP message is completely consistent with the NTP message, the SNTP Client is fully compatible with the NTP Server. Since there are many NTP Servers on the network, you can select one with less network latency as the NTP Server. On the switch.

The specific NTP server address can be obtained by logging in the http://www.time.edu.cn/ or http://www.ntp.org/. E.g. 192.43, 244.18 (time. NIST. Gov)

The switch can be configured with three server addresses at most. The switch uses the first Server address to synchronize the time. If the synchronization fails, the switch uses the second Server address, and so on.

The configuration for adding a Server address is as follows:

Switch# configure terminal

Enter global configuration model

Switch(config)# sntp server 210.72.145.44

Add the SNTP server IP. If the switch already has three Server addresses, the addition will fail. You need to delete the addresses before adding them

The configuration for deleting the Server address is as follows:

Switch(config)# no sntp server

Delete all Server addresses

Switch(config)# no sntp server 210.72.145.44

Delete a Server address for

25.2.3 Configure the interval of SNTP synchronization clock

The SNTP Client needs to synchronize the clock with the NTP Server periodically in order to synchronize the clock.

The configuration is as follows:

Switch# configure terminal

Switch(config)# sntp interval 60

Set the interval of the timing synchronization clock, in seconds, from 60 seconds to 65535 seconds. The default value is 1800 seconds, which is set to 60 seconds here.

Switch(config)# no sntp interval

The interval of the timing synchronization clock is restored to the default of 1800 second

25.2.4 Configure the local time zone

The time obtained after communication through the SNTP protocol is Greenwich Mean Time (GMT). In order to prepare for hunting the local time, it is necessary to set the local area to adjust the standard time. By default, the local time zone of the switch is set to Greenwich MeanTime

The configuration is as follows:

Switch# configure terminal

Switch(config)# sntp time-zone -0

Set the local time zone to GMT

Switch(config)# no sntp time-zone

Local time zone reverts to GMT

25.3 Information display of SNTP

The configuration is as follows:

Switch# show sntp

Switch# show running-config

26. Configuring PTP

This chapter includes the following contents:

- Introducing PTP
- Configuring PTP

26.1. Introducing PTP

PTP: Precision Time Protocol, with the continuous increase and development of network technology, especially Ethernet is more and more widely used in measurement and control systems, the computer and network industry is also committed to solving the problem of insufficient timing synchronization capability of Ethernet, in order to reduce the use of other technologies. Uch as IRIG-B. Therefore, a software-based Network Time Protocol (NTP) has been developed to improve the timing synchronization ability among network devices.

PTP is suitable for use in distributed network communication systems that support multicast messaging, such as EtherNet. Support for unicast messages is also provided. The protocol supports multiple transport protocols, such as UDP/IPv6, Layer-2 EtherNet, and DeviceNet. The protocol uses short frame transmission, and the data frame is less, the algorithm is simple, the use of network resources is less, and the requirement for computing performance is low, so it is suitable for application on low-end equipment.

The IEEE 1588 standard has two versions, Version 1 and Version 2.

Version 1 was released at the end of 2002, and the latest version of Version 2 is IEEE1588-2008, which provides all the functions of Version 1 and aims at the shortcomings of Version 1. Improvements have been made.

Clock synchronization implemented by PTP protocol is mainly divided into two steps:

1.establish a synchronous system, namely establishing a master-slave synchronous system in that whole synchronous system through an optimal mast clock algorithm;

2.in that synchronization process, the local clock is calculated and synchronize by exchanging PTP protocol messages.

26.2. Configuring PTP

26.2.1. PTP Settings

item	Default Value
PTP status	Disable Turn off the PTP services

Turn PTP on and off

The configuration is as follows:

Switch# configure terminal

Enter global configuration model

Switch(config)#ptp tc enable

Turn on SNTP

Switch(config)#no ptp tc enable

Turn off PTP

Default: 2

26.2.2. Configure the protocol version of the interface

Mode: interface configuration mode

Command: IP IGMP version < version >

Configure the protocol version of the interface

Command: no IP IGMP versionl

The protocol version of the recovery interface is the default value

Parameter: < version > indicates the IGMP version number used, which is an integer number between 1 and 3.

Default: 3

26.3. IGMP configuration

(1) configuration

IGMP generally works together with multicast routing protocol (eg: PIM-SM). See PIM-SM configuration example. Starting multicast function (IP multicast routing) and PIM-SM protocol (IP PIM spark mode) of interface will automatically start corresponding IGMP protocol without configuring IP IGMP command separately. When receiving the multicast on demand service flow, you can view the corresponding IGMP group information and interface status.

When the source host and the receiving host are in the same subnet, the multicast data flow does not need to be forwarded across network segments, and the three-layer multicast routing is unnecessary, IGMP protocol and IGMP snooping can be started separately to realize multicast in the subnet. Note that the PIM-SM protocol must be started when writing the hardware table of layer 3 multicast. :

Switch# configure terminal

Switch(config)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.1/24

Switch(config-vlan2)#ip igmp

Switch(config-vlan2)#ip pim sparse-mode passive

Switch(config-vlan2)#interface ge1/1

Switch(config-ge1/1)#switch access vlan 2

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switch access vlan 2

Switch(config-ge1/2)#interface ge1/3

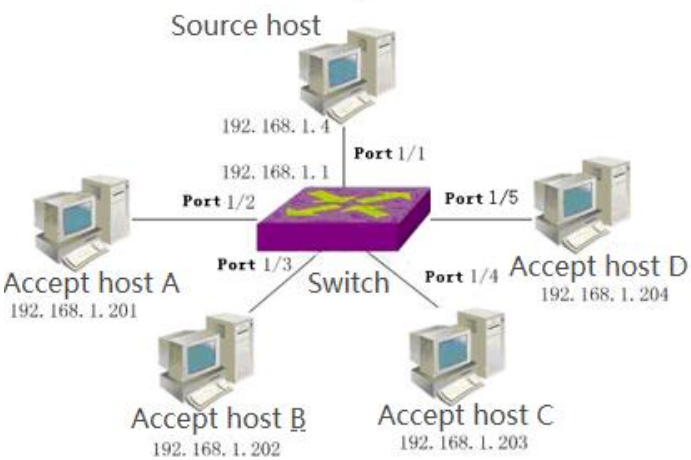
Switch(config-ge1/3)#switch access vlan 2

Switch(config-ge1/3)#interface ge1/4

Switch(config-ge1/4)#switch access vlan 2

Switch(config-ge1/4)#interface ge1/5

Switch(config-ge1/5)#switch access vlan 2



(2) verification

Use the following command to view IGMP informat

show ip igmp group

show ip igmp interface

27. Configuring IGMP

This chapter mainly includes the following content：

- IGMP introduction
- IGMP configuration
- IGMP configuration example

27.1. IGMP introduction

IGMP (Internet Group Management Protocol) is a part of multicast technology. It runs between the host and its directly connected multicast router. On the one hand, the host reports the multicast group it wants to join or leave to the local router. On the other hand, the multicast router can periodically query whether the local host is in the active receiving state for a specific group. IGMP protocol currently has three versions, version 1 (rfc1112), version 2 (rfc2236) and version 3 (rfc3376). IGMP is based on the query response mode. The multicast router uses the query message cycle to query whether the host in the subnet has a specific group it wants to receive. The host uses the report message to notify the local router of the multicast group it wants to join or leave, that is, the membership report. When the host wants to join a specific group, it does not need to wait for the periodic query message, and can immediately send the group membership report to the router. When the router queries the membership of the host in the subnet, the host uses the suppression mechanism to send the report message by delaying a random value between 1 and 10 seconds. When receiving the same group report message from other hosts, the host suppresses the sending of its own group member report, so as to reduce the IGMP traffic in the subnet. When there are multiple routers in the subnet, it is necessary to compare the IP addresses to select one as the inquirer to avoid too many IGMP query messages in the subnet. Version 1 only supports query and report. When a group member leaves, the multicast router will stop forwarding the multicast data stream only after waiting for the group information to timeout. The inquirer depends on other protocols for election. Version 2 supports the immediate departure of group members by adding a departure message. When the last group member leaves the group, it sends a departure message to the router, and the router sends a specific group query message to determine whether there are other receiving hosts in the subnet. When the corresponding group membership message is still not received after sending the configured number of retransmissions, the group becomes invalid, Stop forwarding multicast data stream. Version 2 effectively reduces the departure delay through the departure mechanism. Version 2 provides a searcher election mechanism. When the general query message is received by other routers in the subnet, they select the one with the smallest IP address as the searcher by comparing their own IP address, and start a timer. Each time the query message is received, the timer resets. When the timer terminates, the new election process begins. In order to adjust the response time of the suppression mechanism of the host, the maximum response time field is added in the message of version 2. The inquirer can control the suppression response time of the host by adding this value to the query message. When the host receives the query message, it uses the maximum response time to generate a delay with the machine to start the timer, When the same group membership message of other hosts is received within this delay time, its own report message is inhibited. Version 3 supports specific source multicast. Query messages are divided into general query, specific group query and specific group specific source query; The report message expands the original group address field into group record entries. Each group record contains the group address and its corresponding source address list. Whether to join a specific source or not is distinguished by the group record type. Igmpv3 cooperates with pim-ssm to realize source specific multicast. SPT is directly established from source to receiver without the need of convergence point RP.

27.2. IGMP configuration

IGMP functions are mostly related to interfaces. Configure the corresponding parameters and timer values of each interface and carry out relevant configuration in interface mode。

IGMP configuration includes：

- Start IGMP function of interface
- Configure the group filter access control list for the interface
- Configure the access control list filtered by the interface leaving the group
- Number of specific group queries for the configuration interface
- Configure the specific group query interval of the interface
- Configure the non querier timer time of the interface
- Configure the query timer interval of the interface
- Configure the maximum response time of the interface
- Configure interface parameters
- Configure the protocol version of the interface

27.2.1 Start IGMP function of interface

Mode: interface configuration mode

Command: IP IGMP Open IGMP protocol on the interface

Command: no IP IGMP Turn off IGMP protocol on the interface

Default: do not open IGMP protocol;

Use this command to start the interface to send and receive IGMP protocol messages. If the IP multicast routing command has started the multicast function support in the global configuration mode, the IGMP protocol function of the corresponding interface will be automatically started when the IP PIM spark mode command starts the PIM SM Protocol function in the interface configuration mode. Similarly, in the interface configuration mode, the no IP PIM spark mode command will automatically turn off the IGMP protocol function of the corresponding interface.

27.2.2 Configure the group filter access control list for the interface

Mode: interface configuration mode

Command: IP IGMP access group {< ACL ID > | < ACL name >}

Configure the group filter access control list for the interface

Command: no IP IGMP access group

Delete the group filter access control list for this interface

Parameter: < ACL ID > indicates the standard access control list number, which is an integer number between 1 and 99< ACL name > is the standard access control list name. Use ACL to filter the multicast address table learned by the interface. See the Command Reference Manual for ACL configuration details.

Default: group filtering ACL is not configured

27.2.3 Configure the access control list filtered by the interface leaving the group

Mode: interface configuration mode

Command: IP IGMP immediate leave group list {< acl-id1 > | < acl-id2 > | < ACL name >}

Configure the access control list filtered by the interface leaving the group

Command: no IP IGMP immediate leave

Delete the outgoing group filter access control list of this interface

Parameter: < ACL Id1 > indicates the standard access control list number, which is an integer number between 1 and 99< Acl-id2 > is the number of the extended range of the standard access control list, which is an integer number between 1300 and 1999< ACL name > is the standard access control list name. The ACL can be used to filter the multicast addresses that need to be filtered when the interface receives the departure messages of version 2 and version 3. Refer to the Command Reference Manual for ACL configuration details.

Default: leave group filtering ACL is not configured

27.2.4 Number of specific group queries for the configuration interface

Mode: interface configuration mode

Command: IP IGMP last member query count < count >

Configure the number of interface specific group queries

Command: no IP IGMP last member query count

The number of queries for a specific group of the recovery interface is the default value

Parameter: < count > indicates the number of specific group queries or specific source queries that need to be sent when receiving the departure message, which is an integer between 2-7. It is considered that the group has no receiving host until the group report message is not received during this period.

Default: 2

27.2.5 Configure the specific group query interval of the interface

Mode: interface configuration mode

Command: IP IGMP last member query interval < interval >

Configure the specific group query interval of the interface

Command: no IP IGMP last member query interval

The specific group query interval of the recovery interface is the default value

Parameter: < interval > indicates the time interval of a specific group query or a specific group source query. It is an integer between 1000-25500, in milliseconds; When a departure message is received, it is necessary to send a specific group or a specific source query of a specific group for multiple times. This command configures the sending interval of multiple query messages. Until no group report message is received after multiple queries are sent, it is considered that the group or the source of the group has no receiving host.

Default: 1 seconds

27.2.6 Configure the non querier timer time of the interface

Mode: interface configuration mode

Command: IP IGMP query timeout < time >

Configure the non querier timer time of the interface

Command: no IP IGMP query timeout

The non querier timer time of the recovery interface is the default value

Parameter: < time > indicates the end time of the non inquirer timer, which is an integer between 60-300. When there are multiple switches on the subnet, one needs to be selected as the inquirer to send the query message. During network initialization, all switches send query messages by default. When receiving query messages from other switches, compare each other's IP addresses and select the one with the smaller IP address as the query. If they are not the query, start a timer. The timer is reset every time the query message is received. If the timer terminates, re select the query.

Default: 255 seconds

27.2.7 Configure the query timer interval of the interface

Mode: interface configuration mode

Command: IP IGMP query interval < interval >

Configure the query timer interval of the interface

Command: no IP IGMP query interval

The query timer interval of the recovery interface is the default value

Parameter: < interval > indicates the time interval of the query timer, which is an integer between 1-18000. When the interface starts IGMP protocol, it will start a query timer to send query messages to the subnet regularly; If there are multiple switches, it is necessary to elect a searcher. The searcher uses the timer to send query messages periodically. The non searcher closes the timer and starts a timeout timer. When the timeout timer expires, the searcher is re elected.

Default: 125 seconds

27.2.8 Configure the maximum response time of the interface

Mode: interface configuration mode

Command: IP IGMP query Max response time < time >

Configure the maximum response time carried by the interface when sending query message

Command: no IP IGMP query Max response time

The maximum response time carried by the recovery interface when sending query message is the default value

Parameter: < time > indicates the maximum response time value to be carried by the interface when sending version 2 or version 3 query message, which is an integer between 1-240, with the unit of seconds, but the unit of the maximum response time in the query message is 0.1 seconds. IGMP uses the query response mode to obtain the information of the corresponding group of receiving hosts on the subnet. When a switch sends a query message, multiple hosts on the network will respond to the group report message. In order to avoid the congestion of many IGMP messages, a maximum response time value is carried in the query message, and the host receiving the query message generates a random value according to the maximum response time, The random value delay is used to send the response message. When the consistent group report message sent by other hosts is received during this delay, the group report message of the group to be sent is restrained, which effectively avoids the conflict of IGMP group reports at the same time. It should be noted that the maximum response time range of version 3 is larger than that of version 2, and the maximum response time range of version 2 is less than 128. **Default:** 10 seconds

27.2.9 Configure interface parameters

Mode: interface configuration mode

Command: IP IGMP robustness variable < value >

Configure interface parameters

Command: no IP IGMP robustness variable

Restore the vitality parameter of the interface to the default value

Parameter: < value > indicates the vitality parameter of the interface, which is an integer number between 2 and 7. The vitality parameter describes the robustness of the protocol. When the network environment is bad, the adaptability of the protocol to packet loss, and the configured vitality parameter value affects the number of retransmissions and the interval of relevant timers. The query message of version 3 contains QRV value, which is used to synchronize the vitality parameters locally configured by non inquirers.

28. Configuring PIM-SM

This chapter includes the following contents：

- PIM-SM introduction
- PIM-SM configuration
- PIM-SM configuration example

28.1. PIM-SM introduction

PIM-SM (Sparse Mode Protocol Independent Multicast - Sparse Mode) is a part of multicast technology. It is used for network topology discovery. It is a protocol running between routers. Compared with unicast point-to-point transmission, multicast point-to-multipoint transmission is committed to establishing a distribution tree, so that the source data flow can be transmitted along the distribution tree to the group member hosts that need to be received. There are two forms of distribution tree. One is based on the source. Each source has a distribution tree for each group. The shortest path is from the source to the group members. This active tree is also called the shortest path tree SPT; The other is to share an information distribution point. All sources of a group share a tree. The information of the source needs to be registered at this convergence point (RP: rendezvous point) before it can be transmitted down the distribution tree to the receiving host. This shared tree is also known as RPT. The distributed tree technology of PIM-SM uses the form of one-way shared tree, that is, the data flow can only flow from the source to the receiver, not vice versa. The design goal of PIM-SM is to apply to Wan, that is, the receivers are sparsely distributed in the network, which is different from the diffusion pruning mode of dense mode. PIM-SM uses join pruning mode to establish a shared tree, that is, the receiving host uses explicit join mode (traditional IP multicast mode, the receiving end starts membership). The shared tree is a distribution tree shared by all sources of a group. When different sources need to push data streams, the source needs to register at the aggregation point, and then the aggregation point pushes the data to the receiver. The tree from source to aggregation point is the shortest path tree started by the data. When multiple sources register at the convergence point to forward data streams, the convergence point will become the bottleneck of the network. At this time, PIM-SM allows each source and group to switch to their own shortest path tree without passing through the convergence point. If in a small network, one convergence point is competent. If in a larger network, it is necessary to configure multiple RPS to share tasks, but the static configuration method does not adapt to the dynamic changes of the network. Therefore, PIM-SM provides RP bootstrap mechanism. Multiple candidate BSRs and candidate RPS are configured in the network. The candidate BSR elects the BSR. The candidate RP regularly sends its own group mapping information to the BSR. The BSR collects the RP information and arranges it into bootstrap information, which is regularly diffused in the network. Each router will save a bootstrap information. When a group member joins, look up the bootstrap information, find the RP corresponding to the group and send a join message to the RP direction. If there is no RP corresponding to the group in the bootstrap information, use the hash algorithm to map the group to a RP and send a join message to the RP direction. The assertion mechanism and network sharing mechanism of pim-dr are considered at the same time. Specify that the router Dr should be applied to the process of joining the distribution tree, and the assertion should be applied to the process of forwarding data flow. PIM-SM has become the first choice of intra domain multicast routing protocol because of its exquisite design; Later, pim-ssm is extended to enable users to receive services directly from multicast sources. This model has more outstanding advantages than traditional PIM-SM.

Aiming at the application of multicast protocol on layer 3 switch, the concept of multicast security is proposed. Multicast technology can be divided into three parts: one is multicast source discovery, the other is multicast receiver discovery, and the third is topology discovery. One part of multicast protocol

is the protocol between host and router, such as IGMP; One part is the protocol between routers, such as PIM-SM. Multicast protocol, whether between host and router or between router and router, uses three-layer interface to describe the input and output direction of multicast routing; For a layer-3 switch, if a layer-3 interface is the output interface of a multicast route, then all layer-2 ports in the VLAN corresponding to the layer-3 interface will be output ports. As there is only one VOD host in the downstream VLAN, other output ports in the VLAN are unnecessary. Therefore, IGMP snooping protocol runs in layer 2, which is responsible for monitoring IGMP messages from a port and recording them. When there is a data stream, it is only sent to the requested port when it is output from the VLAN. That is, the information of layer 2 ports needs to be recorded on the layer 3 switch. Similarly, between routers, in order to maintain the multicast distribution tree, it is necessary to send a join pruning message. If the sending and receiving ports of PIM protocol messages are also monitored, the output interface of the multicast routing table will also record the corresponding layer-2 ports. When a data stream flows through the multicast tree, it will only be sent to the ports where the join message arrives in the VLAN, not to all ports in the VLAN. The layer-2 protocol that monitors PIM protocol messages is called PIM snooping. With IGMP snooping and PIM snooping, the multicast routing protocol running on the router can run well on the layer 3 switch. The entries in the multicast routing table will be shown as follows:

Multicast source address multicast group address input interface output interface list output port list

When there is an on-demand data stream, we will see that the branch of the multicast distribution tree from the source to the receiving host is along the layer 2 port where the protocol message once appeared, rather than flooding in the VLAN corresponding to the layer 3 interface.

IGMP snooping and PIM snooping are dynamic monitoring protocols, which record the layer-2 port information according to the protocol message. Currently switch v3 Version 0 only provides the static configuration function of refining multicast routing entries to layer 2 ports. For this function module, we call it multicast security. Through static configuration commands, it specifies that the output of a multicast data stream is only sent to the specific layer 2 port in the VLAN corresponding to the output interface. By default, the data flow will be output to all layer-2 ports in the VLAN corresponding to the output interface.

28.2. PIM-SM configuration

PIM-SM protocol needs to be started one by one on each interface after the layer 3 multicast function is started, and its relevant commands are in global configuration mode and interface configuration mode.

The configuration of PIM-SM includes：

Start multicast routing function

- Configure multicast routing table capacity
- Configure TTL value of multicast interface
- Start interface PIM SM function
- Configure passive mode of interface
- Configure interface priority
- The configuration interface Hello message does not contain genid information
- Configure interface Hello timer interval
- Configure the holding time of neighbours on the interface
- Configure neighbour list filtering of the interface
- Configure the source address of unicast registration message
- Configure the number limit of registered messages

- Check RP when configuring registration
- Configure registration inhibit timer time value
- Configure and register Kat timer time value
- Configure registration source address filtering
- Configure the checksum of the registered message in Cisco mode
- Configure static RP address
- Configure candidate RP
- Configure ignore RP set priority
- Configure c-rp-adv message in Cisco mode
- Configure candidate BSR
- Configure JP timer interval
- Configure SPT (shortest path tree) switching
- Configure SSM (source specific multicast)

28.2.1 Start multicast routing function

Mode: global configuration mode

Command: IP multicast routing Enable multicast routing

Command: no IP multicast routing Turn off multicast routing function

Default: do not start multicast routing function; Use this command to start multicast routing function and PIM-SM and IGMP protocols.

28.2.2 Configure multicast routing table capacity

Mode: global configuration mode

Command: IP multicast route limit < limit > [threshold]

Configure the capacity and alarm threshold of multicast routing table

Command: no IP multicast route limit

Restore the capacity and alarm threshold of multicast routing table to the default value

Parameter: < limit > indicates the capacity of multicast routing table, which is an integer number between 1-2147483647; [threshold] indicates the alarm threshold of the multicast routing table, which is an integer number between 1-2147483647. It can be configured optionally. When the multicast routing table exceeds the alarm threshold, the switch will display a prompt message.

Default: 2147483647

28.2.3 Configure TTL value of multicast interface

Mode: interface configuration mode

Command: IP multicast TTL threshold < threshold >

Configure TTL value of multicast interface

Command: no IP multicast TTL threshold

Recovery multicast interface TTL value is invalid

Parameter: < threshold > indicates the TTL value of the multicast interface, which is an integer between 0-255, and 256 is an invalid value. This command configures the TTL value of the interface and is used to maintain the output interface list of the multicast routing table. When the configured TTL value is between 0-255, the value will be passed to the actual multicast interface. When the value is 256, the actual multicast interface uses its own default TTL value of 1.

Default: 256

28.2.4 Start interface PIM SM function

Mode: interface configuration mode

Command: IP PIM spark mode

Start interface PIM SM Protocol

Command: no IP PIM spark mode

Close interface PIM SM Protocol

Default: the interface does not start the PIM SM Protocol. Use this command to start the PIM SM Protocol function of the interface, send and receive protocol messages, and participate in RP election when bootstrapping is configured. When the interface starts PIM SM, IGMP protocol will be started accordingly. There is no need to configure IP IGMP command.

28.2.5 Configure passive mode of interface

Mode: interface configuration mod

Command: IP PIM spark mode passive

Configure the interface to passive mode

Command: no IP PIM spark mode passive

The active mode of the cancelled interface is the recovery state of the passive interface

Default: the PIM SM Protocol is not started. When the PIM SM function of the interface is started by using the IP PIM spark mode command, it is in the active state, and the interface sends and receives protocol messages normally; When the configuration is in passive mode, the interface does not send protocol messages, does not participate in the registration process, does not participate in the RP election process, and only quietly monitors protocol messages.

28.2.6 Configure interface priority

Mode: interface configuration mode

Command: IP PIM Dr priority < priority >

Configure the priority of interface participating in Dr election

Command: no IP PIM Dr priority [priority]

Restore interface priority to default

Parameter: < priority > indicates the priority of the interface participating in Dr election, which is an integer number between 0-4294967294. When there are multiple switches on the shared network, one is elected as Dr through the Hello protocol, which is responsible for sending the join pruning message to the upstream. In the election of DR, the priority shall be compared first and the one with higher priority shall be selected; With the same priority, select the one with the larger IP address as the Dr.

Default: 1

28.2.7 The configuration interface Hello message does not contain genid information

Mode: interface configuration mode

Command: IP PIM exclude genid

The configuration interface Hello message does not contain the genid domain

Command: no IP PIM exclude genid

The default message recovery interface is configured as hello genid

Default: contains the genid domain; Type 20 in the Hello message option list is the option value of generation ID, which is an unsigned 32-bit value randomly generated during interface startup. It is used to quickly identify whether there is neighbor restart and reduce the delay of relearning RP set

information and adding pruning state due to router restart. The switch retains the genid value in the Hello message, and will update this value after receiving a new Hello message. If the genid changes, it is considered that the neighbour restarts and needs to inform it of relevant information in time, instead of waiting for the timer to terminate before learning by itself, which reduces the convergence time when the network changes.

28.2.8 Configure interface Hello timer interval

Mode: interface configuration mode

Command: IP PIM Hello interval < interval

Configure the Hello timer interval of the interface

Command: no IP PIM Hello interval

The recovery interface Hello timer interval is the default value

Parameter: < interval > indicates the interval of Hello message sent by the interface, which is an integer between 1-65535. The setting of Hello timer interval will affect the holdtime value, which is 3.5 times that of Hello interval. When the value is not configured or the configured value is less than hello interval, it needs to be calculated according to Hello interval.

Default: 30 seconds

28.2.9 Configure the holding time of neighbours on the interface

Mode: interface configuration mode

Command: IP PIM Hello holdtime < value >

Configure the holding time of neighbors sending Hello messages

Command: no IP PIM Hello holdtime

The recovery neighbour retention time is the default value

Parameter: < value > indicates the survival time of neighbors, which is an integer number between 1-65535; If the Hello message is not received within the hold time, it is considered that the neighbor no longer exists. When configuring this value, it must be greater than the value of Hello interval. If it is less than the value of Hello interval, 3.5 times of Hello interval will be used as the value of hold time

Default: 105 seconds (3.5 times the Hello interval)

28.2.10 Configure neighbour list filtering of the interface

Mode: interface configuration mode

Command: IP PIM neighbour filter {< ACL ID > | < ACL name >}

Configure the neighbour list filtering ACL of the interface

Command: no IP PIM neighbour filter {< ACL ID > | < ACL name >}

Cancel neighbour list filtering of interface

Parameter: < ACL ID > indicates the number of the standard access control list, which is an integer number between 1 and 99< ACL name > indicates the standard access control list name. Use ACL to filter the neighbour list of the interface. When the neighbour is filtered by ACL, it will be deleted from the neighbour list of the interface. Refer to the Command Reference Manual for ACL configuration details.

Default: neighbour filtering ACL is not configured

28.2.11 Configure the source address of unicast registration message

Mode: global configuration mode

Command: IP PIM register source {< IP > | < if name >}

Configure the source address or interface name of unicast registration message

Command: no PIM register source

Cancel the configuration of registered source address

Parameter: < IP > indicates the source address of unicast registration message, in dotted decimal format< If name > indicates the source interface name of unicast registration message, which is the layer 3 interface name (eg: vlan2). The address used to register the message source.

Default: the source address of the registration message is not configured, and the interface address of the received packet is used.

28.2.12 Configure the number limit of registered message

Mode: global configuration mode

Command: IP PIM register rate limit < limit >

Configure the threshold of the number of registered messages received within one second

Command: no IP PIM register rate limit

Cancel registration message quantity limit check

Parameter: < limit > indicates the maximum number of registered messages that can be received within 1 second, which is an integer number between 1-65535. The registration message actually encapsulates the data packet. When the source registers, there will be a large data flow impacting the first hop router of the source. At this time, the data flow of PIM SM Protocol can be limited to avoid a large burden on the router. Because PIM SM only needs data flow to trigger SPT establishment from source to RP, the restriction mechanism can be used. When limiting the data flow, check the number of data packets within 1 second. If the arrival interval of two data packets exceeds 1 second, there is no limit.

Default: no limit on the number of registered messages is configured (the threshold value is 0)

28.2.13 Check RP when configuring registration

Mode: global configuration mode

Command: IP PIM register RP reachability

Check whether RP is reachable when configuring registration

Command: no IP PIM register RP reachability

There is no need to check whether the RP is reachable when configuring registration

Default: there is no need to check whether the RP is reachable during registration

28.2.14 Configure registration inhibit timer time value

Mode: global configuration mode

Command: IP PIM register suppression < value >

Configure registration inhibit timer time value

Command: no IP PIM register suppression

The resume registration suppression timer time is the default value

Parameter: < value > indicates the time value of the registration suppression timer, which is an integer number between 1-65535.

Default: 60 seconds

28.2.15 Configure and register Kat timer time value

Mode: global configuration mod

Command: IP PIM RP register Kat < value >

Configure the Kat timer time of (s, g) entries registered and created on RP

Command: no IP PIM RP register Kat

The Kat timer time of recovery (s, g) is the default value

Parameter: < value > indicates the time value of Kat timer of (s, g) entries created by source registration on RP, which is an integer number between 1-65535.

Default: 185 seconds（3 * register-suppression + register-probe）

28.2.16 Registration address configuration

Mode: global configuration mode

Command: IP PIM accept register list {< acl-id1 > | < acl-id2 > | < ACL name >

Configure the source filter list of registration message

Command: no IP PIM accept register

Source filter list of unregistered message

Parameter: < ACL Id1 > indicates the number of the extended access control list, which is an integer between 100 and 199< Acl-id2 > indicates the number of the extended part of the extended access control list, which is an integer number between 2000-2699< ACL name > indicates the name of the access control list. The access control list can be used to filter the source address registered to the RP. if the source address on the RP is filtered by ACL, the corresponding (s, g) entry will be deleted from the multicast routing table. Refer to the Command Reference Manual for ACL configuration details.

Default: ACL of registration source is not configured

28.2.17 Configure the checksum of the registered message in Cisco mode

Mode: global configuration mode

Command: IP PIM Cisco register checksum [group list {< ACL Id1 > | < ACL Id2 > | < ACL name >}]

Configure the checksum of the registered message as Cisco mode

Command: no IP PIM Cisco register checksum [group list {< ACL Id1 > | < ACL Id2 > | < ACL name >}]

The checksum of unregistered message is Cisco mode

Parameter: < ACL Id1 > indicates the number of the standard access control list, which is an integer number between 1-99< Acl-id2 > indicates the number of the extended part of the standard access control list, which is an integer number between 1300 and 1999< ACL name > indicates the name of the standard access control list. The checksum of Cisco mode is to calculate the checksum of the whole registration message (including the data packet part), while the checksum of general registration message only includes the header of PIM SM protocol message and the header of registration message. If the access control list is configured, the ACL is required to filter the corresponding group address when sending the registration message. The Cisco checksum can be used through the ACL, but the general checksum can not be used through the ACL.

Default: Cisco checksum is not configured

28.2.18 Configure static RP address

Mode: global configuration mode

Command: IP PIM RP address < IP > [< acl-id1 > | < acl-id2 > | < ACL name >]

Configure static RP

Command: no IP PIM RP address < IP > [< acl-id1 > | < acl-id2 > | < ACL name >]

Cancel static RP configuration

Parameter: < IP > indicates the address of static RP, in dotted decimal format< ACL Id1 > indicates the number of the standard access control list, which is an integer number between 1 and 99< Acl-id2 > indicates the number of the extended part of the standard access control list, which is an integer number between 1300 and 1999< ACL name > indicates the name of the standard access control list.

Default: static RP is not configured

28.2.19 Configure candidate RP

Mode: global configuration mode

Command: IP PIM RP candidate < if name > [group list {< ACL ID > | < ACL name >} | interval < value1 > | priority < Value2 >]

The configuration interface is c-rp

Command: no IP PIM RP candidate [if name]

Cancel interface C-RP attribute

Parameter: < if name > indicates the name of the interface configured as C-RP, which is the name of the three-tier interface (eg: vlan2)< ACL ID > indicates the number of the standard access control list, which is an integer between 1 and 99< ACL name > indicates the name of the standard access control list< Value1 > indicates the time interval from C-RP periodic unicast c-rp-adv message to BSR, which is an integer number between 1-16383< Value2 > indicates the priority of C-RP, which is an integer number between 0 and 255. It is included in the bootstrap information. It is used to flood in the domain for the selection of RP corresponding to the group.

Default: value1 defaults to 60 seconds; Value2 defaults to 192.

28.2.20 Configure ignore RP set priority

Mode: global configuration mode

Command: IP PIM ignore RP set priority

Configure to ignore priority and use hash algorithm mapping when searching RP in RP set

Command: no IP PIM ignore RP set priority

Configure to find RP usage priority in RP set

Default: find the priority order of RP in RP set

28.2.21 Configure c-rp-adv message in Cisco mode

Mode: global configuration mode

Command: IP PIM CRP Cisco prefix

Configure the c-rp-adv message to a format acceptable to Cisco BSR

Command: no IP PIM CRP Cisco prefix

Configure c-rp-adv message to standard RFC format

Default: c-rp-adv message is in standard RFC format. Cisco BSR does not receive c-rp-adv messages. The prefix CNT domain is 0. If there is no group address by default, the prefix CNT domain is 1. Fill

in a 224.0.0.0 group address. The standard RFC defaults to 0 in the prefix CNT field if there is no group address. This command is compatible with BSR. It is a Cisco router and needs to send c-rp-adv messages that can be recognized by Cisco BSR.

28.2.22 Configure candidate BSR

Mode: global configuration mode

Command: IP PIM BSR candidate < if name > [< hash mask len > | < priority >]

Configure the interface, priority and mask length of hash calculation of the candidate BSR

Command: no IP PIM BSR candidate [if name]

Cancel the candidate BSR identity of the interface

Parameter: < if name > indicates the interface name of the candidate BSR, which is the layer 3 interface name (eg: vlan2)< Hash mash len > indicates the mask length in the hash algorithm, which is an integer number between 0-32< Priority > indicates the priority of the candidate BSR when participating in the BSR election. It is an integer number between 0-255. When the candidate BSR is selected as BSR, its hash mask len and priority are transmitted in the bootstrap message.

Default: the default value of priority is 0; The default value of hash mask len is 10.

28.2.23 Configure JP timer interval

Mode: global configuration mode

Command: IP PIM JP timer < time >

Configure upstream join pruning timer interval

Command: no IP PIM JP timer [time]

Restore the upstream join pruning timer interval to the default time

Parameter: < time > indicates the time interval for the switch to periodically send the pruning message to the upstream, which is an integer number between 1-65535. The switch maintains the forwarding state of the multicast distribution tree through the JP timer. Join the JP timer interval with the holding time of pruning state of 3.5 times, and the holding time is included in the join pruning message.

Default: 60 seconds

28.2.24 Configure SPT switching

Mode: global configuration mode

Command: IP PIM SPT threshold [group list < ACL Id1 > | < ACL Id2 > | < ACL name >]

Configure SPT switching

Command: no IP PIM SPT threshold [group list < ACL Id1 > | < ACL Id2 > | < ACL name >]

Cancel SPT switching

Parameter: < ACL Id1 > indicates the number of the standard access control list, which is an integer number between 1-99< Acl-id2 > indicates the number of the extended part of the standard access control list, which is an integer number between 1300 and 1999< ACL name > indicates the name of the standard access control list. When SPT switching is configured, the access control list can be used to filter the (*, g) entries of the multicast routing table. SPT switching can be configured through ACL, but SPT switching cannot be configured if it fails.

Default: SPT switching is not configured

28.2.25 Configure SSM

Mode: global configuration mode

Command: IP PIM SSM {default | range {< ACL ID > | < ACL name >}}

Configure SSM (source specific multicast)

Command: no IP PIM SSM

Cancel SSM

Parameter: < ACL ID > indicates the number of the standard access control list, which is an integer number between 1 and 99< ACL name > indicates the name of the standard access control list.

Default: SSM is not configured

28.2.26 Configure multicast security

Mode: global configuration mode

Command: IP mroute < SRC addr > < GRP addr > < IIF name > < OIF name > remove < if name >

For a multicast route (s, g), a specific layer-2 port in the corresponding VLAN of an output interface does not forward data flow

Command: IP mroute < SRC addr > < GRP addr > < IIF name > < OIF name > Add < if name >

Add an output port of a multicast route (s, g) back to the output interface corresponding to its VLAN

Parameters: SRC addr indicates the multicast source address of multicast route (s, g)

GRP addr represents the multicast group address of multicast routing (s, g)

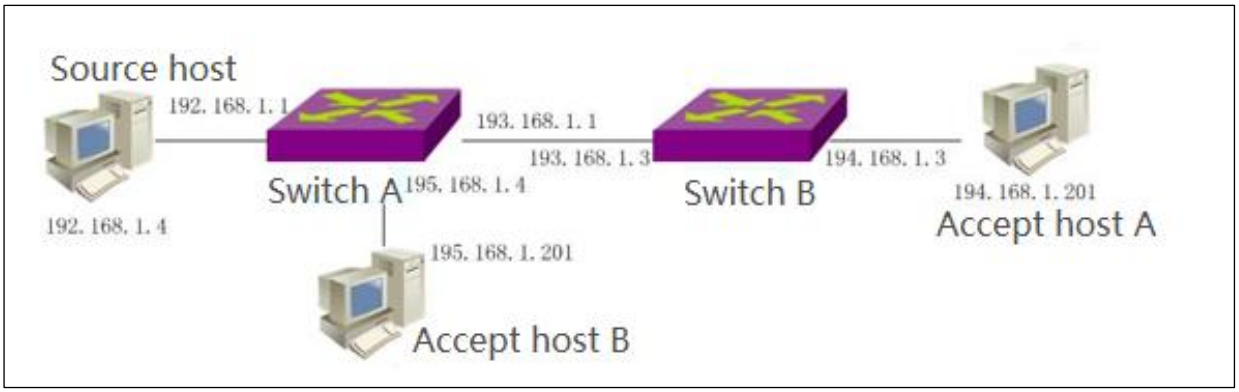
IIF name indicates the input interface of multicast routing (s, g)

OIF name indicates the output interface of multicast routing (s, g)

If name indicates that the output interface of multicast routing (s, g) corresponds to the layer-2 port in the VLAN. The remove command shields the layer-2 port from the VLAN where the output interface is located, that is, the data flow forwarded from the output interface will not be forwarded from the layer-2 port. The add command adds the layer-2 port back to the VLAN where the output interface is located, that is, the data flow forwarded from the output interface will be forwarded from the layer-2 port.

Default: all layer 2 ports in the VLAN corresponding to the output interface will forward multicast data streams

28.3 PIM-SM Configuration example



Configuration

Start PIM-SM protocol to enable the receiving host to receive multicast data stream from the source host。

On switch A：

Switch#configure terminal
Switch(config)#ip multicast-routing
Switch(config)#ip pim rp-address 193.168.1.3
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#ip pim sparse-mode
Switch(config-vlan2)#interface vlan3
Switch(config-vlan3)#ip address 193.168.1.1/24
Switch(config-vlan3)#ip pim sparse-mode
Switch(config-vlan3)#interface vlan5
Switch(config-vlan5)#ip address 195.168.1.1/24
Switch(config-vlan5)#ip pim sparse-mode

On switch B：

Switch#configure terminal
Switch(config)#ip multicast-routing
Switch(config)#ip pim rp-address 193.168.1.3
Switch(config)#interface vlan3
Switch(config-vlan3)#ip address 193.168.1.3/24
Switch(config-vlan3)#ip pim sparse-mode
Switch(config-vlan3)#interface vlan4
Switch(config-vlan4)#ip address 194.168.1.3/24
Switch(config-vlan4)#ip pim sparse-mode

(2) Verification

Use the following command to view PIM-SM information：

show ip pim sparse-mode interface
show ip pim sparse-mode neighbor
show ip pim sparse-mode local-members
show ip pim sparse-mode mroute
show ip pim sparse-mode rp mapping

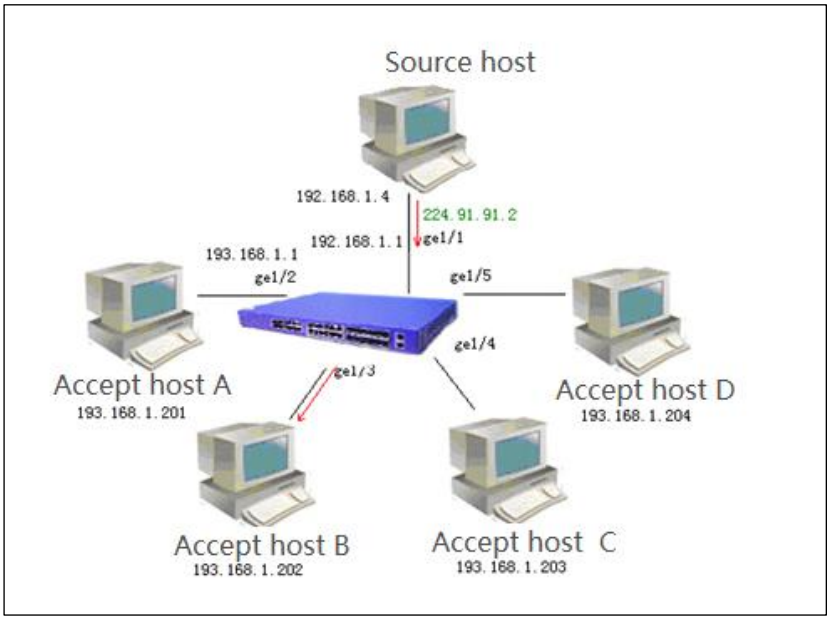
(3) Configure multicast security

The multicast security function module runs on the multicast routing protocol. First start the multicast routing protocol, and then configure the forwarding state of the layer-2 port of its output interface according to the specific origin of a multicast path. As shown in the figure below, vlan2 connects to the multicast source 192.168.1.4; There are four hosts in vlan3, which are connected to ports GE1 / 2, GE1 / 3, GE1 / 4 and GE1 / 5 respectively; As shown by the red arrow in the figure, only the host 193.168.202 on-demand broadcasts the programs of multicast group 224.91.91.2, and the other three hosts do not participate in multicast on-demand, so the data flow forwarded from the three layer-2

ports is unnecessary. GE1 / 2, GE1 / 4 and GE1 / 5 are shielded by configuring static multicast commands。

On the switch：

Switch#configure terminal
Switch(config)#ip multicast-routing
Switch(config)#ip pim rp-address 193.168.1.1
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#ip pim sparse-mode
Switch(config-vlan2)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#interface vlan3
Switch(config-vlan3)#ip address 193.168.1.1/24
Switch(config-vlan3)#ip pim sparse-mode
Switch(config-vlan3)#interface ge1/2
Switch(config-ge1/2)#switchport access vlan 3
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 3
Switch(config-ge1/3)#interface ge1/4
Switch(config-ge1/4)#switchport access vlan 3
Switch(config-ge1/4)#interface ge1/5
Switch(config-ge1/5)#switchport access vlan 3
Switch(config-ge1/5)#exit
Switch(config)#ip mroute 192.168.1.4 224.91.91.2 vlan2 vlan3 remove ge1/2
Switch(config)#ip mroute 192.168.1.4 224.91.91.2 vlan2 vlan3 remove ge1/4
Switch(config)#ip mroute 192.168.1.4 224.91.91.2 vlan2 vlan3 remove ge1/5



29 Configuring RIP

This chapter includes the following.

- RIP Introduction
- RIP configuration
- Sample RIP configuration

29.1 RIP Introduction

RIP (Routing Information Protocol) is a dynamic routing protocol developed earlier, which uses distance vector algorithm and is mostly used in small networks. RIP protocol packets are encapsulated in UDP packets using UDP port 520. The main idea of RIP is to use the hop count to measure the distance to the host, and the hop count increases by 1 every time a router passes through, so as to calculate the weight of the route. Metric) for routing. The RIP convention has a maximum hop count of 15, and a hop count of 16 is marked as unreachable. RIP uses the method of broadcasting the entire routing table to synchronize the routing information of the routers in the network. It updates the message regularly every 30 seconds. If a route entry does not receive an update message from a neighbour within 180 seconds, it marks it as unreachable. If it does not receive a valid update within 120 seconds, it deletes the route.

RIP is easy to implement because of its simple idea, but it also brings the corresponding routing loop problem. In order to prevent the routing loop, RIP introduces the split horizon mechanism to avoid the spoofing between routers. Split horizon means that routing updates are not published out the receiving interface. Split horizon with poison reverse publishes routing updates out the receiving interface, but with the metric marked unreachable, allowing neighbouring routers to quickly identify loops without waiting for the metric to increase to unreachable.

Route entries in the routing table should contain a destination address (host or network), a next-hop address, a forwarding interface, a routing metric, a timer that is reset when a routing update is received, and a routing tag.

When RIP is started, it immediately sends a full table request message in the form of broadcast (RIP-1) or multicast (RIP-2), and the adjacent router receives the request message and sends back its own complete routing table as a response message. When the router receives the response message, it will process the route one by one and modify its own routing table. When there is a new route, it will immediately generate a trigger update message. After a series of updates, RIP eventually converges, and each router in the network maintains the latest and consistent routing information. After the network is stable, RIP still broadcasts the local routing table to the neighbors every 30 seconds, and each router maintains its own routing information according to the received routing update message to select the most preferred route. RIP uses a time-out mechanism to handle routing entries that have not been updated for a long time to ensure that the route is correct in real time.

RIP is mostly used in campus networks and relatively continuous regional networks with simple structure, and it is not competent for large and complex networks.

29.2 RIP Configuration

After starting the RIP protocol, you can configure each function and attribute of RIP. RIP is mostly configured in RIP configuration mode and interface configuration mode.

The configuration of RIP includes:

- Start RIP and enter RIP configuration model
- Enable RIP interface
- Configure unicast message transmission
- Configure the working status of the interface
- Configure the default route weight
- Configuration management distance
- Configure the timer
- Configuration version
- Introducing external routing
- Configure route filtering
- Configure additional routing metric
- Configure the RIP version of the interface
  Configure the receiving and sending status of the interface
- Configure split horizon
- Message authentication
- Configure interface weight

29.2.1 Start RIP and enter RIP configuration model

Mode: Global Configuration Mode

Command：router rip

Start rip and enter rip configuration model

Command：no router rip

Turn off the rip protocol

Default: Do not run the rip protocol

29.2.2 Enable RIP interface

When RIP works, certain interfaces can be designated, and the network where the interfaces are located can be configured as a RIP network, so that RIP protocol messages can be sent and received on the RIP network.

Mode: RIP configuration model

Command：network <network-address>

Enable rip interface

Command：no network <network-address>

Shut down the rip interface

Parameters: There are two forms: A. B. C. D/M and A. B. C. D A. B. C. D. The former specifies the network IP and mask length, while the latter specifies the network IP and mask.

Default: RIP is disabled on all interfaces when it is started

When the RIP protocol is started, it must specify the network segment on which it operates. RIP can only run on interfaces that are on the specified network segment. For those interfaces that are not on the specified network segment, RIP will neither receive nor forward routes. Interfaces that are not in the specified network segment do not exist in the RIP view. The parameter network-address is the enabled or disabled network address, which can be configured as the interface IP address. The network command enables the interface of the network segment of the address. For example, if the IP address of an interface is 192.160. 1.1, use the command network 192.160. 1.1/24, and use the show running-config command to see the network 192.160. 1.0/24.

29.2.3 Configure unicast message transmission

RIP version 1 uses broadcasts to exchange messages, and version 2 uses multicasts (224.0, 0.9) to exchange messages. When RIP is running on a link that does not support broadcasts, it is necessary to specify a specific unicast address to exchange messages.

Mode: RIP configuration model

Command：neighbour <ip-address>

Configure peer unicast IP addr

Command：no neighbour <ip-address>

Cancel setting of peer unicast IP address

Parameters: ip-address is the specified unicast IP address

Default: RIP does not send messages to any unicast addr

29.2.4 Configure the working status of the interface

The RIP protocol operates in some networks where you may only need RIP interface routes and do not want to broadcast RIP routes on that interface. Use the network command to specify that RIP protocol messages are sent and received on the interface, and you can learn the route of the interface. Use the passive-interface command to simply learn the route for that interface and block broadcasts for that interface.

Mode: RIP configuration model

Command：passive-interface <if-name>

Configure the interface to be passive

Command：no passive-interface <if-name>

Cancel the passive state of the interface

Parameter: if-name is the agreed name of the three-layer interface (for example: vlan1, vlan2 …)

Default: none of the enabled RIP interfaces are passive

29.2.5 Configure the default route weight

When an external route is introduced, a route metric is specified; when it is not specified, the default route metric is used.

Mode: RIP configuration model

Command：default-metric <metric>

Set the default route metric when importing an external route

Command：no default-metric [metric]

The default route metric is the default value of 1 when the external route is restored

Parameter: metric value is between 1 and 16, greater than 1 and less than 16.

Default: The metric value is 1. Use the no default-metric command to return to the default value.

29.2.6 Configuration management distance

Each protocol has an agreed priority, and the administrative distance is the priority with which the route is selected when a routing policy is used. When there are two identical routes (from different routing protocols) to the same destination, the smaller the administrative distance, the route of the protocol is preferred.

Mode: RIP configuration model

Command：distance <distance>

Setting the Administrative Distance Value

Command：no distance [distance]

The recovery administrative distance is the default

Parameter: distance is between 1 and 255Parameter: distance is between 1 and 255

Default: The distance value is 120. Use the no distance command to return to the default value.

29.2.7 Configure the timer

The RIP protocol has three timers, one in which the full routing table is broadcast to all RIP interfaces every 30 seconds, and the other in which each route in the RIP routing table is marked with a metric of 16 if it does not receive an update for 180 seconds. The third is that each route in the RIP routing table is deleted from the routing table if it has not been effectively updated for 120 seconds after the metric is 16.

Mode: RIP configuration model

Command：timers basic <update> <timeout> <garbage>

Set three timer values

Command：no timers basic

Resume timer as default

Parameters: The first parameter update is the timer for regularly updating the entire RIP routing table; the second parameter timeout is the timer for not updating each route after timeout; the third parameter garbage is the timer to be deleted after timeout after each route is marked as invalid; the value range of the three timers is 5~(231-1).

Default: update is once every 30 seconds; timeout is 180 seconds, marked as invalid; garbage is deleted in 120 seconds.

29.2.8 Configuration version

The RIP protocol currently has version 1 (RFC1058) and version 2 (RFC2453), and the configured version value will be reflected in the version field of the protocol message.

Mode: RIP configuration model

Command：version <version>

Set the RIP protocol to version 1 or version 2

Command：no version [version]

Restore RIP protocol version to default

Parameter: version can take the value 1 or 2

Default: Version 2

29.2.9 Introducing external routing

RIP allows the user to import routing information from other protocols into the routing table of RIP. The routing protocols (types) that RIP can import include: connected, static, OSPF, IS-is, and BGP.

Mode: RIP configuration model

Command：redistribute {kernel | connected | static | ospf | isis | bgp} [metric <metric> | route-map <route-map-name>]

Introducing Other Protocol Routine

Command：no redistribute {kernel | connected | static | ospf | isis | bgp} [metric <metric> | route-map <route-map-name>]

Cancel Incoming Route

Parameters: The first parameter is the name of other protocols to be introduced, including direct connection, static, OSPF, IS-is, and BGP; the second parameter is the value set during introduction, ranging from 1 to 16; the third parameter is the name of the referenced route-map, which is configured in the global configuration mode. Please refer to the command manual.

Default: RIP protocol does not introduce any external protocol

29.2.10 Configure route filtering

RIP provides the function of route filtering, and configures policy rules to filter the received routes and published routes through the specified access control list and address prefix list.

Mode: RIP configuration model

Command：distribute-list <acl-name> {in | out} [if-name]

Use access-list to filter the input and output of the interface

Command：no distribute-list <acl-name> {in | out} [if-name]

Suppress access-list filtering

Parameters: acl-name indicates the name of the referenced access-list; if-name indicates the RIP interface to which the application is applied; in and out indicate whether the application is applied in the direction in which the route was received or in the direction in which the route was published.

Command：distribute-list prefix <pre-name> {in | out} [if-name]

Filtering with prefix-list

Command：no distribute-list prefix <pre-name> {in | out} [if-name]

Suppress prefix-list filtering

Parameters: pre-name indicates the name of the referenced prefix-list; if-name indicates the RIP interface to which it is applied; in and out indicate whether it is applied in the direction in which the route was received or in the direction in which the route was published.

Default: RIP does not filter any incoming or outgoing rout

The access-list and prefix-list are configured in global configuration mode and can be found in the command manual.

29.2.11 Configure additional routing metric

The additional routing metric is an offset value added to the routing metric of the RIP protocol when it is input or output. It does not directly change the metric of the route in the routing table, but adds an offset when the interface receives and sends the route.

Mode: RIP configuration model

Command：offset-list <acl-name> {in | out} <offset> [if-name]

Use the access-list to add an offset to the weight of the interface's input and output route

Command：no offset-list <acl-name> {in | out} <offset> [if-name]

Offset to cancel the weight of the input/output route

Parameters: acl-name indicates the access-list name of the reference; in and out indicate whether the application is in the input or output direction; offset indicates the value of the offset between 0 and 16; if-name indicates the RIP interface to which the application is applied.

Default: The additional weight value of each route is 1 when receiving a message, and 0 when sending a message.

29.2.12 Configure the RIP version of the interface

RIP is divided into two versions, RIP-1 and RIP-2, and the RIP message version processed by the interface of the enabled RIP protocol can be specified. The receiving direction can be divided into receiving only RIP-1 messages, receiving only RIP-2 messages, and receiving both RIP-1 and RIP-2 messages. In the sending direction, it can be divided into sending RIP-1 messages, sending RIP-2 messages (in the broadcast mode), sending RIP-2 messages (in the multicast mode), and sending both RIP-1 and RIP-2 messages. RIP-2 has two ways to send messages: broadcast and multicast. Using multicast can not only prevent the hosts that do not run RIP in the same network from not receiving the broadcast messages of RIP, but also prevent the hosts that run RIP-1 from processing the routing with subnet mask of RIP-2 incorrectly.

Mode: Interface configuration model

Command：ip rip receive version {1 | 2}

Set the interface to receive only version 1 messages or only version 2 message

Parameter: Version 1 or Version 2

Command：ip rip receive version {1 2 | 2 1}

Set the interface to receive both version 1 and version 2 messages

Parameter: can be written as 1 2 or 2 1

Command：no ip rip receive version [1 | 2 | 1 2 | 2 1]

Recover the setting of interface receiving message to the default value

Default: Version 2 multicast mode

Command：ip rip send version {1 | 2 | 1-compatible}

Set the interface to send only messages of version 1 or only messages of version 2

Parameter: version 1 or version 2; 1-compatible indicates that the interface of version 2 sends a **message compatible with version 1, that is, a broadcast message rather than a multicast message.**

Command：ip rip send version {1 2 | 2 1}

Set the interface to send both version 1 and version 2 messages

Parameter: can be written as 1 2 or 2 1

Command：no ip rip send version [1 | 2 | 1-compatible | 1 2 | 2 1]

The message sent by the recovery interface is set as the default value.

Default: Version 2 multicast mode

29.2.13 Configure the receiving and sending status of the interface

After the RIP interface is enabled by using the network command in the RIP mode, you can also specify the status of receiving and sending protocol messages, whether to receive protocol messages, or whether to send protocol messages in the interface mode.

Mode: Interface configuration model

Command：ip rip receive-packet

Configure interface to receive protocol message

Command：no ip rip receive-packet

Configure the interface not to receive the protocol message

Command：ip rip send-packet

Configure interface to send protocol message

Command：no ip rip send-packet

Configure the interface not to send protocol message

Default: enable to receive and send protocol message

Note the difference. The network command enables a network to run the RIP protocol. The interface in the network sends and receives protocol messages. The interface route is included in the routing table. After the network command takes effect, the passive-interface command prevents the interface from sending and receiving protocol messages, but the interface route is still included in the routing table. The IP rip receive-packet and IP rip send-packet commands also specify whether the interface is to receive or send a protocol packet after the network command comes into effect.

29.2.14 Configure split horizon

Split horizon means that a route received from this interface is not sent out this interface. Split horizon with poison reverse means that the route received from this interface is still sent out this interface, but its metric value is marked as 16. Split horizon can avoid loops to some extent. Split horizon with poison reversal is more efficient than normal split horizon, and direct marking is unreachable. But on NBMA networks, you need to disable split horizon to get the correct route.

Mode: Interface configuration model

Command：ip rip split-horizon [poisoned]

Enable interface split horizon or with poison reverse

Command：no ip rip split-horizon

Disables the split horizon feature on the interface

Parameters: no poisoned parameter means normal split horizon function is enabled, and poisoned parameter means split horizon function with poison reversal is enabled.

Default: Split horizon with poison reversal

29.2.15 Message authentication

RIP-1 does not support message authentication. RIP-2 supports message authentication. There are two authentication methods, plaintext authentication and MD5 authentication. The unencrypted authentication data in plaintext authentication is transmitted with the message, which can not provide security guarantee and can not be applied to the network with high security requirements. There are two kinds of password settings: the common key and the key chain. The common key stores an independent string, and the key chain manages the ID, content, receiving lifetime, and sending lifetime of the key. Key chain management is detailed in the command reference manual.

Mode: Interface configuration model

Command：ip rip authentication mode {text | md5}

Set authentication mode plaintext or MD5

Command：no ip rip authentication mode [text | md5]

Decertification

Parameter: text is plaintext authentication, MD5 authentication.

Default: No authentication

Command：ip rip authentication string <password>

Set the password string for authentication

Command：no ip rip authentication string [password]

Unauthenticated password string

Parameter: 16-byte authentication password

Command：ip rip authentication key-chain <key-chain-name>

Set the key-chain for authentication

Command: no IP rip authentication key-chain key-chain-name] unauthenticated key-chain

Parameter: The name of the referenced key-chain; the key-chain is configured in the global configuration mode. See the command manual.

29.2.16 Configure interface weight

Mode: Interface configuration model

Command：ip rip metric <metric>

Configure interface weight

Command：no ip rip metric

Restore interface weights to default values

Parameter**: The metric value is between 1 and 16, indicating the metric to be increased for the routing** entry learned by the interface.

Default: 1

29.2.17 Display Information

Mode: Normal or Privileged

Command：show ip protocols

Displays information about all protocols that are running

Command：show ip protocols rip

Displaying RIP Protocol Information

Command：show ip rip

Displaying RIP Routine

Command：show ip rip database

Show RIP Database

Command：show ip rip database count

Displays the number of RIP database entries

Command：show ip rip interface [if-name]

Displaying RIP Interface Information

Parameter: if-name is the agreed three-layer interface name

Mode: Privileged Mode

Command：show running-config

Displays the current configuration of the switch, including RIP configuration.

Command：show running-config rip

Displays the current configuration of the RIP protocol.

29.3. Sample RIP configuration

(1) configuration

The three switches are connected in pairs and have six network segments respectively, and rip protocol is enabled, so that the three PCs can communicate with each other in pairs.

On Switch 1:

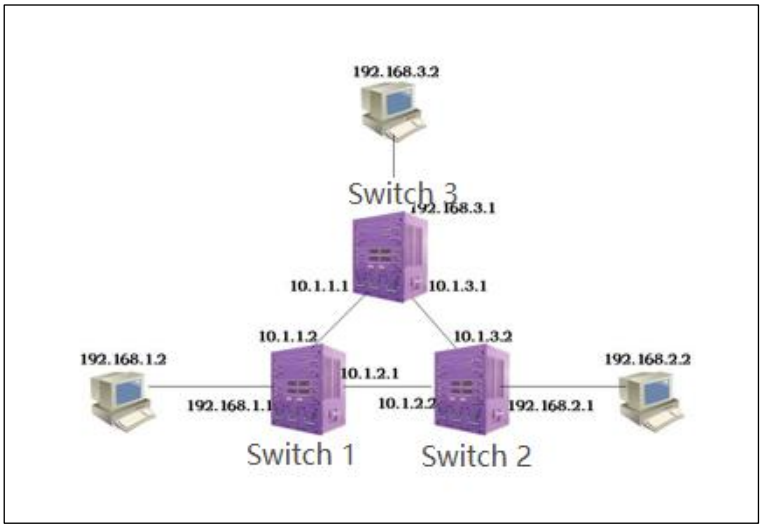
Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.1.0/24

Switch(config-rip)#network 10.1.1.0/24

Switch(config-rip)#network 10.1.2.0/24



On Switch 2:

Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.2.0/24

Switch(config-rip)#network 10.1.2.0/24

Switch(config-rip)#network 10.1.3.0/24

On Switch 3:

Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.3.0/24

Switch(config-rip)#network 10.1.1.0/24

Switch(config-rip)#network 10.1.3.0/24

(1) Verification

Use the following command to view RIP information:

show ip protocols rip

show ip rip database

show ip rip interface

30. Configuring RIPng

This chapter includes the following contents：

- RIPng introduction
- RIPng configuration
- RIPng configuration example

30.1 RIPng introduction

RIPng is a relatively simple internal gateway protocol, which is the application of rip in IPv6 network. RIPng is mainly used in smaller networks, such as campus networks and regional networks with simple structure. Since the implementation of RIPng is relatively simple, and it is much easier than OSPFv3 and IS-IS for IPv6 in configuration and maintenance management, RIPng is still widely used in practical networking

With the construction of IPv6 network, dynamic routing protocol is also needed to provide accurate and effective routing information for IPv6 message forwarding. Therefore, on the basis of retaining the advantages of rip, IETF forms Rip (RIP next generation) for IPv6 network modification. RIPng is mainly used to provide routing function in IPv6 network. It is an important protocol of routing technology in IPv6 network.

Differences between RIPng and rip

In order to realize the application in IPv6 network, RIPng modifies the original rip protocol：

- RIPng uses port 521 of UDP (RIP uses port 520) to send and receive routing information.
- The destination address of RIPng uses a 128 bit prefix length (mask length).
- RIPng uses a 128 bit IPv6 address as the next hop address.
- RIPng uses the link local address fe80:: / 10 as the source address to send RIPng routing information update message.
- RIPng sends routing information periodically by multicast, and uses ff02:: 9 as the router multicast address within the local range of the link.
- RIPng message is composed of header and multiple route table entries. In the same RIPng message, the maximum number of RTE is determined according to the MTU value of the interface.

30.2 RIPng configuration

After starting RIPng protocol, you can configure various functions and attributes of RIPng. RIPng is mostly configured in RIPng configuration mode and interface configuration mode.

- RIPng configuration includes:
- Start RIPng and enter RIPng configuration mode
- Enable RIPng interface
- Configure specific neighbors to send updates
- Configure the working state of the interface
- Configure default routing weights
- Configure timer
- Introducing external routing
- Configure routing filtering
- Configure additional routing weights
- Configure horizontal segmentation
- Configure interface weights

30.2.1 Start RIPng and enter RIPng configuration mod

Mode: global configuration mode

Command: router IPv6 rip

Start RIPng and enter RIPng configuration mode

Command: no router IPv6 rip

Close RIPng protocol

Default: RIPng protocol is not run

30.2.2 Enable RIPng interface

When RIPng works, some interfaces can be specified, and the network it is in can be configured as RIPng network, on which RIPng protocol messages can be sent and received.

Mode: interface configuration mode

Command: IPv6 Router rip

Enable RIPng interface

Command: no IPv6 Router rip

Close RIPng interface

Parameter: none.

Default: disabled on all interfaces after RIPng protocol is started

After RIPng protocol is started, its working interface must be specified, and RIPng can only run on the specified interface.

30.2.3 Configure specific neighbours to send updates

Specify neighbours and send updates to specific neighbours.

Mode: Rip configuration mode

Command: neighbour < neighbour address > < ifname >

Configure IPv6 addresses for specific neighbours

Command: neighbour < neighbour address > < ifname >

Cancel specific neighbour configuration

Parameter: neighbour address is the IPv6 address of a specific neighbour

30.2.4 Configure the working state of the interface

RIPng protocol runs in some networks. It may only need RIPng interface routing and does not want to broadcast RIPng routing on this interface. Use the passive interface command to only know the route of the interface and block the broadcast of the interface.

Mode: RIPng configuration mode

Command: passive interface < if name >

Configure the interface to be passive

Command: no passive interface < if name >

Cancel interface passive state

Parameter: if name is the agreed three-tier interface name (for example: vlan1, vlan2...)

30.2.5 Configure default routing weights

When introducing an external route, you need to specify a route weight; When the routing weight is not specified, this default routing weight is used.

Mode: RIPng configuration mode

Command: default metric < metric >

Set the default route weight when introducing external routes

Command: no default metric [Metric]

When the external route is restored, the default route weight is 1

Parameter: metric value is between 1 and 16, greater than 1 and less than 16.

Default: the metric value is 1. Use the no default metric command to restore to the default value.

30.2.6 Configure timer

RIPng protocol has three timers. One is that the complete routing table broadcasts to all RIPng interfaces every 30 seconds. The other is that each route in RIPng routing table is marked with metric of 16 if it does not receive update in 180 seconds. The third is that each route in RIPng routing table is deleted from the routing table if it is marked with metric of 16 and not effectively updated in 120 seconds.

Mode: RIPng configuration mode

Command: timers basic < update > < timeout > < garbage >

Set three timer values

Command: no timers basic

The recovery timer is the default

Parameters: the first parameter update is the timer for regularly updating the entire RIPng routing table, the second parameter timeout is the timer for each route timeout without updating, and the third parameter garbage is the timer to be deleted after each route is marked as invalid; The value range of the three timers is 5 ~ (231-1).

Default: update every 30 seconds; When timeout is 180 seconds, it is marked as invalid; Garbage is deleted in 120 second.

30.2.6 Introducing external routing

RIPng allows users to introduce the routing information of other protocols into the routing table of rip. The routing protocols (types) that RIPng can introduce include connected, static, OSPF, IS-IS and BGP.

Mode: RIPng configuration mode

Command: redistribute {kernel | connected | static | ospf6 | Isis | BGP} [Metric < metric > | route map < route map name >]

Introducing other protocol routes

Command: no redistribute {kernel | connected | static | ospf6 | Isis | BGP} [Metric < metric > | route map < route map name >] Cancel incoming route

Parameter: the first parameter is the name of the imported other protocols, including direct connection, static, OSPF, is is and BGP; The second parameter is the weight set during import, with a value between 1 and 16; The third parameter is the name of the referenced route map. Route map is configured in the global configuration mode. Please refer to the command manual.

Default: RIPng protocol does not introduce any external protocols

30.2.7 Configure routing filtering

RIPng provides the function of route filtering. It filters the received routes and published routes and configures policy rules through the specified access control list and address prefix list.

Mode: RIPng configuration mode

Command: distribute list < ACL name > {in | out} [if name]

Use access list to filter the input and output of the interface

Command: no distribute list < ACL name > {in | out} [if name]

Cancel access list filtering

Parameter: ACL name indicates the name of the referenced access list; If name indicates the RIPng interface applied to; In and out indicate whether the application is in the direction of receiving routes or publishing routes.

Command: distribute list prefix < pre name > {in | out} [if name]

Filter using prefix list

Command: no distribute list prefix < pre name > {in | out} [if name]

Cancel using prefix list filtering

Parameter: pre name indicates the name of the referenced prefix list; If name indicates the RIPng interface applied to; In and out indicate whether the application is in the direction of receiving routes or publishing routes.

Default: RIPng protocol does not filter any received and sent routes

Access list and prefix list are configured in global configuration mode. Please refer to the command manual.

30.2.8 Configure additional routing weight

The additional routing weight is an offset value added to the routing weight of RIPng protocol during input and output. It does not directly change the weight of the route in the routing table, but adds an offset when the interface receives and sends the route.

Mode: RIPng configuration mode

Command: offset list < ACL name > {in | out} < offset > [if name]

Use access list to add an offset to the weight of interface input-output route

Command: no offset list < ACL name > {in | out} < offset > [if name]

Cancel the offset of the weight of the input-output route

Parameter: ACL name indicates the access list name of the reference; In and out indicate whether the application is in the input or output direction; Offset represents the value of the offset, which is between 0 and 16; If name indicates the RIPng interface applied to.

Default: when receiving a message, the additional weight of each route is 1, and when sending a message, the additional weight of each route is 0.

30.2.9 Configure horizontal segmentation

Horizontal segmentation means that the route received from this interface is not sent from this interface. Horizontal segmentation with toxic inversion means that the route received from this interface is still sent from this interface, but its metric value is marked as 16. Horizontal segmentation can avoid loops to a certain extent. The horizontal segmentation with toxic inversion is more efficient than ordinary horizontal segmentation, and direct labeling is not reachable. However, in nBMA network, it is necessary to prohibit horizontal segmentation to obtain the correct route.

Mode: interface configuration mode

Command: IPv6 rip split horizon [poisoned]

Start the horizontal division function of the interface or with toxic inversion

Command: no IPv6 rip split horizon

The horizontal division function of the interface is prohibited

Parameters: no poisoned parameter means to start the normal horizontal segmentation function, and with poisoned parameter means to start the horizontal segmentation function with toxic inversion.

Default: horizontal segmentation with toxic inversion

30.2.10 Configure interface weights

Mode: interface configuration mode

Command: IPv6 rip metric offset < metric >

Configure interface weight

Command: no IPv6 rip metric offset < metric >

Restore the interface weight to the default value

Parameter: the metric value is between 1-16, indicating the weight to be added to the routing entry learned by the interface.

Default: 1

30.2.11 Display information

Mode: normal mode or privileged mod

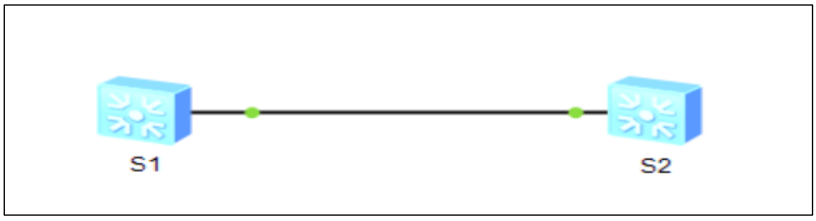
Command: Show IPv6 rip

Displays information about the current system RIPng

Command: Show IPv6 route rip

Displays the currently active RIPng routing information

30.3 RIPng configuration example



S1 switch is configured as follows

Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::1/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 rip
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router rip
Switch(config-vlan1)#

S2 switch is configured as follows

Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::2/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 rip
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router rip
Switch(config-vlan1)#

31. Configuring OSPF

This chapter includes the following contents:

- OSPF Introduction
- OSPF configuration
- Sample OSPF configuration

31.1 OSPF Introduction

OSPF (Open Shortest Path First Protocol Open Shortest Path First) is a protocol based on link-state algorithm, which can support large-scale networks and has fast convergence speed.

Each router running the OSPF protocol maintains a link-state database (LSDB), which describes the topology of the entire autonomous system, like a map. When the databases of all routers are synchronized, each router takes its own perspective, The shortest route to other destination nodes in the autonomous system is calculated and maintained in its own routing table. When the topology of the network changes, the router only needs to encapsulate the changed link state in the link state update (LSU) message and broadcast it, and all the routers will synchronize the local database again and recalculate the route. Each router publishes the link-state broadcast (LSA) it sees and collects them to form the topology description LSDB of the whole network. Convert it to a weighted directed graph, and you can use the SPF algorithm to calculate the routing table.

In the broadcast network, each router needs to broadcast its own state information to other routers, and multiple pairwise adjacencies will be established, which will bring a lot of unnecessary message transmission. For this reason, OSPF specifies a designated router (DR) and a backup designated router (BDR). The router sends the link information to the DR, which collects and collates it and sends it to all routers. The number of adjacencies between routers on the broadcast network is effectively reduced.

OSPF supports five types of protocol messages:

① The HELLO message is periodically broadcasted to the neighbours to discover and maintain the neighbours and conduct DR election. It contains some interface attribute values. Some parameters in the HELLO message must be consistent to establish the neighbours.

② DD message (Database Description) uses DD message to describe its own LSDB during synchronization, including the head of each LSA.An LSA can be uniquely determined through the LSA head, and the peer router can determine whether it has the LSA; if not, it requests a complete LSA.

③ LSR message (Link State Request) After two routers exchange DD messages, they will know which LSAs of the peer router are missing locally. At this time, they need to send LSR messages to request complete LSAs. Only the LSA head is required for the request.

④ LSU message (Link State Update) is a collection of multiple LSAs.

⑤ LSAck message (Link State Acknowledgement) acknowledges the received LSU message to ensure reliable transmission of link information. Confirm with LSA head.

Router-id concept: The unique identification of a router within an autonomous system. area: If OSPF runs in a large network, the number of routers will increase greatly, which will lead to a very large LSDB, increase the time of synchronization and route calculation, and occupy a large amount of storage space and CPU resources. And the larger the network, the more frequent the topology changes, which makes the network often in change, and the router needs to spend a lot of time to transmit messages and calculate the route.It needlessly occupies the network bandwidth.

Therefore, OSPF introduces the concept of area and divides routers into different areas. LSDB only synchronizes and calculates routes in the area, and the routing interaction between areas is completed by the border router (ABR). In this way, the number of routers in the area will be limited, LSDB will be limited to a smaller capacity, the time to calculate the route will be greatly reduced, and the convergence will be fast when the topology changes.

The concept of area effectively groups a large-scale network and undertakes a small-scale routing function within each area. Routes between areas interact on the backbone area (area with area ID 0). Therefore, all non-backbone areas must be connected to the backbone area, that is, the ABR has at least one interface connected to the backbone area. If the network planning indicates that a non-backbone area cannot be connected to the backbone area, a virtual link must be configured to establish a logical path, that is, an ABR in the backbone area and an ABR in the non-backbone area establish a point-to-point link through a transmission area. Then the inter-domain routing information on the backbone area will also be published to the non-backbone area through the virtual link.

31.2 OSPF configuration

After the OSPF protocol is started, enter the OSPF configuration mode to set the corresponding attributes and functions. OSPF configuration commands are mostly used in OSPF configuration mode and interface configuration mode.

The configuration of OSPF includes:

- Start OSPF and enter OSPF mode
- Enable interface
- Specified host
- IDConfigure the router ID
- Configuration of Adjacent Points
- Prohibit the interface from sending messages
- Configure SPF timer
- Configuration management distance
- Introducing external routing
- Configure the network type of the interface
- Configure the time interval for sending the hello message
- Configure that failure time of the neighbour router
- Configure retransmission interval
- Configure interface delay
- Configure the priority of interfaces in DR election
- Configure the cost of sending messages on the interface
- Configure whether to fill MTU value in DD message sent by interface
- Configure interface message authentication
- Configure area virtual link
- Configure regional route aggregation
- Configure regional message authentication
- Configure stub area
- Configure the nssa area
- Configure external route aggregation
- Configure the default metric of the external route

31.2.1 Start OSPF and enter OSPF model

The OSPF protocol can run multiple copies, which are identified by the process number (process-id). When starting the OSPF protocol, it is necessary to specify which process number is started. If there is no parameter, the process number is 0.

Mode: Global Configuration Mode

Command：router ospf [process-id]

Start the OSPF process with process number process-id and enter its model

Command：no router ospf [process-id]

Shut down the OSPF process with process number process-id

Parameter: The value of process-id is between 1 and (216-1), indicating the number of the OSPF process to be started. If the parameter process-id is not included, OSPF with the process number of 0 will be started.

Default: OSPF protocol is not running

31.2.2 Enable interface

The merit of OSPF protocol is that it introduces the idea of layering and divides a complete autonomous system into different areas in order to establish a conceptual hierarchical network model. Zones are logical, artificial groupings of routers in an autonomous system. When different interfaces of a router belong to different areas, that is, across areas, it is called a border router ABR. Each network segment that starts the OSPF protocol can only belong to a specific area, that is, each interface running the OSPF protocol on the router must belong to a specified area. An area is identified by an area number (area-id), and an area with an area number of 0 is a backbone area. Routing information between different areas is passed through border routers. Unlike the RIP protocol, the OSPF protocol must specify the area to which it belongs when it is run on an interface.

Mode: OSPF Configuration Mode

Command：network <network-address> area <area-id>

Specified area specifies the interface running the OSPF protocol

Command：no network <network_address> area <area-id>

Turn off OSPF on a specific interface in a specific area

Parameter: network-address has two forms: A. B. C. D/M and A. B. C. D A. B. C. D. The former specifies the network IP and mask length, and the latter specifies the network IP and mask. There are also two forms of area-id: A. B. C. D, which uses dotted decimal format, and integers, which take values between 0 and (232-1).

Default: The interface is not enabled after the OSPF protocol is started

31.2.3 Specified host

Mode: OSPF Configuration Mode

Command：host <ip-address> area <area-id> [cost <cost>]

Configure Host Routine

Command：no host <ip-address> area <area-id> [cost <cost>]

Cancel Host Route

Parameters: ip-address uses the A. B. C. D format to represent a specific host within an area, which is represented as a stub on the router's link. The area-id is as described in the network command. The cost indicates the cost of the specified link and is an optional parameter.

Default: if cost is not configured, the default is 0

31.2.4 Configure the router ID

The router ID is a 32-bit unsigned integer that uniquely identifies a router in an autonomous system. The router ID can be configured manually to ensure that no two routers in the autonomous system have the same ID. If not configured, the router uses the IP address of the loopback interface; if the loopback has no IP, the highest address is selected from the IP addresses of the current interface as the ID. In order to ensure the stable operation of OSPF, the router ID should be divided and configured manually during network planning.

Mode: OSPF Configuration Mode

Command：ospf router-id <router-id>

Configure the Router ID

Command：no ospf router-id

Cancel Router ID

Command：router-id <router-id>

Command：no router-id [router-id]

Parameters: router-id uses the A. B. C. D format

Default: When the OSPF protocol is started, the router ID is automatically generated according to the rules. The rule is as follows: firstly, select the router-id configured by the command; if there is no router-id, select the IP address of the loopback; if there is no router-id, select the highest IP address of the current interface; if there is no router-id, select 0.0.

Both sets of commands have the same function.

31.2.5 Configuration of Adjacent Points

The OSPF protocol interaction protocol message uses a multicast address 224.0, 0.5 or 224.0, and 0.6 in a multicast mode. When the OSPF protocol runs on a link that does not support broadcasting, such as NBMA, some configuration must be made to use unicast to exchange protocol messages. In this case, you can manually specify the IP address of the peer and the corresponding attribute value.

Mode: OSPF Configuration Mode

Command：neighbour <ip-address> [priority <prio> | poll-interval <deadtime> | cost <cost>]

Specify Opposite Adjacency Points and Set Properties

Command：no neighbour <ip-address> [priority <prio> | poll-interval <deadtime> | cost <cost>]

Cancel setting of adjacent point and attribute of opposite end

Parameter: ip-address: the IP address of the opposite end, in the format of A. B. C. D; prio: the priority of the opposite end, with the value ranging from 0 to 255; deadtime: the timing when the opposite end is considered to be down. If the timing is terminated, no hello message will be sent to the opposite end, with the value ranging from 1 to (216-1); The cost is the cost of the link to the opposite end, and the value is between 1 and (216-1).

Default: priority is 1 (if it is 0, it will not participate in DR election); poll-interval is 120 seconds; cost is 10.

31.2.6 Prohibit the interface from sending messages

In a simple network, when the interface of the OSPF protocol only represents a network segment between two devices and is only used for data transmission, the interface is set to the passive state, and the hello message is blocked from being broadcast on the link, which does not affect the acquisition of the interface route.

Mode: OSPF Configuration Mode

Command：passive-interface <if-name>

Configure the interface to be passive

Command：no passive-interface <if-name>

Cancel the passive state of the interface

Parameter: if-name is the name of the three-layer interface (for example: vlan1 vlan2 …)

Default: The interfaces that are enabled after the OSPF protocol is started are not passive

If the interface running the OSPF protocol is designated as passive, the directly connected route of the interface can still be published, but the OSPF message on the interface will be blocked, and the interface cannot establish a neighbour relationship. In some networking cases, it can effectively save network resources.

31.2.7 Configure SPF compute times

When the link state database (LSDB) of OSPF changes, the shortest path needs to be recalculated. If the shortest path is calculated immediately for each change, it will take up a lot of resources and affect the efficiency of the router. By configuring the two values delay and hold to adjust the time interval of the SPF calculation, the frequent SPF calculation caused by the frequent change of the network can be inhibited, so as to avoid occupying a large amount of system resources in one time and affecting the operation efficiency of the router.

The SPF calculation has a timer that starts the next calculation each time according to the dead time. When the timer expires and needs to start the SPF calculation, recalculate the holdback time from the last SPF calculation to this time, and if the configured holdback time has been exceeded, use the configured delay time to start the timer. If the configured holdback time has not been exceeded, the configured holdback time is used to calculate the required delay time. If the delay time is less than the configured delay time, the configured delay time is used, otherwise, the calculated delay time is directly used to start the SPF calculation.

Mode: OSPF Configuration Mode

Command：timers spf <delay> <hold>

Configure the delay and hold values for the SPF calculation interval

Command：no timers spf

Revert to Default

Parameters: delay indicates the time required for calculating SPF; hold indicates the time required for restraining between two SPF calculations.

Default: delay is 5S; hold is 10 second

31.2.8 Configuration management distance

Multiple routing protocols can be running on a router at the same time, and administrative distance is required to select from the routing information learned by multiple routing protocols. When different protocols find the same route, the one with smaller administrative distance is preferred.

Mode: OSPF Configuration Mode

Command：distance <distance>

Configuration Management Distance

Command：no distance <distance>

The recovery administrative distance is the default

Command：distance ospf {intra-area <distance> | inter-area <distance> | external <distance>}

Configure different types of administrative distances

Command：no distance ospf

Restore three types of administrative distances to default values

Parameter: the value of distance is between 1 and 255; intra-area represents the administrative distance of intra-domain routing; inter-area represents the administrative distance of inter-domain routing; and external represents the management distance of external routing.

Default: The administrative distance of OSPF protocol is 110; the administrative distance of intra-domain route, inter-domain route and external route is 0.

31.2.9 Introducing external routing

Multiple dynamic routing protocols can run on a router, and different routing protocols can share routing information. OSPF regards the routes learned by other routing protocols as routes outside the autonomous system, which are introduced by the autonomous system boundary router ASBR. Attributes such as weight and weight type can be specified when introducing an external route.

There are four types of OSPF routes: intra-domain routes and inter-domain routes, both of which are within the autonomous system; and external routes of type-1 and type-2, both of which describe routes to destinations outside the autonomous system. The route of type-1 is the route from other IGP. OSPF considers that its credibility is relatively high, and it is comparable with the route weight in the autonomous system. Therefore, the cost of this kind of external route is the sum of the cost of the router itself to the ASBR and the cost of the ASBR to the destination. The route of type-2 is the route from other EGPs. OSPF considers that its credibility is not very high, and its cost is far greater than that of the route in the autonomous system, so it is not comparable. Therefore, the cost of this kind of external route only uses the cost of ASBR to the destination and ignores the cost of the router itself to ASBR.

Mode: OSPF Configuration Mode

Command：redistribute {kernel | connected | static | rip | isis | bgp} [metric <metric> | metric-type <type> | route-map <route-map-name> | tag <tag>]

Command：no redistribute {kernel | connected | static | rip | isis | bgp} [metric <metric> | metric-type <type> | route-map <route-map-name> | tag <tag>]

Parameter: the first required parameter is the type of external route that can be introduced, including direct connection, static, RIP, IS-is and BGP; the second parameter is the weight value set when introducing external route, and the value is between 0 and (224-1); The third parameter is the two types of external routes introduced, including type-1 and type-2, where type-1 is the IGP route and type-2 is the EGP route. The third parameter is the name of the referenced route-map, which is

configured in the global configuration mode. Refer to the command manual; The fourth parameter is tag, and the value is between 0 and (232-1), which is the external routing attribute.

Default: No external routing protocol is introduced

31.2.10 Configure the network type of the interface

The OSPF protocol is based on its own router. Each router describes its adjacent network topology and passes it to other routers. OSPF divides the network type of the interface link into four types according to the protocol type of the link layer: the broadcast type (the protocol of the link layer is Ethernet, FDDI, etc.); the NBMA non-broadcast multiple access type (the protocol of the link layer is FR, ATM, HDLC, X.25, etc.); The third is the point-to-multipoint type. No link layer protocol is considered to be point-to-multipoint by default. The point-to-multipoint type must be forcibly configured by other network types. The most common practice is to change a partially connected NBMA to a point-to-multipoint network. Fourth, point-to-point type (link layer protocols are PPP, LAPB, POS).

On broadcast networks that do not have multiaccess capability, interfaces can be configured as NBMA type. Interfaces can be configured as point-to-multipoint when not all routers in the NBMA network are directly reachable from each other.

The NBMA network agreed in the OSPF protocol is fully connected, non-broadcast, and multi-point reachable. A point-to-multipoint network is not necessarily fully connected. NBMA requires DR selection, and there is no DR in a point-to-multipoint network. The NBMA network multicasts the message through the designated neighbour unicast message and the point-to-multipoint network.

Mode: Interface configuration model

Command：ip ospf network <type>

Configure the network type for the interface link

Command：no ip ospf network

Restore the network type of the interface link to the default values

Parameter: type can select broadcast, non-broadcast, point-to-point, point-to-multipoint [non-broadcast]; The first type is a broadcast network, the second type is a non-broadcast network, that is, NBMA, the third type is a point-to-point network, and the fourth type is a point-to-multipoint network; the point-to-multipoint network is divided into a broadcast network and a non-broadcast network, and a non-broadcast neighbour cannot be automatically discovered and must be specified.

Default: broadcast network

31.2.11 Configure the time interval for sending the hello message

The Hello message is sent to the neighbour router periodically to discover and maintain the neighbour relationship, and to elect the DR and BDR. The interval of Hello messages can be configured manually, but the interval of hello timers between neighbours in the network should be kept consistent. The value of the Hello timer is inversely proportional to the router convergence rate and the network load.

Mode: Interface configuration model

Command：ip ospf hello-interval <seconds>

Configure the interval for the hello timer

Command：no ip ospf hello-interval

Restore hello timer interval to default

Parameter: seconds is between 1 and (216-1), indicating the time interval between two hello messages.

Default: hello interval of 10 seconds on broadcast and point-to-point networks; hello interval of 30 seconds on NBMA and point-to-multipoint networks**.**

31.2.12 Configure that failure time of the neighbour router

Mode: Interface configuration model

Command：ip ospf dead-interval <seconds>

Configure neighbour expiration times

Command：no ip ospf dead-interval

The recovery neighbour expiration time is the default value

Parameter: the value of seconds is between 1 and (216-1), indicating that the neighbour is considered to be invalid if the hello message of the neighbour is not received after seconds. The dead timer of the neighbour will be updated every time the hello message is received.

Default: The neighbour failure time is 40 seconds on the broadcast network and the point-to-point network; the neighbour failure time is 120 seconds on the NBMA network and the point-to-multipoint network; when the network type is modified, the hello interval and the dead interval will use the default values.

31.2.13 Configure retransmission times

OSPF is a reliable link-state protocol, which is reflected in the fact that the LSU messages it interacts with require an LSU-ack response from the opposite end. When the acknowledgement message is received, the link state update is considered to have been received. If no acknowledgement is received within the retransmission interval, the LSA is retransmitted to the neighbor. The retransmission interval can be configured manually. It needs to be longer than the round-trip time of a message transmitted between two routers. If it is set too small, it will cause unnecessary retransmission.

Mode: Interface configuration model

Command：ip ospf retransmit-interval <seconds>

Configure the retransmission interval for the interface

Command：no ip ospf retransmit-interval

The recovery retransmission interval is the default

Parameter: seconds is between 1 and (216-1), which indicates the interval of retransmission when the peer does not receive the LSA.

Default: retransmission interval is 5S

31.2.14 Configure interface delay

Each link state broadcast LSA in the link state update message LSU has an age time domain, and the transmission delay of the sending interface needs to be added before transmission. This parameter mainly considers the time required by the interface to send the message, especially in the low-speed network, this parameter needs to be configured.

Mode: Interface configuration model

Command：ip ospf transmit-delay <seconds>

Sets the transmission delay for the interface

Command：no ip ospf transmit-delay

The transmission delay of the recovery interface is the default value.

Parameter: The value of seconds is between 1 and (216-1), indicating that the age field of the LSA sent on this interface needs to increase this delay value.

Default: the transmission delay of the interface is 1s

31.2.15 Configure the priority of interfaces in DR election

In the broadcast network, in order to avoid repeated point-to-point transmission of link information, it is necessary to elect a designated router DR and BDR responsible for broadcasting the link information in the network segment. The priority of an interface indicates its qualification in the election of a DR. In the event of a conflict in the election, the interface with the highest priority is considered first. If the priority is 0, the router does not participate in the election, and if the priority is greater than 0, the router is a candidate. Each router contains its own priority information and its own DR in its own hello message, which is broadcast in the broadcast network. Finally, the router with higher priority is selected as the DR. If the priority is equal, the router ID with higher priority will be compared.

Aft that DR fails, the router in the network need to go through a process of re-electing the DR, which takes a long time and cause routing calculation errors during this time. The concept of BDR is to smooth the transition to the new DR. The BDR is the backup of the DR and is elected at the same time in the DR election. It also establishes an adjacency relationship with other routers in the network, but the node for collecting and publishing information in the network is in the DR instead of the BDR, and the BDR only maintains the synchronization of the adjacency. When the DR fails, the BDR immediately becomes the DR and is responsible for collecting the information in the network segment. At this time, a new process is started to elect the BDR, but the election of the BDR does not affect the calculation of the route.

Mode: Interface configuration model

Command：ip ospf priority <prio>

Configure the priority of the interface in DR election

Command：no ip ospf priority

Restore interface priority as default

Parameter: The value of prio is 0 ~ 255, indicating the priority in DR selection. When it is 0, it means not participating in the election.

Default: Priority is 1

31.2.16 Configure the cost of sending messages on the interface

Traffic is controlled by configuring different links with different costs in the network, and the cost of an interface represents the cost of sending messages from the interface. If not configured manually, OSPF will automatically calculate the interface cost based on the interface baud rate.

Mode: Interface configuration model

Command：ip ospf cost <cost>

Command：no ip ospf cost

Parameter: The cost value is between 1 and (216-1), indicating the cost of sending a message on this interface.

Default: Interface cost 10

31.2.17 Configure whether to fill MTU value in DD messages sent by interface

Mode: Interface configuration model

Command：ip ospf mtu-ignore

Set the MTU value in the DD message not to be checked

Command：no ip ospf mtu-ignore

Cancel Do not check MTU value in DD message

Default: Check MTU value in DD message

31.2.18 Configure interface message authentication

The message authentication of OSPF protocol on the interface supports plaintext mode and MD5 mode.

Mode: Interface configuration model

Command：ip ospf authentication <mode>

Configure Authentication Mode

Command：no ip ospf authentication

Decertification

Parameter: No parameter means clear text authentication; message-digest means MD5 authentication; null means no authentication

Command：ip ospf authentication-key <password>

Configure plaintext authentication password strings

Command：no ip ospf authentication-key

Cancel plaintext authentication password string

Parameter: password represents the password string for plaintext authentication

Command：ip ospf message-digest-key <key-id> md5 <password>

Configure MD5 authentication password

Command：no ip ospf message-digest-key <key-id>

Cancel MD5 authentication password

Parameter: the value of key-id is between 1 and 255, which is used to sort in the key chain; password represents the password string.

Default: No authentication is configured

31.2.19 Configure area virtual link

The OSPF protocol uses the idea of layering to divide the routers in the autonomous system into different groups. These groups are called areas. All areas are not equal, but have a hierarchical relationship. Among them, the 0.0. 0.0 area is the most special, which is the backbone area. Other non-backbone areas must exchange inter-domain routes through the backbone area. Therefore, all non-backbone areas must be connected to the backbone area, that is, at least one interface on the ABR is in area 0. If some areas cannot ensure physical access to the backbone area due to the limitation of network topology, virtual links need to be configured to ensure logical access. Both ends of the virtual link are ABRs, and the middle passes through a non-backbone area, which is called a transit area. When configuring the virtual link, it is necessary to specify the ID of the transmission area and the ID of the ABR at the opposite end, which must be configured on the ABRs at both ends to take effect.

When the virtual link is activated after the route of the transmission area is calculated, it is logically equivalent to forming a point-to-point connection between two endpoints, so the parameters of the interface can be configured on the physical interface and the authentication function can be started.

What is transmitted between the ABRs is a unicast packet, and the router that forwards the unicast packet in the transmission area forwards it as an ordinary IP packet, so it can only be understood that

a logical link is provided in the transmission area, and protocol packets can be exchanged between the two ABRs.

Mode: OSPF Configuration Mode

Command： area <area-id> virtual-link <router-id>

Configure the transmission area of the virtual link and the ID of the opposite end

[authentication <mode> |

Configure the authentication mode of the virtual link

authentication-key <password> |

Configuring virtual link plaintext authentication password

message-digest-key <key-id> md5 <password> |

Configure virtual link MD5 authentication password

hello-interval <seconds> |

Configure the hello interval for the virtual link

dead-interval <seconds> |

Configure Virtual Link Neighbour Failure Time

retransmit-interval <seconds> |

Configure virtual link retransmission interval

transmit-delay <seconds> |

Configuring virtual link interface delay

Command： no area <area-id> virtual-link <router-id>

[authentication <mode> |

authentication-key <password> |

message-digest-key <key-id> md5 <password> |

hello-interval <seconds> |

dead-interval <seconds> |

retransmit-interval <seconds> |

transmit-delay <seconds>]

Cancel Virtual Link Settings

Parameter: Area-id represents the ID of the transmission area. It can be a A. B. C. D in dotted decimal format or an integer format. The value is between 0 and (232-1). Router-id represents the ID of the router at the opposite end of the virtual link, in A. B. C. D format. The authentication and sending interface attributes are optional. Please refer to the related command description.

Default: no virtual link is configured

31.2.20 Configure regional route aggregation

Mode: OSPF Configuration Mode

Command： area <area-id> range <ip-prefix> [advertise | not-advertise]

Configure Aggregation Range

Command： no area <area-id> range <ip-prefix> [advertise | not-advertise]

Unaggregate

Parameter: Area-id represents the area ID, and specifies to aggregate the routes in the area. It can be A. B. C. D in dotted decimal format or integer format, and the value is between 0 and (232-1). Ip-prefix uses the prefix format A. B. C. D/M to indicate the aggregation range. The optional parameters advertise and not-advertise indicate whether to broadcast the aggregation range, that is, ip-prefix. The original network routes are broadcast.

31.2.21 Configure regional message authentication

All routers in an area need to have the same authentication type. The authentication password string of all routers in a network segment shall be consistent. The configuration area authentication only starts the authentication function (plaintext or MD5), and the password uses the corresponding **configuration value of the interface. Refer to the interface message authentication configuration.**

Mode: OSPF Configuration Mode

Command：area <area-id> authentication [message-digest]

Configure Regional Authentication Mode

Command：no area <area-id> authentication

Cancellation of regional certification

Parameter: Area-id represents the area ID and specifies the area to be authenticated; the dotted decimal format A. B. C. D can be used, and the integer format can also be used; the value is between 0 and (232-1). No optional parameter indicates plaintext authentication, and message-digest indicates MD5 authentication.

Default: regional authentication is not enabled

31.2.22 Configure stub area

Mode: OSPF Configuration Mode

Command：area <area-id> stub [no-summary] **Configure the router to be in the stub area**

Command：no area <area-id> stub [no-summary] **Remove the router from the stub zone**

Command：area <area-id> default-cost <cost>

Configure the default cost for ABR broadcast routes connected to the stub area

Command：no area <area-id> default-cost

The default cost of recovery is the default

Parameter: Area-id represents area ID, indicating which area attribute is stub; A. B. C. D in dotted decimal format or integer format can be used, and the value is between 0 and (232-1). No-summary means that no inter-domain route is injected into the stub area.

The first set of commands configures the router in the stub area, and the second set of commands configures the ABR with the interface connected to the stub area.

Default: Do not configure stub area

31.2.22 Configure the nssa area

Mode: OSPF Configuration Mode

Command：area <area-id> nssa [options] **Configure nssa properties**

Command：no area <area-id> nssa [options] **Unset the nssa zone attribute**

Parameters: area-id indicates the area ID. For details about options, see the command manual.

Default: nssa zone is not configured

31.2.23 Configure external route aggregation

Routes introduced from other protocols are broadcasted one by one in the LSU of type-5. Use the aggregation command to specify a prefix range in which the covered routes are suppressed and only the aggregated route is broadcasted. When the number of external routes is huge, it can effectively reduce the size of the LSDB.

Mode: OSPF Configuration Mode

Command：summary-address <ip-prefix> [not-advertise | tag <tag>]

Configure the aggregation scope and properties

Command：no summary-address <ip-prefix> [not-advertise | tag <tag>]

Unaggregate external route

Parameter: ip-prefix uses the address prefix format A. B. C. D/M to indicate the route range to be aggregated; Not-advertise indicates that the aggregated route will not be broadcasted; tag is the set tag value, the value is between 0 and (232-1), and the default is 0.

Default: Do not aggregate external incoming rout

31.2.24 Configure the default metric of the external route

When external routes are introduced, the default metric is used if the redistribute command does not specify a metric value.

Mode: OSPF Configuration Mode

Command：default-metric <metric>

Configure the default metric when importing an external route

Command：no default-metric [metric]

Restore the default weight to the default value when the external route is introduced

Parameter: metric value is between 0 and (224-1)

Default: The default weight value is 1

31.2.25 Display Information

Mode: Normal or Privileged

Command：show ip protocols

Command：show ip protocols ospf **Display OSPF protocol information**

Command：show ip ospf [process-id] **Display OSPF process information**

Parameter: instance-id is the process number

Take values between 0- (216-1).

Command：show ip ospf border-routers **Display ABR information**

Command：show ip ospf database <type> **Display LSDB information**

Parameter: type is the LSA of each type and the summary information. See the command manual for details.

Command：show ip ospf interface [if-name] **Display OSPF interface information**

Parameter: if-name is the agreed three-layer interface name

Command：show ip ospf route [count] **Displays the OSPF routing table**

Parameter: count means to display the total number of entries in the routing table

Command：show ip ospf virtual-links **Displays OSPF virtual connection information**

Command：show ip ospf neighbor [options] **Displays OSPF neighbour information**

Parameters: options See the command manual for details.

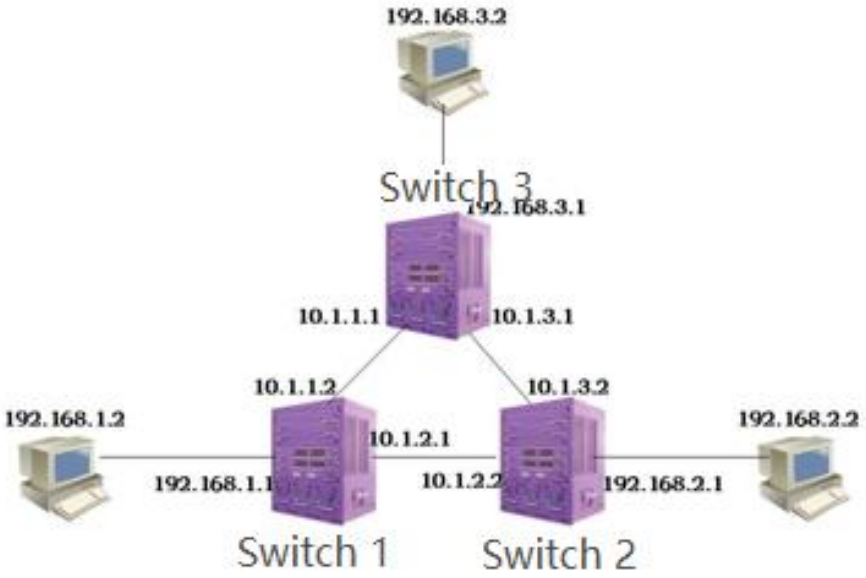
Mode: Privileged Mode

Command：show running-config

Displays the current configuration of the switch, including OSPF configuration.

Command：show running-config ospf **Displays the current configuration of the OSPF protocol**.

31.3 Sample OSPF configuration



(1) configuration

The three switches are connected in pairs and have six network segments respectively, and the OSPF protocol is enabled to realize the intercommunication between the three PCs in pairs. Interfaces are required to be in the same area, area 0.

On Switch 1:

Switch#configure terminal

Switch(config)#router ospf 100

Switch(config-ospf-100)#network 10.1.1.0/24 area 0

Switch(config-ospf-100)#network 10.1.2.0/24 area 0

Switch(config-ospf-100)#network 192.168.1.0/24 area 0

On Switch 2:

Switch#configure terminal

Switch(config)#router ospf 100

Switch(config-ospf-100)#network 10.1.2.0/24 area 0

Switch(config-ospf-100)#network 10.1.3.0/24 area 0

Switch(config-ospf-100)#network 192.168.2.0/24 area 0

On Switch 3:

Switch#configure terminal

Switch(config)#router ospf 100

Switch(config-ospf-100)#network 10.1.1.0/24 area 0

Switch(config-ospf-100)#network 10.1.3.0/24 area 0

Switch(config-ospf-100)#network 192.168.3.0/24 area 0

(2) Verification

show ip ospf database

show ip ospf interface

show ip ospf neighbor

show ip route ospf

show ip ospf route

32. Configuring OSPFv3

This chapter includes the following contents：

- OSPFv3 introduction
- OSPFv3 configuration
- OSPFv3 configuration example

32.1 OSPFv3 introduction

OSPF (open shortest path first) is an internal gateway protocol based on link state developed by IETF Interior gateway protocol.

At present, OSPF version 2 is used for IPv4 protocol and OSPF version 3 is used for IPv6 protocol.

- OSPFv3 is short for OSPF version 3.
- OSPFv3 is an OSPF routing protocol running on IPv6 (rfc5340, the same as rfc2740).
- OSPFv3 is modified on the basis of ospfv2 and is an independent routing protocol。

The main purpose of OSPFv3 is to develop a routing protocol independent of any specific network layer. To achieve this,

The internal router information of OSPFv3 has been redesigned.

OSPFv3 differs from ospfv2 in that：

- OSPFv3 does not insert IP based data into the header of the message at the beginning of the packet and link state announcement (LSA) Data.
- OSPFv3 uses information independent of network protocol to perform key tasks that required IP message header data in the past Services, such as identifying the LSA that publishes routing data。

Basic principle of OSPFv3

OSPFv3 is an OSPF routing protocol (rfc2740) running on IPv6. It is added on the basis of ospfv2

Strong, is an independent routing protocol。

- working principle and of OSPFv3 in Hello message, state machine, LSDB, flooding mechanism, routing calculation, etc Ospfv2 is consistent.
- OSPFv3 protocol divides the autonomous system into one or more regions in the logical sense through LSA (link) Publish routes in the form of state advertisement.
- OSPFv3 relies on the interaction of OSPFv3 messages between devices in OSPFv3 area to achieve the unification of routing information.
- OSPFv3 message is encapsulated in IPv6 message and can be sent in the form of unicast and multicast.

OSPFv3 Message type

Message type	Message function
Hello Message	Send periodically to discover and maintain OSPFv3 neighbour relationship.
DD Message（Database Description packet）	Describes the summary information of the local LSDB, which is used for database synchronization between two devices.
LSR Message（Link State Request packet）	Used to request the required LSA from the other party. The device will send LSR message to OSPFv3 neighbours only after they successfully exchange DD message.
LSU Message（Link State Update packet）	Send the required LSA to the other party.
LSAck Message（Link State Acknowledgment packet）	Used to confirm the received LSA.

LSA type	LSA function
Router-LSA（Type1）	The device will generate an LSA for the area where each OSPFv3 interface is running, which describes the link state and overhead of the device and propagates in the area to which it belongs.
Network-LSA（Type2）	Generated by Dr, it describes the link state of the link and propagates in the area to which it belongs.
Inter-Area-Prefix-LSA（Type3）	Generated by ABR, it describes the route of a network segment in the area and notifies other relevant areas.
Inter-Area-Router-LSA（Type4）	Generated by ABR, it describes the route to ASBR and notifies other relevant areas except the area where ASBR is located.
AS-external-LSA（Type5）	Generated by ASBR, it describes the route outside the as and notifies all areas (except stub area and NSSA area).
NSSA LSA（Type7）	enerated by ASBR, it describes the route to the outside of the as and propagates only in the NSSA area
Link-LSA（Type8）	Each device will generate a link LSA for each link, describe the link local address and IPv6 prefix address on this link, and provide the link options that will be set in the network LSA. It only propagates within this link.
Intra-Area-Prefix-LSA（Type9）	Each device and Dr will generate one or more such LSAS and propagate in its area such LSA generated by the equipment, describing the IPv6 prefix address associated with the route LSA such LSA generated by Dr, describing the IPv6 prefix address associated with the network LSA。

32.2 OSPFv3 configuration

32.2.1 Start OSPFv3 and enter OSPFv3 configuration mode

OSPFv3 protocol can run multiple copies, which are identified by process ID; When starting OSPFv3 protocol, it is necessary to specify which process number is started; If there are no parameters, the process number is 0.

Mode: global configuration mode

Command: router IPv6 OSPF [process ID]

Start OSPFv3 process with process ID and enter its mode

Command: no IPv6 Router OSPF [process ID]

Close OSPFv3 process with process ID

Parameter: the value of process ID is between 1 and 216-1, indicating the OSPF process number started; If there is no parameter process ID, OSPFv3 with process number 0 will be started.

Default: OSPFv3 protocol is not running

32.2.2 Configure router ID

The router ID is a 32-bit unsigned integer, which is the unique identification of a router in the autonomous system. The router ID can be configured manually. During configuration, it is necessary to ensure that the IDs of any two routers in the autonomous system are different. If not configured, the router uses the IP address of the loopback interface; If loopback has no IP address, select the highest address from the IP addresses of the current interface as the ID. In order to ensure the stable operation of OSPFv3, the router ID should be divided and configured manually during network planning.

Mode: OSPFv3 configuration mode

Command: router ID < router ID > **Configure router ID**

Command: no router ID **Cancel router ID**

Command: router ID < router ID >

Command: no router ID [router ID]

Parameter: router ID uses a.b.c.d format

Default: after OSPFv3 protocol is started, the router ID will be automatically generated according to the rules. The rules are as follows: first, select the router ID configured by the command; If not, select the IP address of loopback; If not, select the highest IP address of the current interface; 0.0.0.0 if none.

The functions of the two groups of commands are the same.

32.2.3 Prohibit the interface from sending messages

When in a simple network, the interface of OSPFv3 protocol only represents a network segment between two devices for data transmission, set the interface to passive state and block the Hello message broadcast on its link, which does not affect the knowledge of the interface route.

Mode: OSPFv3 configuration mode

Command: passive interface < if name > **Configure the interface to be passive**

Command: no passive interface < if name > **Cancel interface passive state**

Parameter: if name is the name of the three-tier interface (for example: vlan1, vlan2...)

Default: after OSPFv3 protocol is started, all enabled interfaces are not in passive state

Specify the interface running OSPFv3 protocol as passive state, and the direct route of the interface can still be published, but the OSPFv3 message on the interface will be blocked, and the interface cannot establish neighbor relationship. In some networking cases, it can effectively save network resources.

32.2.4 Configure SPF calculation time

When the link state database LSDB of OSPFv3 changes, the shortest path needs to be recalculated. If the shortest path is calculated immediately for each change, it will occupy a lot of resources and affect the efficiency of the router. By configuring the two values of delay and hold to adjust the time interval of SPF calculation, we can restrain the too frequent SPF calculation caused by the frequent changes of the network, so as to avoid occupying a lot of system resources in one time and affecting the operation efficiency of the router.

SPF calculation has a timer, which starts the next calculation according to the inhibition time each time. When SPF calculation needs to be started when the timer terminates, recalculate the inhibition time from the last SPF calculation to this time. If the configured inhibition time has been exceeded, use the configured delay time to start the timer. If the configured inhibit time has not been exceeded, the configured inhibit time is used to calculate the required delay time. If the delay time is less than the configured delay time, use the configured delay time; otherwise, directly use the calculated delay time to start SPF calculation.

Mode: OSPFv3 configuration mode

Command: timers SPF < delay > < hold >

Configure the delay and hold values of SPF calculation interval

Command: no timers SPF **Restore to default**

Parameter: delay indicates the delay time required to calculate SPF; Hold indicates the time to suppress between two SPF calculations.

Default: delay is 5S; Hold is 10 seconds

32.2.5 Configure management distance

Multiple routing protocols can be run on the router at the same time. How to choose from the routing information learned by multiple routing protocols requires the use of management distance. When different protocols find the same route, the one with small management distance is preferred.

Mode: OSPFv3 configuration mode

Command: distance < distance > **Configure management distance**

Command: no distance < distance >

The recovery management distance is the default value

Command: distance OSPFv3 {intra area < distance > | inter area < distance > | external < distance >}

Configure different types of management distances

Command: no distance OSPFv3

Restore the three types of management distance to the default value

Parameter: distance is between 1 and 255; Intra area refers to the management distance of routes in the domain; Inter area refers to the management distance of inter domain routing; External indicates the management distance of the external route.

Default: the management distance of OSPFv3 protocol is 110; The management distance of intra domain route, inter domain route and external route is 0.

32.2.6 Introducing external routing

Multiple dynamic routing protocols can be run on the router, and routing information can be shared between different routing protocols. OSPFv3 regards the route learned by other routing protocols as the route outside the autonomous system, which is introduced by the autonomous system boundary

router ASBR. When introducing an external route, you can specify attributes such as weight and weight type.

OSPFv3 has four types of routes. One is intra domain routing, and the other is inter domain routing. These two types of routes are in autonomous systems; The third is the external route of type-1, and the fourth is the external route of type-2. These two types of routes describe the route to the destination outside the autonomous system. The route of type-1 is from other IGPS. OSPFv3 believes that it has high reliability and is comparable with the route weight in the autonomous system. Therefore, the cost of this kind of external route is the sum of the cost from the router itself to ASBR and the cost from ASBR to the destination. The route of type-2 is from other eGPS. OSPFv3 believes that its reliability is not very high, and its cost is far greater than that in the autonomous system, so it is not comparable. Therefore, the cost of this kind of external route only uses the cost from ASBR to the destination, and ignores the cost from the router itself to ASBR.

Mode: OSPFv3 configuration mode

Command: redistribute {kernel | connected | static | rip | Isis | BGP} [Metric < metric > | metric type < type > | route map < route map name > | tag < tag >]

Command: no redistribute {kernel | connected | static | rip | Isis | BGP} [Metric < metric > | metric type < type > | route map < route map name > | tag < tag >]

Parameter: the first required parameter is the type of external route that can be introduced, including direct connection, static, rip, IS-IS and BGP; The second parameter is the weight value set when introducing external route, which is between 0 ~ 224-1; The third parameter is the introduction of two types of external routes, which are divided into type-1 and type-2. Type-1 is IGP route and type-2 is EGP route; The third parameter is the name of the referenced route map. The route map is configured in the global configuration mode. Please refer to the command manual; The fourth parameter is tag, which is between 0 and 232-1. It is an external routing attribute.

32.2.7 Configure the network type of the interface

OSPFv3 protocol takes its own router as the perspective. Each router describes its adjacent network topology and passes it to other routers. OSPFv3 divides the network types of interface links into four types according to the link layer protocol types: one is the broadcast type (the link layer protocols are Ethernet, FDDI, etc.); The second is nBMA non broadcast multiple access type (link layer protocols are fr, ATM, HDLC, X.25, etc.); The third is the point to multipoint type. No link layer protocol will be regarded as the point to multipoint type by default. The point to multipoint type must be forcibly configured by other network types. The most common approach is to change the non fully connected nBMA to point to multipoint network. The fourth is the point-to-point type (the link layer protocols are PPP, LAPB and POS).

On broadcast networks without multiple access capability, the interface can be configured as nBMA type. When not all routers are directly accessible in nBMA network, the interface can be configured as point to multipoint type.

The nBMA network agreed in OSPFv3 protocol is fully connected, non broadcast and multi-point reachable. Point to multipoint networks are not necessarily fully connected. NBMA needs to select Dr, and there is no DR in point to multipoint network. NBMA network multicast message through designated neighbor unicast message and point-to-multipoint network multicast message.

Mode: interface configuration mode

Command: IPv6 ospf network < type > **Configure the network type of the interface link**

Command: no IPv6 ospf network

The network type of the recovery interface link is the default value

Parameter: Type: you can select broadcast, non broadcast, point to point, point to multipoint [non broadcast]; The first type is broadcast network, the second type is non broadcast network, i.e. nBMA, the third type is point-to-point network, and the fourth type is point-to-multipoint network; Point to multipoint networks are divided into broadcast and non broadcast networks. Non broadcast neighbors cannot be found automatically and must be specified.

Default: broadcast network

32.2.8 Configure Hello message sending interval

Hello message is used to send to neighbour router periodically, find and maintain neighbour relationship, and elect DR and BDR. The interval of Hello message can be configured manually, but attention should be paid to keeping the interval of Hello timer between neighbours in the network consistent. The value of Hello timer is inversely proportional to the convergence speed of router and network load.

Mode: interface configuration mode

Command: IPv6 OSPF Hello interval < seconds > **Configure the interval of Hello timer**

Command: no IPv6 OSPF Hello interval **Restore the Hello timer interval to the default value**

Parameter: the value of seconds is between 1 and 216-1, indicating the time interval between two Hello message sending.

Default: on broadcast network and point-to-point network, the Hello interval is 10 seconds; On nBMA network and point to multipoint network, the Hello interval is 30 seconds.

32.2.9 Configure neighbour router expiration time

Mode: interface configuration mode

Command: IPv6 OSPF dead interval < seconds > **Configure neighbour expiration time**

Command: no IPv6 OSPF dead interval **Recovery neighbour failure time is the default value**

Parameter: the value of seconds is between 1 and 216-1, which means that the neighbour is considered invalid if no Hello message is received after seconds; Every time a hello message is received, the neighbour's dead timer will be updated.

Default: the failure time of neighbours on broadcast network and point-to-point network is 40 seconds; On nBMA network and point to multipoint network, the neighbour failure time is 120 seconds; When the network type is modified, the Hello interval and dead interval will use the default values.

32.2.10 Configure retransmission time

OSPFv3 is a reliable link state protocol, which is manifested in that the LSU messages it interacts with need the LSU ack from the opposite end. When receiving the confirmation message, the party considers that the link state update is received. If no acknowledgement message is received within the retransmission interval, the LSA will be retransmitted to the neighbor. The retransmission interval can be configured manually. It needs to be longer than the time for a message to be transmitted back and forth between two routers. If it is set too small, it will cause unnecessary retransmission.

Mode: interface configuration mode

Command: IPv6 OSPF retransmit interval < seconds >

Configure the retransmission interval of the interface

Command: no IPv6 OSPF retransmit interval

The recovery retransmission interval is the default value

Parameter: the value of seconds is between 1 and 216-1, which indicates the interval of retransmission when the opposite end does not receive LSA.

Default: retransmission interval 5S

32.2.11 Configure interface delay

In the link state update message LSU, each link state broadcast LSA has a time domain. Before transmission, it is necessary to increase the transmission delay of the transmitting interface. This parameter mainly considers the time required for the interface to send messages, especially on low-speed networks.

Mode: interface configuration mode

Command: IPv6 OSPF transmit delay < seconds >

Set the transmission delay of the interface

Command: no IPv6 OSPF transmit delay

The transmission delay of the recovery interface is the default value

Parameter: the value of seconds is between 1 and 216-1, indicating that the delay value needs to be increased in the age domain of the LSA sent by the interface.

Default: the transmission delay of the interface is 1s

32.2.12 Configure the priority of interface in Dr election

In order to avoid repeated point-to-point transmission of link information in the broadcast network, it is necessary to elect the designated router DR and BDR to be responsible for broadcasting the link information in the network segment. The priority of the interface indicates its qualification in the election of Dr. in case of election conflict, the one with higher priority shall be considered first. If the priority is 0, they will not participate in the election. If the priority is greater than 0, they are candidates. Each router contains its own priority information and its own DR in its own Hello message, broadcasts in the broadcast network, and finally selects the one with higher priority to become Dr. If the priorities are equal, the higher the router ID will prevail.

When Dr fails, the router in the network needs to go through a process of re electing Dr, which takes a time, and during this time, it will cause routing calculation errors. The concept of BDR is to make a smooth transition to the new Dr. BDR is the backup of Dr. it is selected at the same time in the Dr election. It also establishes an adjacency relationship with other routers in the network. Only the information collection and publishing node in the network is in Dr rather than BDR. BDR only maintains the synchronization of adjacency. When the Dr fails, the BDR will immediately become a DR and be responsible for collecting information in the network segment. At this time, a new process will be started to elect the BDR, but the election of the BDR will not affect the calculation of the route.

Mode: interface configuration mode

Command: IPv6 OSPF priority < prio > **Configure the priority of interface in Dr election**

Command: no IPv6 OSPF priority **Restore interface priority to default**

Parameter: the value of prio is 0 ~ 255, which indicates the priority in Dr selection. When it is 0, it indicates that it does not participate in the election.

Default: priority is 1

32.2.13 Configure the cost of sending messages on the interface

In the network, the traffic is controlled by configuring different links at different costs. The cost of the interface represents the cost of sending messages from the interface. If it is not configured manually, OSPFv3 will automatically calculate the interface cost according to the interface baud rate.

Mode: interface configuration mode

Command: IPv6 OSPF cost < cost >

Command: no IPv6 OSPF cost

Parameter: the value of cost is between 1 and 216-1, indicating the proxy value of the message sent on the interface.

Default: interface cost 10

32.2.14 Whether to fill in MTU domain for DD message sent by configuration interface

Mode: interface configuration mode

Command: IPv6 OSPF MTU ignore **Set not to check MTU value in DD message**

Command: no IPv6 OSPF MTU ignore **Cancel not checking MTU value in DD message**

Default: check MTU value in DD message

32.2.15 Configure regional virtual link

OSPFv3 protocol adopts the layered idea to divide the routers in the autonomous system into different groups. These groups are called regions. All regions are not equal and parallel, but have hierarchical relations. Among them, 0.0.0.0 region is the most special, which is the backbone region. Other non backbone regions must exchange inter domain routes through the backbone region. Therefore, all non backbone areas must be connected with the backbone area, that is, at least one interface on the ABR is in area 0. If some areas cannot guarantee the physical path with the backbone area due to the limitation of network topology, virtual links need to be configured to ensure the logical path. Both ends of the virtual link are ABR, and the middle passes through a non backbone area, which is called the transmission area. When configuring the virtual link, it is necessary to specify the ID of the transmission area and the ID of the opposite ABR, and it must be configured on the ABR at both ends before it can take effect.

When the route of the transmission area is calculated and the virtual link is activated, it is logically equivalent to forming a point-to-point connection between two endpoints. Therefore, the parameters of the interface can be configured on its physical interface and the authentication function can be started.

The unicast message is transmitted between ABRs. The router forwarding the unicast message in the transmission area will forward it as an ordinary IP message. Therefore, it can only be understood that a logical link is provided in the transmission area, and protocol messages can be exchanged between two ABRs.

Mode: OSPFv3 configuration mode

Command: Area < area ID > virtual link < router ID >

Configure the transmission area and peer ID of the virtual link

hello-interval <seconds>

Configure the Hello interval of virtual link

dead-interval <seconds> |

Configure virtual link neighbour failure time

retransmit-interval <seconds> |

Configure virtual link retransmission interval

transmit-delay <seconds> |

Configure virtual link interface delay

Command: no area < area ID > virtual link < router ID >|

hello-interval <seconds> |

dead-interval <seconds> |

retransmit-interval <seconds> |

transmit-delay <seconds>]

Cancel virtual link setting

Parameter: area ID refers to the ID of the transmission area. It can use dotted decimal format a.b.c.d or integer format. The value is between 0 ~ 232-1. Router ID refers to the ID of the peer router of the virtual link, in a.b.c.d format. Authentication and sending interface properties are optional. Please refer to relevant command descriptions.

Default: virtual link is not configured

32.2.16 Configure regional routing aggregation

Mode: OSPFv3 configuration mode

Command: Area < area ID > range < IPv6 prefix > [advertise | not advertise]

Configure aggregation scop

Command: no area < area ID > range < IPv6 prefix > [advertise | not advertise]

Cancel aggregation

Parameter: area ID refers to the area ID, which specifies the aggregation of routes in the area. You can use dotted decimal format a.b.c.d or integer format, and the value is between 0 ~ 232-1. IPv6 prefix uses the prefix format X: X:: X: X / m to represent the aggregation range. The optional parameters advertise and not advertise indicate whether to broadcast the aggregation range, that is, IPv6 prefix. The original network routes will be broadcast.

32.2.17 Configure stub area

Mode: OSPFv3 configuration mode

Command: Area < area ID > stub [no-summary]

Configure the router in the stub area

Command: no area < area ID > stub [no summary]

Cancel the properties of the router in the stub area

Command: Area < area ID > default cost < cost >

Configure the default cost of ABR broadcast routing connected to the stub area

Command: no area < area ID > default cost

Restore default cost to default value

Parameter: area ID refers to area ID, indicating which area attribute is stub; You can use dotted decimal format a.b.c.d or integer format, with values between 0 ~ 232-1. No summary means that inter domain routes are not injected into the stub area.

The first group of commands is to configure the router located in the stub area, and the second group of commands is to configure the ABR with the interface connected to the stub area.

Default: the stub area is not configured

32.2.18 Configure default weights for external routes

The default value of the red metric command is not used when importing external weights.

Mode: OSPFv3 configuration mode

Command: default metric < metric >

Configure the default weight when introducing external routes

Command: no default metric [Metric]

The default weight is the default value when restoring the introduction of external route

Parameter: metric value between 0 ~ 224-1

Default: the default weight is 1

32.2.19 Display information

Command: Show IPv6 OSPF [process ID **Display OSPFv3 process information**

Parameter: instance ID is the process number,

The value is between 0 - (216-1).

Command: Show IPv6 OSPF database < type > **Display LSDB information**

Parameter: type refers to all types of LSA and summary information. See the command manual for details.

Command: Show IPv6 OSPF interface [if name] **Display OSPFv3 interface information**

Parameter: if name is the agreed three-tier interface name

Command: show ip ospf route **Display OSPF routing table**

Command: Show IPv6 OSPF virtual links **Display OSPF virtual connection information**

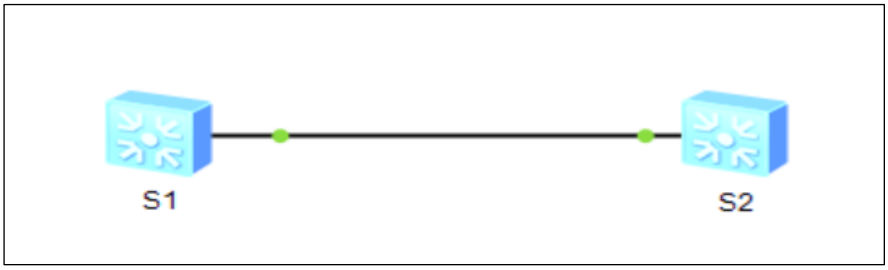
Command: Show IPv6 OSPF neighbor [options] **Display OSPF neighbour information**

Parameter: options. See the command manual for detail

Mode: privileged mode

32.3 OSPFv3 Configuration example

The two switches are connected, as shown in the figure below.



S1 The switch configuration is as follows

Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::1/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 ospf
Switch(config-router)#router-id 1.1.1.1
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router ospf area
Switch(config-vlan1)#

S2 The switch configuration is as follows

Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::2/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 ospf
Switch(config-router)# router-id 5.5.5.5
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router ospf area 0
Switch(config-vlan1)#

Display the neighbour information of two OSPFv3

Switch#show ipv6 ospf neighbor
OSPFv3 Process (*null*)

Neighbor ID	Pri	State	Time	Interface	Instance ID
5.5.5.5	1	Full/DR	00:00:39	vlan1	0

Switch#

33. Configuring BGP

This chapter includes the following contents：

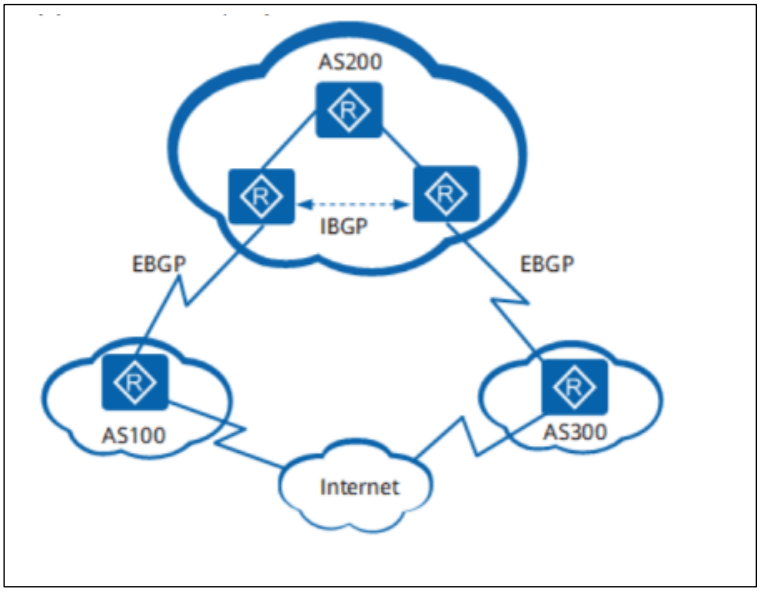
- PIM-SM introduction
- PIM-SM configuration
- PIM-SM configuration example

33.1 BGP introduction

Border Gateway Protocol BGP (border gateway protocol) is a distance vector routing protocol that realizes the reachability of routing between autonomous systems as (autonomous system) and selects the best route. The three versions released earlier are bgp-1 (rfc1105), bgp-2 (rfc1163) and bgp-3 (rfc1267). BGP-4 (rfc1771) was used in 1994. After 2006, the version used in unicast IPv4 network is BGP-4 (rfc4271), and the version used in other networks (such as IPv6) is MP-BGP (rfc4760).

BGP is divided into ebgp (external / external BGP) and iBGP (internal / internal BGP) according to the operation mode

The operation mode of BGP is shown in the following diagram.



① **Ebgp:** BGP running between different AS Areas as is called ebgp. In order to prevent a loop between, when BGP equipment receives the route sent by ebgp peer, it will discard the route with local as number.

② **IBGP**: BGP running in the same as is called iBGP. In order to prevent loop generation in as, BGP equipment does not announce the route learned from iBGP peers to other iBGP peers, and establishes full connection with all iBGP peers. In order to solve the problem of too many connections of iBGP peers, BGP designs routing reflector and BGP alliance.

There are five kinds of messages, six kinds of state machines and five principles in the interactive process of establishing, updating and deleting BGP peers.

BGP peers interact with each other through the following five types of messages, of which keepalive messages are sent periodically and the rest are triggered:

- Open message: used to establish BGP peer connection.
- Update message: used to exchange routing information between peers.

- Notification message: used to interrupt BGP connection.
- Keepalive message: used to maintain BGP connection.
- Route refresh message: used to request the peer to resend the routing information after changing the routing policy. Only BGP devices that support route refresh capability will send and respond to this message.

There are six state machines in the interaction process of BGP peers: idle, connect, active, open message sent (opensent), open message confirmed (openconfirm) and connection established (established). In the process of establishing BGP peers, the three commonly visible states are idle, active and established.

The BGP device adds the optimal route to the BGP routing table to form a BGP route. After the BGP device establishes the neighbor relationship with the peer, the following interaction principles shall be adopted:

- BGP route obtained from iBGP peer, BGP device only publishes to its ebgp peer.
- BGP routes obtained from ebgp peers, and BGP devices publish them to all ebgp and iBGP peers.
- When there are multiple valid routes to the same destination address, the BGP device only publishes the optimal route to the peer.
- When the route is updated, the BGP device only sends the updated BGP route.
- BGP device will receive all routes sent by peers.

BGP and IGP use different routing tables in the equipment. In order to realise the mutual communication between different AS, BGP needs to interact with IGP, that is, BGP routing table and IGP routing table are introduced into each other.

BGP protocol itself does not find routes, so other routes need to be introduced into BGP routing table to realise routing interworking between as. When an as needs to publish routes to other as, the as edge router will introduce IGP routes into the BGP routing table. In order to better plan the network, when BGP introduces the route of IGP, it can use the route strategy to filter the route and set the route attribute or set the Med value to guide the ebgp peer to judge the route when the traffic enters the as.

BGP supports import and network when introducing routes:

- The import method is to import the routes of rip, OSPF, Isis and other protocols into the BGP routing table according to the protocol type. In order to ensure the effectiveness of the introduced IGP route, the import mode can also introduce static route and direct route.
- The network method is to introduce the existing routes in the IP routing table into the BGP routing table one by one, which is more accurate than the import method

IGP introduces BGP routing

When an as needs to introduce routes from other as, the as edge router will introduce BGP routes into the IGP routing table. In order to avoid the impact of a large number of BGP routes on devices in as, when IGP introduces BGP routes, routing policies can be used to filter routes and set routing attributes

33.2 BGP configuration

33.2.1 Start BGP and enter BGP configuration mode

BGP protocol uses as number to identify; When starting BGP protocol, it is necessary to specify which autonomous system is started.

Mode: global configuration mode

Command: router BGP < as number > **Start the BGP protocol process and enter its mode**

Command: no router BGP < as number > **Close the BGP protocol and delete its configuration**

Parameter: as number value: 1-4294967295.

Default: BGP protocol is not run

33.2.2 Inject routing information into BGP protocol

At the beginning of running, the routing information of BGP is empty. There are two ways to inject routing information into BGP: manually inject routing information into BGP through network command. Through the interaction with IGP protocol, route information is injected from IGP. BGP publishes the injected route to its neighbours. This section mainly describes the manual injection of routing information.

Mode: BGP configuration mode

Command: network < network number > mask < mask > [route map < map tag >] [backdoor]

This command configures the network information to be announced by this BGP speaker.

Command: no network < network number > mask < mask > [route map] [backdoor]

This command deletes the set network information

33.2.3 Configure BGP timer

BGP uses keepalive timer to maintain effective connection with peers and holdtime timer to judge whether peers are effective. By default, the value of keepalive timer is 60 scores and the value of holdtime timer is 180 seconds. When a BGP connection is established between BGP speakers, both parties will negotiate the holdtime, and the holdtime with smaller value will be selected, while the selection of keepalive timer value will be based on the smaller of 1 / 3 of the negotiated holdtime and the configured keepalive value.

Mode: BGP configuration mode

Command: timers BGP < keepalive > < holetime >

This command is used to adjust the network timer of BGP.

Command: no timers BGP < keepalive > < holetime >

This command restores the default values.

33.2.4 Configure BGP and IGP synchronization

For the routing information that will cross this as to another as, it is allowed to publish the routing information to another as only when it is ensured that all routers in this as learn the routing information. Otherwise, if the router (running IGP protocol) in this as does not learn the routing information, when the data message passes through this as, it may discard the data message because these routers do not know the route, which will cause the routing black hole phenomenon.

Ensure that all routers in the as learn the routing information outside the as. We call it the synchronization of BGP and IGP. The simple way to realize synchronization is that BGP speaker redistributes all the routes learned by BGP protocol to IGP, so as to ensure that the router inside as can learn these routing information.

In two cases, the synchronization mechanism of BGP can be cancelled:

1. There is no routing information across this as (generally, this as is a terminal as);

2. All routers in this as run BGP protocol, and all BGP speakers establish full connection relationship (BGP speakers establish adjacency relationship)..

Mode: BGP configuration mode

Commands: synchronization

This command starts the synchronization mechanism of BGP and IGP routing information.

Command: no synchronization

This command cancels the synchronization mechanism between BGP and IGP.

33.2.5 Configure the interaction between BGP and IGP

Inject the route information generated by IGP protocol into BGP. By default, redistributing the default route is not allowed. If you want to redistribute the default route, use the following command to control it.

Mode: BGP configuration mode

Command: redistribute < protocol type > [route map < map tag >]

This command can redistribute the routing information of other routing protocols to BGP.

Command: no redistribute < protocol type > [route map < map tag >]

This command deletes the function and its parameter configuration.

33.2.6 Selection of BGP optimal path

The selection of optimal routing is a very important part of BGP protocol. We will describe the selection process of BGP routing protocol in detail below:

If the routing table entry is invalid, it will not participate in the selection of the optimal route;.

Otherwise, elect local_ Routes with high pref attribute value;

Otherwise, select the route generated by the BGP speaker;

The routes generated by this BGP speaker include those generated by network command, redistribute command and aggregate command.

Otherwise, select the route with the shortest as length;

Otherwise, select the route with the lowest origin attribute value;

Otherwise, select the route with the lowest Med value

Otherwise, the priority of ebgp path is higher than that of iBGP path and as alliance, and the priority of iBGP path and as alliance is the same;

Otherwise, the route with the smallest IGP metric to the next hop is elected

Otherwise, in the route from ebgp, the election receives the earlier route;

Otherwise, the route with a smaller router ID of the BGP speaker of the route will be announced

Otherwise, the route with a large length of the election cluster;

Otherwise, the route wi

Mode: BGP configuration mod

Command: BGP bestpath < as path ignore | compare confirmed aspath | compare routerid | don compare originator ID | Med [confirmed | missing as worst | remove recv Med | remove send Med] | tie break on age >

This command sets the election of BGP optimal route.

Command: no BGP bestpath < as path ignore | compare confirmed aspath | compare routerid | don compare originator ID | Med [confirmed | missing as worst | remove recv Med | remove send Med] | tie break on age >

This command deletes the election of BGP optimal route.

33.2.7 Configure BGP routing aggregation

BGP-4 supports CIDR, so it is allowed to create aggregation table entries to reduce the size of BGP routing table. Of course, the BGP aggregation table entry is added to the BGP routing table only when there is a valid path within the aggregation range.

Mode: BGP configuration mode

Command: aggregate address < IP address > / < mask length > [as set | summary only]

This command sets the IPv4 / IPv6 aggregation routing table entry of BGP.

Command: no aggregate address < IP address > / < mask length > [as set | summary only]

This command deletes the aggregation routing table entry.

33.2.8 Configure BGP routing reflector

In order to speed up the convergence of routing information, all BGP speakers in an as will usually establish a full connection relationship (BGP speakers establish an adjacency relationship between two). When there are too many BGP speakers in the as, it will increase the resource overhead of BGP speakers, increase the workload and complexity of configuration tasks for network administrators, and reduce the expansion performance of the network.

In this regard, two methods of routing reflector and as alliance are proposed to reduce the number of iBGP peers in as. Routing reflector is a method to reduce the number of iBGP peer connections in autonomous system. A BGP speaker is set as a routing reflector, which divides iBGP peers in the autonomous system into two categories: client and non client.

The routing reflector is implemented in the as, and its rules are as follows:

Configure the routing reflector and specify its client. The routing reflector and its client form a group. Route Reflector

A connection relationship will be established between and the client.

The client of an intra group routing reflector should not establish a connection relationship with other BGP speakers outside the group.

In as, a complete connection relationship is established between iBGP peers of non clients. Here, the iBGP of non clients

Peers include the following situations: between multiple routing reflectors in a group; Routing reflectors and groups within a group

BGP speakers that do not participate in the routing reflector function (usually these BGP speakers do not support the routing reflector function); Between the routing reflectors in the group and the routing reflectors in other groups.

The processing rules of a route received by the route reflector are as follows:

The route update received from ebgp speaker will be sent to all clients and non clients;

The route update received from the client will be sent to other clients and all non clients;

Routing updates received from iBGP non clients will be sent to all their clients.

Mode: BGP configuration mode

Command: neighbour [peer address | peer tag] route reflector client

This command configures the device as a routing reflector and specifies its client.

Command: no neighbour [peer address | peer tag] route reflector client

This command cancels the setting of the client.

33.2.9 Configure BGP's as Federation

Federation is another way to reduce the number of iBGP peer connections in autonomous systems.

An autonomous system is divided into several sub autonomous systems, and these sub autonomous systems are formed into an alliance by setting a unified alliance ID (i.e. alliance as number). For the outside of the alliance, the whole alliance is still considered as an as, and only the as number of the alliance is visible. Within the alliance, a complete iBGP peer connection is still established between BGP speakers within the sub autonomous system, and an ebgp connection is established between BGP speakers between the sub autonomous systems. Although the ebgp connection is established between the BGP speakers of the sub autonomous system, when exchanging information, for next_ Hop, Med and local_ Path attribute information such as pref remains unchanged..

Mode: BGP configuration mode

Command: BGP confirmation identifier < as number >

This command configures the identifier of the as Federation.

Command: no BGP confirmation identifier

This command cancels the identifier of the as Federation.

33.2.10 Configure BGP management distance

The management distance indicates the reliability of a routing information source, which ranges from 1 to 255. The greater the value of the management distance, the lower the reliability.

BGP sets different management distances for different sources of learned routing information, which are divided into external distance, internal distance and local distance:

External distance: learn the management distance from ebgp peers to routing.

Internal distance: learn the management distance from iBGP peers to routing.

Local distance: learned from peers, but it is considered that there are pipes that can learn better routing from IGP

Manage distances. These routes are usually represented by the network backdoor command.

Mode: BGP configuration mode

Command: distance BGP < external distance > < internal distance > < local distance >

This command sets different management distances for different types of BGP routes.

Command: no distance BGP < external distance > < internal distance > < local distance >

This command restores the default management distance.

33.2.11 Configure BGP routing update mechanism

BGP routing update mechanism includes two parts: regular scan update and event triggered update. Scheduled scan update means,

BGP uses a timer to start the scanning mechanism regularly and update the routing table. The event triggered update means that when the user configures BGP, resulting in the change of BGP configuration command or the change of the next hop of BGP route, it triggers BGP to start the scanning mechanism and update the routing table..

Mode: BGP configuration mode

Command: BGP scan time < time >

This command sets the time interval of regular scanning of BGP protocol.

Command: no BGP scan time [time]

The time interval for the command to resume the regular scanning of BGP protocol is 60 seconds.

33.2.12 Configure BGP local AS

BGP's local as function is used to configure a local as different from BGP's real as (router BGP as) for a specific peer, which is similar to virtualizing a new as with the peer device, so that when the local BGP's real as changes, the BGP configuration of the peer device does not need to be changed to realize the establishment of BGP connection. This function is mainly

The migration and consolidation of as for large networks can ensure that the configuration of equipment in other interconnected as will not be affected.

In the BGP protocol, when the local device establishes a BGP connection with the peer, it will announce the local as number to the peer device through the open message. The peer device will check whether the BGP as announced by the connection end is the same as the locally configured peer as. If not, it will reject the BGP connection. By default, the local as in the BGP connection is the real as of BGP. By configuring the local as for the peer, the local device will use the configured local as to replace the real as and establish the BGP connection when establishing the BGP connection with the peer

Mode: BGP configuration mode

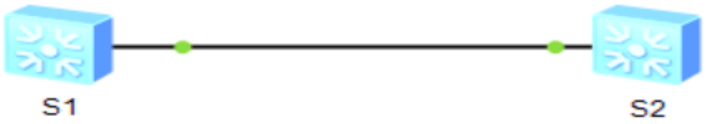
Command: neighbor [peer address | peer tag] local as < as number >

Set to configure a local as number for a BGP peer. At this time, the peer device can use the local as as its remoteAS to establish a BGP connection with the device..

Command: no neighbor [peer address | peer tag] local as < as number >

This command deletes the configured local as.

33.3 BGP Configuration example



S1 The switch configuration is as follows

Switch(config)#

Switch(config)#int vlan1

Switch(config-vlan1)#ip address 192.168.0.1/64

Switch(config-vlan1)#exit

Switch(config)#router bgp 1

Switch(config-router)#bgp router-id 1.1.1.1

Switch(config-router)#neighbor 192.168.0.2 remote-as 1

Switch(config-router)#neighbor 192.168.0.2 interface vlan1

Switch(config-router)# neighbor 192.168.0.2 next-hop-self

Switch(config-router)#exit

S2 The switch configuration is as follows

Switch(config)#

Switch(config)#int vlan1

Switch(config-vlan1)#ip address 192.168.0.2/64

Switch(config-vlan1)#exit

Switch(config)#router bgp 1

Switch(config-router)#bgp router-id 2.2.2.2

Switch(config-router)#neighbor 192.168.0.1 remote-as 1

Display neighbour BGP information

Switch#show bgp neighbors

BGP neighbor is 192.168.0.2, remote AS 1, local AS 1, internal link

BGP version 4, remote router ID 2.2.2.2

BGP state = Established, up for 00:02:09

Last read 00:02:09, hold time is 90, keepalive interval is 30 seconds

Neighbor capabilities:

For address family: IPv4 Unicast

BGP table version 2, neighbor version 2

Index 1, Offset 0, Mask 0x2

NEXT_HOP is always this router

Community attribute sent to this neighbor (both)

1 accepted prefixes

0 announced prefixes

Connections established 1; dropped 0

Local host: 192.168.0.1, Local port: 53557

Foreign host: 192.168.0.2, Foreign port: 179

Nexthop: 192.168.0.1

Nexthop global: fe80::82:44ff:fe13:4803

Nexthop local: ::

BGP connection: non shared network

Switch#

Switch(config-router)#neighbor 192.168.0.1 interface vlan1

Switch(config-router)# neighbor 192.168.0.1 next-hop-self

Switch(config-router)#exit

Route refresh: advertised and received (old and new)

Address family IPv4 Unicast: advertised and received

Received 7 messages, 0 notifications, 0 in queue

Sent 6 messages, 0 notifications, 0 in queue

Route refresh request: received 0, sent 0

Minimum time between advertisement runs is 5 seconds

34. Configuring VRRP

This chapter includes the following contents:

- VRRP Introduction
- VRRP configuration
- VRRP Configuration Example

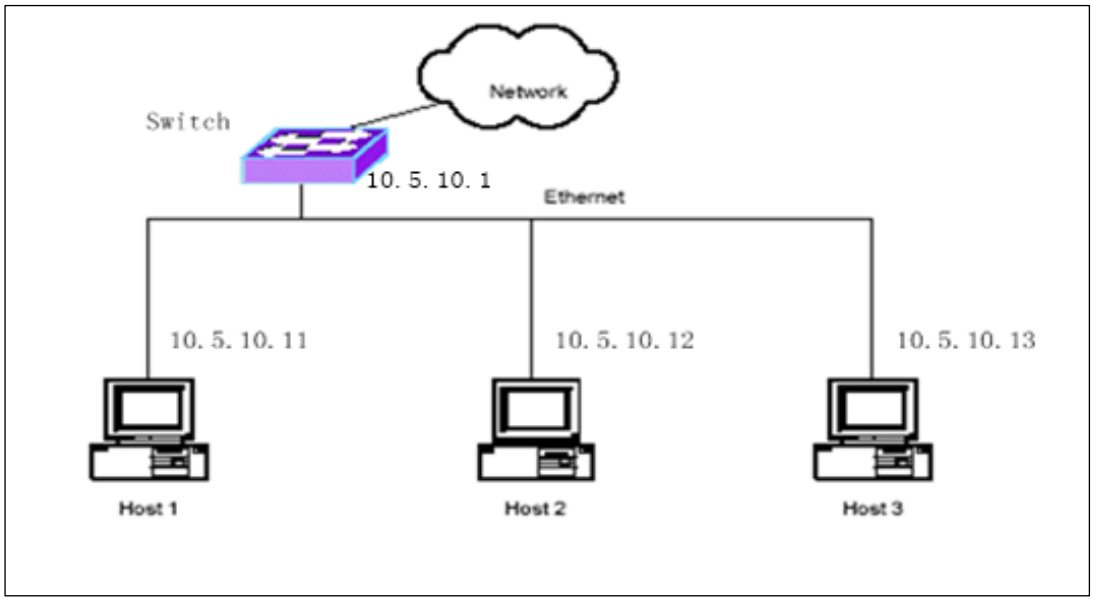
34.1 VRRP Introduction

VRRP is the abbreviation of Virtual Router Redundancy Protocol. It is an important three-layer reliability protocol, which is used for the redundant backup of the default gateway. This section describes the VRRP protocol in detail, mainly including the following contents:

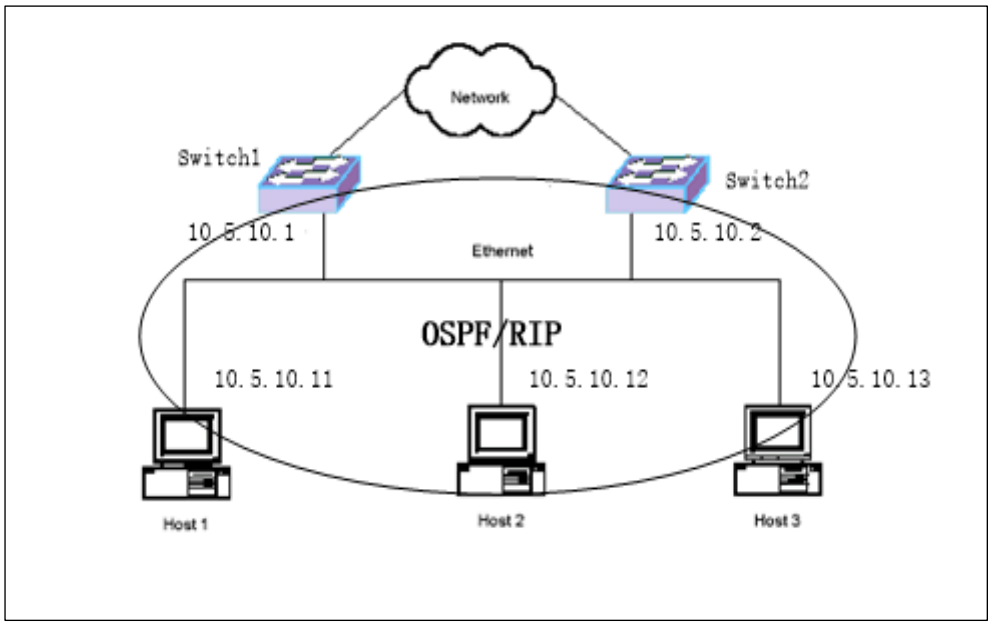
- VRRP Overview
- VRRP Terminology
- VR RP protocol interaction
- Election of virtual master router
- Status of the virtual router
- VRRP tracing

34.1.1 VRRP Overview

The following figure shows a typical intranet networking scheme. One interface of the switch is connected to the external network, and the other interface is connected to the internal network. The IP address of the interface connected to the internal network is 10.5. 10.1, hosts 1, 2, and 3 are all configured with IP addresses, and they are all in the 10.5 of the network segment. 10.0/24. Hosts 1, 2, and 3 are configured with a default gateway, a next hop to the switch, and the IP address of the next hop is 10.5. 10.1. In this way, a message whose destination IP address is not in the local network segment sent by the host will match the default route and be sent to the switch, and then the switch will forward the message, and the switch will also forward the message sent by the external network to the corresponding host, so that the host can communicate with the external network.



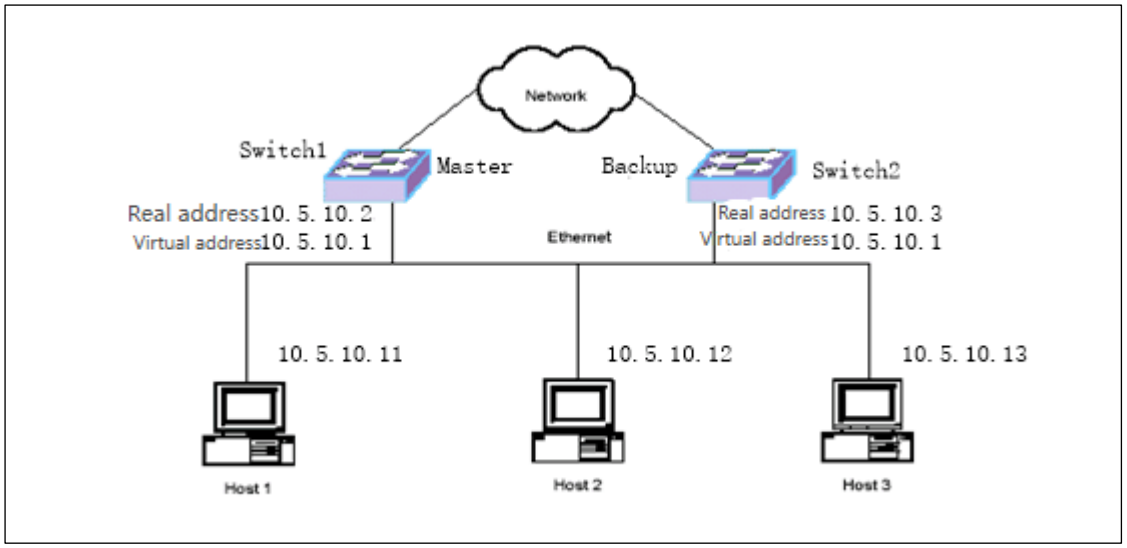
In the above networking diagram, the communication between the host and the external network can only pass through the only switch. When the switch fails, all the hosts are disconnected from the external network. In order to solve this problem, one solution is to expand one switch into two or more switches, and run the dynamic routing protocol OSPF or RIP between the host and the switch, as shown in the following figure.



After the host runs the dynamic routing protocol, the host can learn all the routes of the external network. When communicating with the external network, the host searches the route according to the destination IP address of the packet to get the next hop to determine whether the packet is sent to switch1 or switch2. When one of the switches fails, the route in the host can be relearned in a very short time, and the next hop of the route will point to the non-failed router, so that the communication between the host and the external network will not be interrupted.

However, it is not practical to implement a dynamic routing protocol on the host. For hosts, running dynamic routing protocols is too much load, for networks, running dynamic routing protocols on hosts will cause too much unnecessary data traffic on the network, and some hosts do not support dynamic routing protocols at all.

In order to solve the problem of single point of failure, VRRP protocol is the best choice. The VRRP protocol is proposed specifically for this problem. As shown in the figure below, Switch1 and Switch2 form a virtual router. The real IP addresses of the interfaces of the two switches are different, but there is a common virtual IP address 10.5. 10.1, the default gateway of the host is set to the virtual IP address 10.5. 10.1.When Switch1 is the virtual master switch, the communication between the host and the external network is forwarded through Switch1. However, when Switch1 fails, Switch2 takes over Switch1 to become the virtual master switch, and the communication between the host and the external network is forwarded through Switch2. Using the VRRP protocol, the host only needs to set the default gateway, and does not need to run other protocols on the host. The load of the host is small, and only a few VRRP protocol flows need to be added on the network.



34.1.2 VRRP Terminology

Here are a few terms that are often used:

1) VRRP

Virtual Router Redundancy Protocol is a fault-tolerant protocol for default gateways that improves network reliability.

2) Virtual Router

A virtual router, an abstract object, based on a subnet interface, consists of a virtual router identifier (VRID) and an IP address, also known as a virtual IP address, which acts as a default gateway for hosts.

3) VRRP Router

VRRP routers are routers that run the VRRP protocol. A VRRP router can be added to a virtual router.

4) IP Address Owner

IP Address Owner. A VRRP router where the virtual IP address of the virtual router is the same as the real IP address of the interface.

5) Virtual Router Master

The virtual main router is responsible for forwarding the three-layer data packet passing through the virtual router and responding to the ARP request of the IP address of the virtual router. If a VR RP router is the IP address owner, it is always the virtual master.

6) Virtual Router Backup

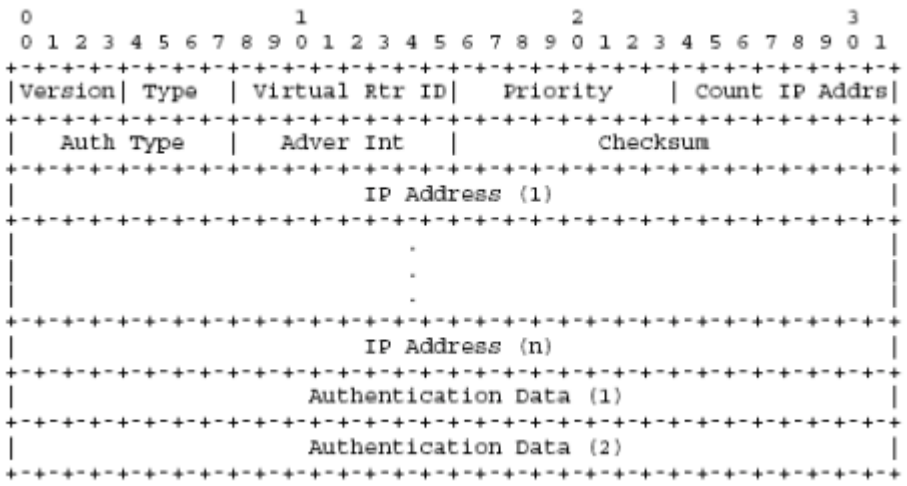
The virtual backup router does not forward Layer 3 packets, does not reply to ARP requests for virtual IP addresses, and takes over the work of the virtual primary router when the virtual primary router fails.

To better understand these terms, note the following:

- a switch may include multiple interfaces, and the VRRP protocol may be enabled on multiple interface subnets.
- One virtual router can exist on one interface subnet.
- a VRID identifies a virtual router.

34.1.3 VRRP protocol interaction

The VRRP protocol packet is encapsulated in the IP packet, and the VRRP message header is shown in the following figure:



1) MAC frame header field of VR RP packet

Source MAC address: The virtual MAC address of the virtual router is 00-00-5e-00-01- { VRID }, where VRID is the virtual router identifier. For example, if the VRID of the virtual router is 1, the virtual MAC address is 00-00-5e-00-01-01.

Destination MAC address: VRRP multicast MAC address, 01-00-5e-00-00-12.

2) IP header field of VR RP packet

Source IP address: The primary IP address of the interface that sends the VRRP packet.

Destination IP address: The multicast IP address is 224.0. It is 0.18 and cannot be used for Layer 3 forwarding.

TTL: 255, to prevent remote VR RP packet attack.

Protocol：112.

3) VR RP header field

Version：2.

Type: the type of VR RP package. Only one type is supported: 1 -- ADVERTISEMENT, VRRP notification package.

VRID: Identifies a virtual router.

Priority: The priority of the sending VRRP router for this virtual router.

Count IP Addrs: The number of virtual IP addresses. A virtual router can have multiple virtual IP addresses.

Auth Type: An authentication method between VRRP routers in a virtual router.

Advertisement Interval: The interval time of advertisement. The default is 1 second.

Checksum: checksum, starting from the Version of the VRRP header.

IP Address (es): One or more virtual IP addresses.

Authentication Data: Authentication data.

4) VRRP priority

Each VRRP router in a virtual router needs to be configured with a priority. The priority ranges from 0 to 255, where 0 and 255 are used for special purposes. The configurable priority ranges from 1 to 254. The default is 100. The higher the value of the priority, the higher the priority, and the more likely it is to become a virtual master router.

In a virtual router, when a VRRP router is the IP address owner, its priority is 255.

When the virtual main router needs to notify other backup routers that it is no longer the main router, it sends a VR RP packet with a priority of 0 to other backup routers, which can quickly trigger other backup routers to become virtual main routers.

5) VRRP certification

VRRP protocol provides three authentication methods, which can be selected according to the security requirements of the network in actual use.

0 --- No Authentication **No certification.**

1 --- Simple Text Password **Simple password authentication**

2 --- IP Authentication Header

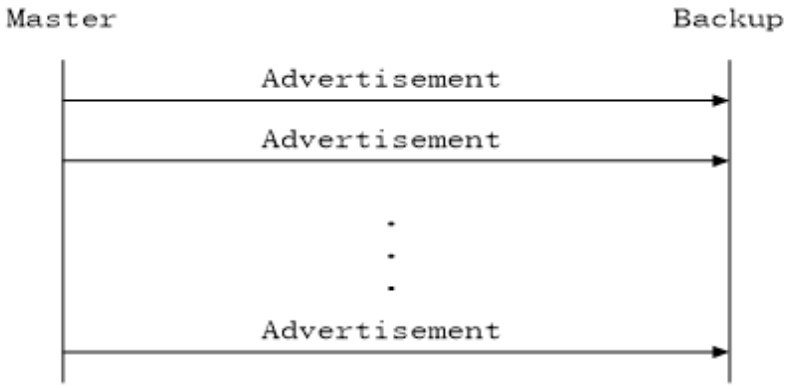
IP authentication header, which calculates a message digest by the HMAC-MD5 method

No authentication or simple password authentication can be used in the network with low security, and HMAC authentication can be used in the network with high security.

For the 0 and 2 authentication methods, the Authentication Data field is filled with 0. For the 1 authentication method, the Authentication Data field is filled with the password. For the 2 authentication method, the message digest is filled in the IP Authentication Header field, that is, the AH field is added to the IP header.

6) VR RP package interaction

The VRRP protocol has only one type of packet, the ADVERTISEMENT packet. In a virtual router, the virtual active router sends an Advertisement packet every Advertisement Interval (the default is 1 second). The virtual backup router determines whether state migration is required according to the received VRRP notification packet. The protocol interaction between the master and the slave is shown in the figure below:



34.1.4 Election of virtual master router

The selection of the virtual primary router in a virtual router is determined by the following factors:

- **IP Address Owner**

If a VR RP router is the IP address owner (its interface IP address is the same as the virtual IP address), it is a virtual master if the router is functioning properly.

- **VRRP priority**

The working VRRP router with the highest priority becomes the virtual master router. The configurable priority ranges from 1 to 254. The IP address owner's router has a priority of 255. When the virtual master router notifies the virtual backup router that it is no longer the master, a priority of 0 is given in the VR RP packet.

The size of the actual IP address of the interface. When the priority is the same, the VRRP router with the larger actual IP address of the interface becomes the virtual active router.

An active-standby switchover occurs in a virtual router when:

1) When the virtual active router fails, active/standby switchover will occur. In this case, there are two possibilities:

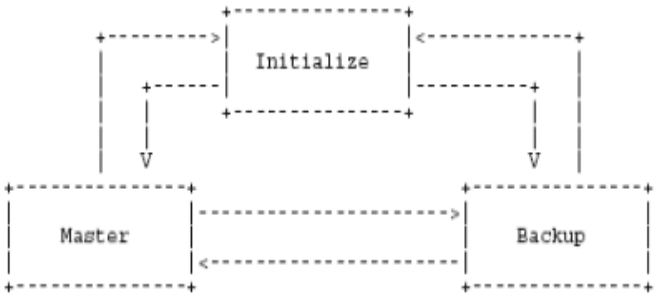
- If the virtual active router is still active, it will send a VRRP packet with a priority of 0. After receiving this packet, the backup router will switch to the virtual active router if it does not receive the VRRP packet from the virtual active router within Skew _ Time time. In this case, the switching speed is relatively fast, and the switching can be realized within 1 second.
- If the virtual master router is not active, the virtual backup router will switch to the virtual master router if it does not receive the VR RP packet from the virtual master router within the Master Down Interval. Master_Down_Interval = (3 * Advertisement_Interval) + Skew_Time Skew_Time = ((256 – Priority) / 256)

2) When the virtual active router is not the IP address owner, but now a router with an IP address owner joins the network, the router will become the virtual active router, and active-standby switching occurs.

3) When a VRRP router joins the network, if the priority of the router is higher than that of the virtual active router and the router is in the preemption mode (the Preempt _ Mode of the configuration variable is TRUE), the router will become the virtual active router, and active-standby switchover occurs.

34.1.5 Status of the virtual router

Each VRRP router in a virtual router executes a state machine. The migration of the state machine is shown in the following figure:



1) Initialize status

The Initialize state is the initial state of a virtual router in which to wait for the Startup event. If a Startup event is received in this state, the process is as follows:

- If the priority of the VRRP router is 255 (that is, the IP address owner), the router becomes a virtual master router and migrates to the Master state.

- otherwise, that rout becomes a virtual backup rout,Migrate to the Backup state.

After the router migrates to the Master state, the actions are as follows:

- Send a VRRP notification packet.
- Broadcast an ARP request containing the virtual IP address and the corresponding virtual MAC address.
- set a Adver _ Timer timer, and set a time interval to be a Advertisement _ Interval.

After the router migrates to the Backup state, the actions are as follows:

- set a Master _ Down _ Timer timer, wherein that time interval is Master _ Down _ Interval.

2) Backup status

The purpose of Backup status is to monitor the availability and status of the virtual master router and take over the work of the virtual master router at any time.

If a Shutdown event is received, cancel the Master _ Down _ Timer timer and return to the Initialize state.

If the Master _ Down _ Timer expires, it becomes a virtual master router and migrates to the Master state.

If a VRRP notification packet is received, the following conditions exist:

- If the priority field in the VR RP packet is 0, the Master _ Down _ Timer is set, and the timing interval is Skew _ Time.
- Otherwise, if the preemption mode (Preempt _ Mode) is FALSE or the priority in the VRRP packet > = the priority of the VRRP router, the Master _ Down _ Timer is reset, and the time interval is set to the Master _ Down _ Interval.
- Otherwise, discard the VR RP packet.

3) Master status

The VRRP router in the Master state is responsible for forwarding Layer 3 packets through the virtual router.

if the Shutdown event is received, canceling the Adver _ Timer timer, sending a VRRP notification packet with the priority of 0, and migrating to the Initialize state.

If the Adver _ Timer timer expires, a VRRP notification packet is sent to reset the Adver _ Timer timer.

If a VRRP notification packet is received, the following conditions exist:

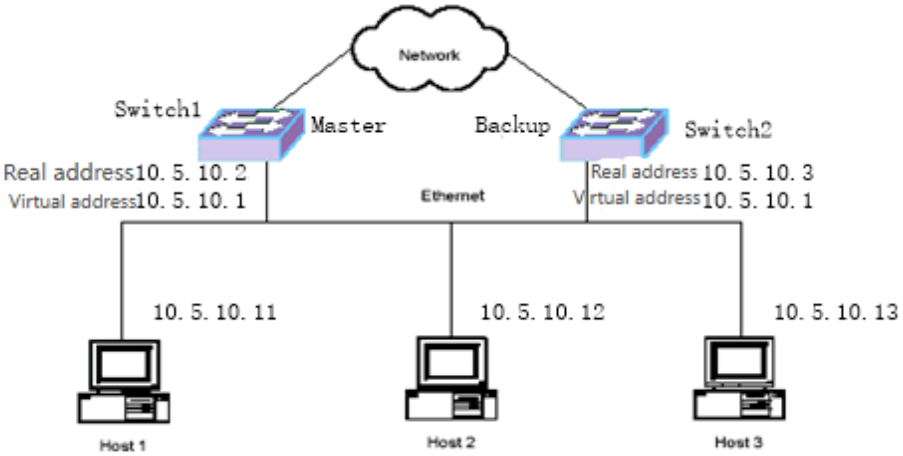
- if that priority in the packet is 0, sen a VRRP notification packet to reset the Adver _ Timer.
- otherwise, if the priority in the packet is greater than that of the VRRP router or the priorities are the same, but the IP address for sending the packet is greater than the main IP address of the interface of the VRRP router, canceling the Adver _ Timer timer, setting the Master _ Down _ Timer, and migrating to the Backup state.
- Otherwise, the VRRP notification packet is discarded.

34.1.6 VRRP tracing

The VRRP protocol itself can only detect the fault inside the virtual router, such as the interface LINK DOWN where the virtual router is located or the VRRP router crashes, but cannot detect the fault outside the virtual router. When faults occur outside the virtual router, the virtual router cannot select the virtual main router according to these faults, which will cause the interruption of network data. VRRP tracing can solve this problem. The VRRP router traces the specified external events. When an

external failure occurs, the VRRP router changes its running priority and reselects the virtual master router to ensure that the network data is not interrupted.

As shown in the figure below, when the external interface of the virtual active router Switch1 is LINK DOWN, if the VRRP tracing function is not enabled, Switch1 cannot detect this external fault, Swith1 continues to be the virtual active router, and the host cannot access the external network. If the VRRP tracing function is enabled, Switch1 can find the external fault, modify its running priority, and re-select the virtual main router. Switch1 changes to the virtual backup router, and Switch2 changes to the virtual main router, so that the host can continue to access the external network.



VRRP tracing includes interface tracing, route tracing and PING tracing. Interface tracing means that the VRRP router traces the interface outside the virtual router. If one of the traced interfaces is LINK DOWN, it indicates that an external fault has occurred. Route tracing is that the VRRP router traces the route in its learned routing table. If the route does not exist or the route exists but is not active, it indicates that an external fault has occurred. A PING trace is a device that the VR RP router always pins to be traced,If the device does not answer the PING within the specified time, it indicates an external fault. The virtual router can trace the interface, route and PING at the same time. For each type of trace, multiple events can be traced. As long as one of the traced events fails, it indicates that the virtual router has an external failure. Only when all the traced events are normal, it indicates that the virtual router has no external failure.

34.2 VRRP configuration

The VRRP configuration includes the following:

- Create and delete virtual router
- Configure the virtual IP address of the virtual router
- Configure parameters for the virtual router
- Configuring VRRP Tracing
- Starting and shutting down the virtual router
- View VRRP Information

34.2.1 Create and delete virtual router

Virtual routers are established on subnet interfaces and require a VRID to be specified. Virtual routers are not created by default.

When a virtual router is no longer needed, it can be deleted. If the virtual router has been started, the virtual router will be closed first and then deleted.

The commands to create and delete a virtual router are as follows:

Command	Description	CLI Mode
router vrrp <vrid>	Create a virtual router and enter VRRP configuration mode. If the virtual router already exists, enter VRRP configuration mode directly. The argument is the VRID, which ranges from 1 to 255	Configuration Mode
no router vrrp [vrid]	Delete a virtual router, the parameter is VRID	Configuration Mode

34.2.2 Configure the virtual IP address of the virtual router

A virtual IP address must be configured on the virtual router. In theory, a virtual router can have one or more virtual IP addresses, but a virtual router supports only one virtual IP address when the switch is implemented. By default, the switch is not configured with a virtual IP address.

The command to configure the virtual IP address of the virtual router is as follows:

Command	Description	CLI Mode
virtual-ip <virtual-ip> <backup | master>	Set the virtual IP address of the virtual router.	VRRP Configuration Mode
no virtual-ip	Delete the virtual IP address of the virtual router.	VRRP Configuration Mode

Notice:

The virtual IP address of the virtual router must be configured successfully when the virtual router is closed, and cannot be configured successfully when the virtual router is started.

The virtual IP address set must be in the same network segment as the main IP address of the interface, otherwise the configuration is not successful.

34.2.3 Configure parameters for the virtual router

The parameters of the virtual router include priority, pre-emption mode, advertisement interval, authentication method, and authentication data. These parameters have default values, as shown in the following table:

Parameters	Defaults
Priority	100
Preemption Mode	TRUE
Announcement Interval	1 Second
Authentication Method	Do Not Authenticate
Authentication Data	None

During configuration, for the virtual router, the advertisement time interval, authentication method, and authentication data must be configured the same, and the priority and pre emption mode parameters can be configured the same.

The priority is divided into configuration priority and operation priority. In most cases, the operation priority uses the configuration priority, but when the VRRP router is the IP address owner, the operation priority is 255, and the configuration priority is not used.

For the authentication method, at present, the switch only implements two modes of no authentication and simple password authentication, but does not implement the IP authentication header mode.

The command for configuring the parameters of the virtual router is shown in the following table:

Command	Description	CLI Mode
priority < priority-value >	Sets the priority of the virtual router from 1 to 254.	VRRP Configuration Mode
preempt-mode {false | true}	Set the preemption mode of the virtual router. TRUE means preemption. FALSE means no preemption.	VRRP Configuration Mode
advertisement-interval <interval>	Sets the advertisement interval of the virtual router from 1 to 255 in seconds.	VRRP Configuration Mode
authentication none	Set the authentication method of the virtual router to no authentication.	VRRP Configuration Mode
authentication simple-password <key>	Set the authentication method of the virtual router as simple password authentication, and set the authentication data, that is, the password.	VRRP Configuration Mode

Notice:

The configuration of the parameters of the virtual router must be successful when the virtual router is turned off. The configuration cannot be successful when the virtual router is turned on.

34.2.4 Configuring VRRP Tracing

At present, the switch only implements the VRRP interface tracking function. A VRRP router can track an interface, which can be a Layer 2 interface or an aggregation interface. The switch is not configured with tracked interfaces by default.

An administrator can configure a VRRP trace if the VRRP router is the IP address owner, but the VRRP trace will not actually take effect, meaning that the virtual master will not be reselected even if the virtual router has an external failure. If you want to use the VRRP trace feature, do not configure the virtual router as the IP address owner.

VRRP tracing takes effect when the administrator configures VRRP tracing, specifies the one to trace, and starts the virtual router. When the VRRP router finds a tracked interface LINK DOWN, it is considered that an external fault has occurred, and the running priority of the virtual router is set to the value of source priority minus priority-value, and the virtual main router can be reselected through the interaction of VRRP protocol packets. When the traced interfaces are all LINK UP, the failure is recovered and the running priority of the virtual router is reset to the configuration priority.

The commands for configuring VRRP tracing are shown in the following table:

Command	Description	CLI Mode
circuit-failover <if-name> <priority-value>	Set the interfaces to be tracked by the virtual router.	VRRP Configuration Mode
no circuit-failover	Clears the tracked interfaces of the virtual router.	VRRP Configuration Mode

Notice:

Configuring a VRRP trace must be successful when the virtual router is down and cannot be successful when the virtual router is up.

34.2.5 Starting and shutting down the virtual router

When the virtual router is created and the virtual IP address and parameters are set, the virtual router is not really running and is still in the Initialize state. Starting the virtual router will start the running of the protocol, send a Startup event to the protocol, and the state machine will migrate to the Master state or Backup state. Shutting down the virtual router shuts down the protocol, sends a Shutdown event to the protocol, and returns the state to Initialize.

You must ensure that the virtual IP address is configured before starting the virtual router. When the virtual router is started, if the virtual IP address or parameters need to be modified, the virtual router must be shut down before configuration, and the virtual router can be started after the configuration is completed.

The commands to start and shut down the virtual router are as follows:

Command	Description	CLI Mode
enable	Start the virtual router.	VRRP Configuration Mode
disable	Shut down the virtual router.	VRRP Configuration Mode

34.2.6 View VRRP Information

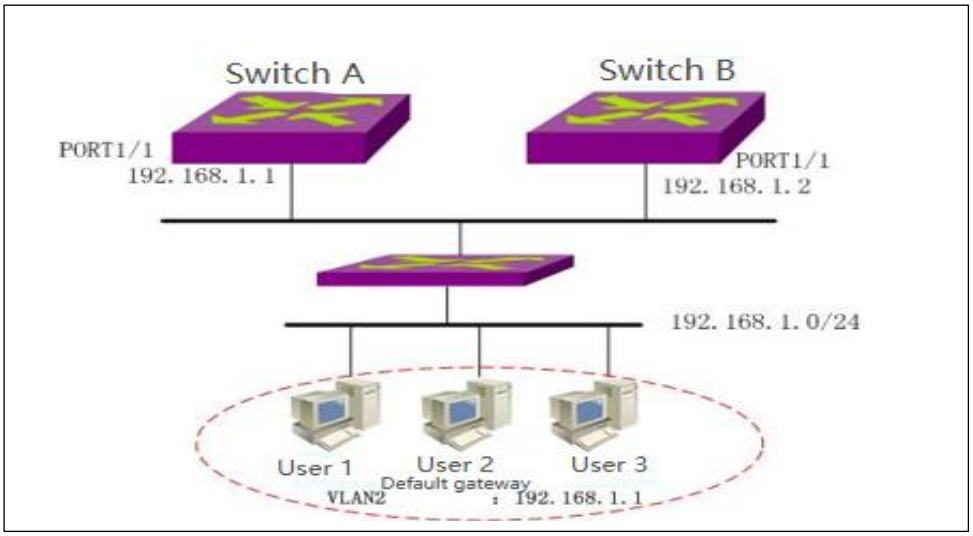
The running status and configuration information of VRRP can be viewed through the command. The command for viewing VRRP information is as follows:

Command	Description	CLI Mode
show vrrp [vrid]	If no parameters are entered, all virtual router information is displayed.	Normal Mode, Privileged Mode
show running-config	View the current configuration of the system. You can view the configuration of VRRP.	Privileged Mode

34.3 VRRP Configuration Example

(1) Configuration

The VRRP function is enabled on the two switches to provide the three-layer routing redundancy function for the users in the LAN and eliminate the routing failure in the network. Switch 1 is set as the Master switch, and switch 2 is set as the Backup switch.



Configuration on Switch A:

Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#exit
Switch(config)#ip interface vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp 1
Switch(config-vrrp)# virtual-ip 192.168.1.1 master
Switch(config-vrrp)#enable

Configuration on Switch B:

Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#exit
Switch(config)#ip interface vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.2/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp 1
Switch(config-vrrp)# virtual-ip 192.168.1.1 backup
Switch(config-vrrp)#enable vrrp

(2) Verification

Use the following command to view information about VRRP:

show running-config
show vrrp
show vrrp 1

35. Configuring VLLP

This chapter includes the following contents:

- Introduction to VLLP
- VLLP configuration
- VLLP Configuration Example

35.1 Introduction to VLLP

VLLP (VRRP Layer-2 Loop Protect Protocol) is a private protocol proposed to solve the problem of Layer 2 Loop in the application of VRRP. When two three-layer switches are used to realize the redundant backup of the virtual route, a loop is formed between the three-layer switch and the two-layer switch, and the VLLP protocol informs each other of the port status on the respective link through message interaction,And calculate that that loop sets the state of the specific port to block so as to cut off the loop. A port set to the block state will be reset to the forward state if the timer expires. The VLLP protocol monitors and maintains the loop state of the port by notifying the port state change and timer timeout in time, and ensures that the loop is cut off in time. The VLLP protocol uses a query-reply approach to gather port status information. When two Layer 3 switches running the VLLP protocol start up,One is automatically elected to be in the sender state and the other in the receiver state. The sender is responsible for sending the query message regularly, and the receiver receives the query message and sends back the response message. When the receiver has a port status change, it needs to actively send a link status change message to notify the sender to make a corresponding change. The VLLP protocol needs to work with the VRRP protocol to start and maintain the state of the relevant ports in the VLAN on the VLAN. The VLLP protocol only needs to run on the VRRP switch, and the Layer 2 switch does not need to run any loop protection protocol.

Basic concept of VLLP protocol:

VLLP device: a VLLP protocol entity running on a VLAN is called a VLLP device.

VLLP port: a port that participates in VLLP protocol interaction in the VLAN corresponding to the VLLP device.

VLLP device status: The VLLP device has two statuses: sender and receiver.

a. **Sender:** The VLLP device in the sender state actively and periodically sends a VLLP query message.

b. **Receiver:** The VLLP device in the receiver state responds to the query message and actively sends the VLLP link state change message when the link state changes.

VLLP port status: The VLLP port has three STP statuses: disable, block, and forward.

Master port: When the VLLP device is in the sender state, a VLLP port is selected as the master port; a VLLP sender has only one master port. The VLLP port with high priority and mapping relationship can preempt to become the master port.

VLLP port mapping relationship: There is a VLLP port that performs VLLP protocol message interaction with the peer switch.

VLLP equipment receiver election principle:

a. The one with high priority becomes the receiver;

b. With the same priority, the one with the largest MAC address becomes the receiver.

Main port election principle:

a. The port must be link up

b. VLLP port must have a mapping relationship

If there is no VLLP port satisfying the condition, the master port does not exist;

If there are multiple VLLP ports that meet the conditions, the one with higher priority is selected as the master port; if the priorities are the same, the one with the earliest mapping relationship is selected as the master port.

VLLP port status determination principle:

If the VLLP device is the sender, the status of the master port must be forward;

The VLLP device is the sender, the link state is link up, and the VLLP port state without a mapping relationship is forward

The VLLP device is the sender, the link state is link up, a.nd the VLLP port state with the mapping relationship is block;

The VLLP device is the receiver, the link state is link up, and the VLLP port state is forward;

VLLP port with link down status is disable.

encapsulating the VLLP protocol message in the MAC frame

<table>
<tr><td colspan="5">Destination MAC Address (6 bytes)</td></tr>
<tr><td colspan="5">Source MAC Address (6 bytes)</td></tr>
<tr><td colspan="3">0x8100</td><td>Prio</td><td>Vlan ID (12 bits)</td><td>Ethernet Type (2 bytes)</td></tr>
<tr><td>Version</td><td>Type</td><td colspan="3">Port1(2 bytes)</td></tr>
<tr><td>Priority</td><td>Query Inter</td><td colspan="3">Main port</td></tr>
<tr><td colspan="5">Reserved (4 bytes)</td></tr>
<tr><td colspan="3">Port2</td><td>Link state</td><td>STP state</td></tr>
</table>

There are three types of VLLP protocol messages

1. Link state query message LQ
2. Link state response message LA
3. Link status change message LC

Value range of each domain in the message format:

Des MAC: Fixed to 00:09:ca:ff:ff

Src MAC: MAC of VLAN sending VLLP protocol message

Ethernet Type: fixed as 0x268e

Version: currently 1

Type: LQ is 1; LA is 2; LC is 3;

Port 1: index value of the port sending VLLP protocol message

Priority: VLLP device priority, value 1 ~ 255;

Query Interval: VLLP sender query timer interval, 5 seconds by default;

Main port: index value of main port of VLLP sender, only in LQ message;

Reserved: Reserved field is zero

Port 2: the index value of the port with status change in the LC message, and port2 is consistent with port1 in the LQ and LA messages;

Link state: the link state of port2, where link up is 1 and link down is 2;

STP state: STP state of port2, disable is 1, block is 2, and forward is 3.

VLLP protocol principle:

A VLLP device is configured in one VLAN and the VLLP protocol is started, and a VLLP device is also configured in the corresponding VLAN of the opposite-end switch and the VLLP protocol is started. The VLLP protocol entities (VLLP devices) running on the VLAN then form a sender and receiver pair. When the protocol is started, both sides are senders and send LQ messages to the other side. When the VLLP device receives the LQ message, it will elect a receiver according to the priority carried in the message and the MAC address of the opposite end. The winner becomes the receiver and responds to the sender's LQ message instead of sending the LQ message. When the receiver's timer times out and has not received the LQ message, the receiver will return to the sender state and start sending the LQ message.

In a VLAN in which the VLLP protocol is enabled, the port participating in VLLP protocol message interaction needs to be configured as a VLLP port. The VLLP port can be a valid layer 2 port (including a trunk group), but the trunk member is not allowed to be configured as a VLLP port. VLLP protocol messages are sent and received through VLLP ports. The VLLP port and the VLLP port configured in the VLAN of the opposite end switch which starts the VLLP protocol correspondingly form a pair of mapping relations, which determine the mapping relation with the opposite end port by sending a query message and receiving a response message or changing a message, and calculate the loop which may exist in the network according to the mapping relation and the link state thereof, Stops loops in the topology by maintaining the STP state of the ports according to the VLLP port state determination.

Multiple VLLP ports can be enabled within a VLAN that has the VLLP protocol enabled, and they may or may not be physically linked to the peer switch. When a port belongs to multiple VLANs, the same VLLP port can also appear in multiple VLLP devices. The VLLP protocol dynamically collects the information of the link state change of the VLLP port and the STP state of the opposite VLLP port to calculate the loop in time and effectively prevent the occurrence of the loop in the network.

When there are multiple VLANs with the same port configuration, but the VLLP protocol needs to be started on multiple VLANs, each layer 2 port needs to send and receive multiple VLLP protocol messages running on different VLANs, resulting in the burden of the switch, so the concept of attached VLAN is proposed. That is, VLANs with identical port configurations run the VLLP protocol on only one VLAN, the primary VLAN, while the remaining VLANs are added as secondary VLANs on the instance of the primary VLAN.A result of that calculation of the loop by the VLLP protocol on the primary VLAN is written to the in-instance port state. It should be noted that when configuring the secondary VLAN, ensure that all VLLP ports of the primary VLAN are in the secondary VLAN and all ports of the secondary VLAN are in the primary VLAN. When the affiliated VLAN is configured and a layer 2 port is added to the affiliated VLAN, if the port is also in the main VLAN, the main VLAN manages the port state uniformly; if the port is not in the main VLAN, the port state cannot be managed, and an alarm message is prompted.

35.2 VLLP configuration

After the VLLP protocol is started, the related attribute configuration and port creation can be performed, and the related commands are in the VLLP configuration mode.

Configurations for VLLP include:

- Create a vllp device on a Layer 3 interface
- Enable the vllp device
- Create a vllp port on the Layer 2 interface
- Configure vllp device priority
- Configure the vllp device query timer interval
- vlanconfigure an affiliated VLAN
- Configure vllp port priority

35.2.1 Create a vllp device on a Layer 3 interface

Mode: Global Configuration Mode

Command：router vllp <if-name>　Create a vllp device and enter VLLP configuration mode

Command：no router vllp <if-name>　Remove vllp device

Parameter: if-name is the agreed three-layer interface name (for example:　vlan1 vlan2 …)

Default: Do not start the vllp protocol

35.2.2 Enable the vllp device

Mode: VLLP Configuration Mode

Command：vllp enable　Enable the vllp device

Command：vllp disable　Disable vllp device

Default: vllp device is not started after creation

35.2.3 Create a vllp port on the Layer 2 interface

Mode: VLLP Configuration Mode

Command：vllp port <if-name>　Create vll p port

Command：no vllp port <if-name>　Delete vllp port

Parameter: if-name is the agreed L2 interface name (for example: ge1/1 tr unk1 …)

Default: The vllp protocol is not applied to the Layer 2 port. The vllp protocol cannot be applied when the layer 2 interface is a trunk member.

35.2.4 Configure vllp device priority

Mode: VLLP Configuration Mode

Command：vllp priority <priority>　Configure vllp device priority

Command：no vllp priority [priority]　Restore vllp device priority to default

Parameter: priority value is between 1 and 255.　The priority is used by the vllp device to elect a recipient.

Default: 100

35.2.5 Configure the vllp device query timer interval

Mode: VLLP Configuration Mode

Command：vllp query-interval <interval> Configure Local Query Timer Interval

Command：no vllp query-interval [interval] Resume query timer interval is default

Parameter: interval is between 1 and 255. The configuration values take effect when the vllp device is the sender or when it is migrated back to the sender.

Default: 5 second

35.2.6 Configure an affiliated VLAN

Mode: VLLP Configuration Mode

Command：vllp dependency <if-name> configure an affiliated VLAN

Command：no vllp dependency <if-name> Remove attached VLAN

Parameter: if-name is the agreed three-layer interface name (for example: vlan1 vlan2 …)

Default: no secondary VLAN is configured

35.2.7 Configure vllp port priority

Mode: VLLP Configuration Mode

Command：vllp port <if-name> priority <priority> Configure vllp port priority

Command：no vllp port <if-name> priority [priority] Restore vllp port priority to default

Parameter: if-name is the agreed L2 interface name (for example: ge1/1 trunk1 …) ; the priority value is between 1 and 255. The priority is used by the vllp sender to elect the primary port.

Default:100

35.2.8 Display Information

Mode: Normal or Privileged

Command：show vllp Displays a list of vllp devices for the vllp protocol

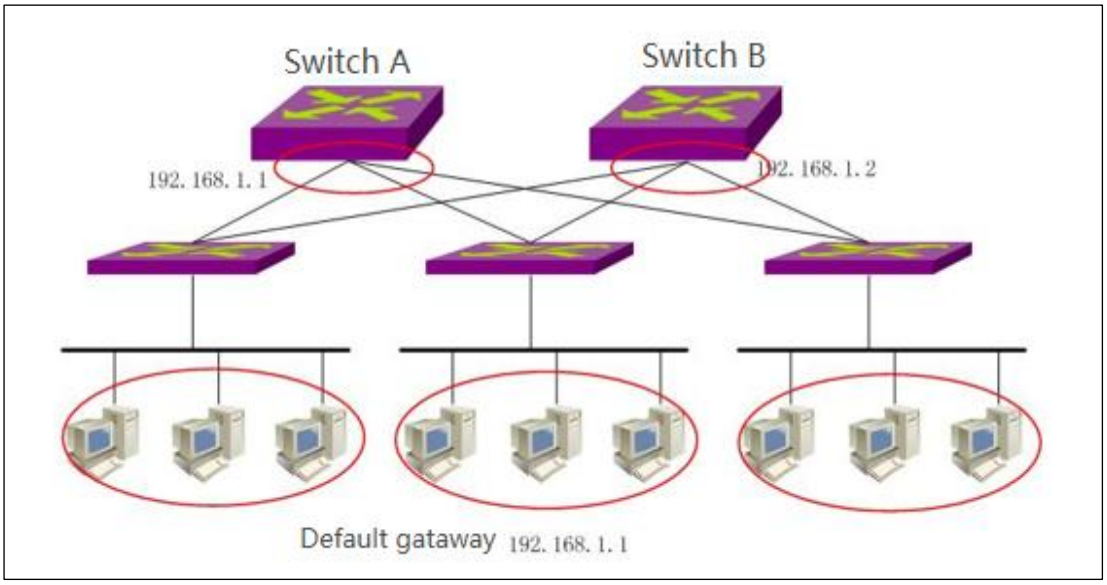
Command：show vllp <if-name> Displays detailed information about a vllp device

Parameter: if-name is the agreed three-layer interface name (for example: vlan1 vlan2 …)

Command：show vllp map Display the mapping relationship of each vllp port in the vllp protocol

35.3 VLLP Configuration Example

(1) Configuration



Configuration on Switch A:

Switch#configure terminal

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#ip interface vlan 2

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport access vlan 2

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switchport access vlan 2

Switch(config-ge1/2)#interface ge1/3

Switch(config-ge1/3)#switchport access vlan 2

Switch(config-ge1/3)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.1/24

Switch(config-vlan2)#exit

Switch(config)#router vrrp 1

Switch(config-vrrp)# virtual-ip 192.168.1.1 master

Switch(config-vrrp)#enable

Switch(config-vrrp)#exit

Switch(config)#router vllp vlan2

Switch(config-vllp)#vlllp port ge1/1

Switch(config-vllp)#vllp port ge1/2

Switch(config-vllp)#vllp port ge1/3

Switch(config-vllp)#vllp enable

Configuration on Switch B:

Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config)#ip interface vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 2
Switch(config-ge1/3)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.2/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp 1
Switch(config-vrrp)# virtual-ip 192.168.1.1 backup
Switch(config-vrrp)#virtual-interface vlan1
Switch(config-vrrp)#enable
Switch(config-vrrp)#exit
Switch(config)#router vllp vlan2
Switch(config-vllp)#vlllp port ge1/1
Switch(config-vllp)#vllp port ge1/2
Switch(config-vllp)#vllp port ge1/3
Switch(config-vllp)# enable

(2) Verification

Use the following command to view VLLP information:

show vllp
show vllp <if-name>
show vllp map

36. Configuring Policy Routing

This chapter includes the following contents:

- Introduction to Policy Routing
- Policy routing configuration
- Policy Routing Configuration Example

36.1 Introduction to Policy Routing

Policy-based routing is a routing mechanism based on user's policy. Different from simply looking up the routing table according to the destination address of the IP packet for forwarding, policy routing is based on some attributes of the packet information, such as destination address, source address and other information to flexibly select the route. And that route knowledge of the router is enrich.

36.2 Policy routing configuration

The configuration includes the following:

- Create a new policy route
- Insert a policy route
- Delete a policy rout
- Move a policy route
- View policy routing information

36.2.1 Create a new policy route

The following command creates a new policy route in global configuration mode:

policy route <ID> <SIP> <DIP> <next-hop>

ID: Indicates the ID of the newly created policy routing rule, ranging from 1 to 100.

SIP, DIP: There are three input methods for source and destination IP:

1) A.B. C. D wildcard can control IP addresses from one network segment;

2) any is equivalent to the A. B. C. D 255.255. 255.255

3) host A. B. C. D is equivalent to A. B. C. D 0.0. 0.0

wildcard: Determines which bits need to be matched. '0' means match is required, and' 1 'means no match is required.

next-hop: Indicates the address of the next-hop host, in the format of A. B. C. D.

36.2.2 Insert a policy route

The following command inserts a new policy route in global configuration mode:

policy route insert <ID> <SIP> <DIP> <next-hop> before <EXIST_ID>

ID: Indicates the ID of the newly inserted policy rule, ranging from 1 to 100.

SIP, DIP: There are three input methods for source and destination IP:

1) A.B. C. D wildcard can control IP addresses from one network segment;

2) any is equivalent to the A. B. C. D 255.255. 255.255

3) host A. B. C. D is equivalent to A. B. C. D 0.0. 0.0

wildcard: Determines which bits need to be matched. '0' means match is required, and' 1 'means no match is required.

next-hop: Indicates the address of the next-hop host, in the format of A. B. C. D.

EXIST _ ID: Indicates which rule to insert before. Range: 1-100.

36.2.3 Delete a policy route

The following command deletes a policy route in global configuration mode:

no policy route <ID>

ID: Indicates the ID of the policy rule to be deleted, in the range of 1-100.

36.2.4 Move a policy route

The following command moves a policy route to a destination in global configuration mode:

policy route move <ID> (before|after) <TO_ID>

ID: Indicates the rule that needs to be moved.

(Before after): Indicates before or after the move target rule

36.2.5 View policy routing information

The following command is executed in normal or privileged mode to view all policy routing information:

show policy route

36.3 Policy Routing Configuration Example

Configure the source IP address as 192.168.3.100 and the gateway as 192.168.0.20.

Switch#configure terminal

Switch#(config)#policy route 1 host 192.168.3.100 any 192.168.0.20

Configure a gateway with a destination IP address of 192.168.10.100 and route to 192.168.2.1.

Switch#configure terminal

Switch#(config)#policy route 2 any host 192.168.10.100 192.168.2.1

Configure the source IP address as 192.168.3.100, the destination IP address as 10.10.10.100, and the gateway as 192.168.5.1.

Switch#configure terminal

Switch#(config)#policy route 3 host 192.168.3.100 host 10.10.10.100 192.168.5.1

37. Configuring the System Log

This chapter includes the following contents:

- System Log Introduction
- Syslog Configuration

37.1 System Log Introduction

The system log module is an important part of the switch, which is used to record the operation of the whole system, abnormal behavior and user's operation behavior, and help administrators to understand and monitor the work of the system in time. The system log module manages all the log information of the system from the running modules, and collects, classifies, stores and displays the log information.

In the log system, there is also an important debugging function. With debugging, system logs can help administrators or other technicians to monitor the operation of the network, debug and diagnose the faults in the network. The administrator can easily select the content to be debugged, and locate and solve the fault of the device or network by observing the log information output by debugging.

This section mainly includes the following contents:

- Format of log information
- Log storage
- Log display
- debugging tool

37.1.1 Format of log information

The format of the log information is as follows:

Timestamp, priority, module name, log content

There is a space between the timestamp and the priority, a colon and a space between the priority and the module name, and a colon and a space between module name and log content.

An example of the format of the log information is as follows:

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2

In this log message, the timestamp is 2006/05/20 13:56:34; the priority is Warning; the module name is MSTP; and the log content is Port up notification received for port ge1/2.

1) Timestamp

Format of timestamp: year/month/day hour: minute: second.

The hour is a 24-hour clock, from 0 to 23.

The time stamp records the time when the log information is generated, and the system time of the switch is used. The system time has been set when the switch leaves the factory and can be modified by the administrator. The system time can still run after the device is powered off.

2) Priority

The priority records the importance of the log information. According to the importance of the log information, the log information is divided into four levels. The order of priority from high to low is: Critical, Warning, Informational and Debugging. The priority is described in the following table:

Priority	Description
Critical	Serious error
Warning	General errors, warnings, and very important tips
Informational	Important tips, general tips, diagnostic information
Debugging	Debugging information

3) Module name

The module name records the module generated by this log information. The following table lists some major modules that generate log information:

Module name	Description
CLI	Command line interface module
MSTP	Multi-instance Spanning Tree Protocol Module
VLAN	VLAN function module
ARP	ARP protocol module
IP	IP protocol module
ICMP	ICMP protocol module
UDP	UDP protocol module
TCP	TCP protocol module

4) Log content

Log content is a phrase or sentence, representing the main idea of the log information. Administrators can know what happened to the system by reading the log content.

37.1.2 Log storage

Logs are generally stored in three ways:

- The log is stored in memory.
- Log is stored in NVM.
- Log is stored in the server.

There are four log tables in the memory according to the priority of the log, and each table stores the log information of one priority, that is, the log is divided into four categories according to the priority of the log, and each category of log is stored in a separate log table. Each log table has 1K entries, which can store 1K log information. When the log table is full, the following log covers the longest log information. This storage method has a problem, when the system restarts, the log information is gone, the administrator can not see the log information when the system crashes, and can not locate the problem.

For the important log information, such as the log information with the priority of Critical and Warning, the log information can be stored in the NVM of the system. In this way, after the system is restarted, the log information in the NVM can be retained, which is convenient for the administrator to locate the problem when the system crashes. However, a problem with this storage method is that due to the capacity limitation of NVM, the log information entries stored in NVM are very limited.

Another better way is to store the log information in the server, which can be achieved by using the SYSLOG protocol. The log information can be sent to the server in real time, and the server saves the log information and displays it on an interface. This storage method is not only convenient for users to

view log information, but also has a huge capacity, which can store a large number of log information on the server.

Currently, the system only supports storing the log information in the memory, and does not support storing the log information in the NVM or the server.

37.1.3 Log display

There are two ways to display the log: manual display and real-time display. Manual display means that the user displays the log information by inputting commands. Real-time display means that when the log information is generated, the log information is directly output to the terminal, and the user can see it in time.

For the manual display mode, the user can view all the log information. The display order of the log information is that the last log information is placed in the front, so that the user can see the latest operation status of the switch first.

For the real-time display mode, the user must turn on the terminal real-time display switch. If the switch is on, the generated log information is not only written to the log table, but also output to the terminal. If the switch is off, the log information will not be displayed on the terminal in real time. Currently, the system can only output log information to the Console terminal in real time, and does not support outputting log information to the Telnet terminal.

37.1.4 Debugging tool

debugging is a diagnostic tool for devices and networks. It tracks the sending and receiving of data packets of the system and modules, and the changes of the state machine of the modules, so that the administrator can understand and monitor the running process of the system and modules. If the network or devices are abnormal, it can be tracked through the debugging tool.

The debugging tool provides a wealth of switches that administrators can control to keep track of what they are interested in.When the device or network is abnormal, the administrator can turn on the debugging switch related to the abnormality and find the problem by tracing the execution process of the system and module.

When a debugging switch is turned on, the system will generate relevant log information, which will be written to the corresponding log table. In general, the priority of log information generated by debugging is Informational. When the terminal real-time display switch is turned on, the log information will be output to the terminal in real time. When the debugging switch is turned off, the system will not generate relevant log information.

37.2 Syslog Configuration

System log configuration includes the following:

- Configure terminal real-time display switch
- View log information
- Configure debugging switch
- View debugging information

37.2.1 Configure terminal real-time display switch

By default, the terminal real-time display switch is turned off, and the log information generated by the system is written into the log table, but will not be displayed on the terminal in real time. Some log information in the system is not restricted by this switch, and these log information will always be output to the Console terminal in real time.

At present, the switch can only display the log information in real time on the Console terminal, but not on the Telnet terminal.

When the user uses the write command to store the current configuration of the system into the configuration file, the configuration of the terminal real-time display switch will not be stored in the configuration file of the system. When the system is restarted, these configurations will be lost and need to be reconfigured.

The commands for configuring the real-time display switch of the terminal are shown in the following table:

Command	Description	CLI Mode
log stdout	Turn on the terminal real-time display switch	Configuration Mode
no log stdout	Close the real-time display switch of the terminal	Configuration Mode

37.2.2 Set Log Level

The commands for setting the log level are shown in the following table:

Command	Description	CLI Mode
log trap <[alerts | critical | debugging | emergencies | errors | informational | notifications | warnings]>	Set Log Level	Configuration Mode

37.2.3 View log information

The commands for viewing log information are shown in the following table:

Command	Description	CLI Mode
show log	Show all log information	Configuration Mode

37.2.4 Configure debugging switch

The system provides rich debugging switches, which involve multiple modules. Only the schematic commands of each module are listed here. For the complete format of the commands, see the command manual.

When the user uses the write command to store the current configuration of the system in the configuration file, the configuration of the debugging switch will not be stored in the configuration file of the system. When the system is restarted, these configurations will be lost and need to be reconfigured.

The commands for configuring the debugging switch is as follows:

Command	Description	CLI Mode
debug ip …	Turn on relevant debugging switches for the system to send and receive IP packets	Privileged mode
no debug ip …	Turn off the power switch related to sending and receiving IP packets of the system	Privileged mode
debug ip icmp …	Turn on related debugging switches for the system to send and receive ICMP packets	Privileged mode
no debug ip icmp …	Turn off the debugging switch related to sending and receiving ICMP packets by the system	Privileged mode
debug ip arp …	Turn on related debugging switches for the system to send and receive ARP packets	Privileged mode
no debug ip arp …	Turn off the debugging switch related to sending and receiving ARP packets by the system	Privileged mode
debug ip udp …	Turn on related debugging switches for the system to send and receive UDP packets	Privileged mode
no debug ip udp …	Turn off the debugging switch related to sending and receiving UDP packets by the system	Privileged mode
debug ip tcp …	Turn on related debugging switches for the system to send and receive TCP packets	Privileged mode
no debug ip tcp …	Turn off the debugging switch related to sending and receiving TCP packets by the system	Privileged mode
debug mstp …	Turn on the debugging switch related to MSTP protocol diagnosis	Privileged mode
no debug mstp …	Turn off the debug switch related to MSTP protocol diagnosis	Privileged mode
debug igmp snooping …	Turn on the debugging switch related to IGMP SNOOPING protocol diagnosis	Privileged mode
no debug igmp snooping …	Turn off the debug switch related to IGMP SNOOPING protocol diagnosis	Privileged mode
debug dhcp snooping …	Turn on the debugging switch related to DHCP SNOOPIN protocol diagnosis	Privileged mode
no debug dhcp snooping …	Turn off the debug switch related to DHCP SNOOPIN protocol diagnosis	Privileged mode
no debug all	Turn off all debugging switches on the system	Privileged mode

37.2.5 View debugging information

The command to view debugging information is as follows:

Command	Description	CLI Mode
	View the debugging switch configuration. If no parameter is entered, check the debugging switch configuration of all modules. If only one parameter is entered, check the debugging switch configuration of only one module. If the input parameter is IP, the debugging switch configuration of IP, ICMP, ARP, UDP, and TCP modules will be checked.	Normal mode, privileged mode

37.3 Configuring SYSLOG

SYSLOG includes the following:

- Introduction to SYSLOG
- SYSLOG configuration
- SYSLOG Configuration Example

37.3.1 Introduction to SYSLOG

SYSLOG is a standard protocol for device log information management, which is widely used because of its simple design. In the SYSLOG system, it is divided into three parts.

One is to define each sub-module so as to distinguish the log information generated by different modules, and to define different log information levels so as to observe the equipment operation status. All kinds of log information of the device are collected according to this agreement.

The second is the configuration file, which defines how to process the collected log information. It can be saved locally, sent to the designated server on the network, and distributed to the designated login users. The configuration file determines how to save the log information generated by the device.

The third is to send the SYSLOG protocol message according to the message format defined by RFC. It can be seen that in our switch system, the working convention of the whole SYSLOG is the system log module.

The first part of the SYSLOG protocol is completed by each functional sub-module in the switch, which sends its own log information of each level to the system log module. Four levels of log tables are maintained in the syslog module.

In the second part of the SYSLOG protocol, the system log module is used to uniformly distribute the log information. First, the log information is displayed on the serial port terminal in real time or manually through the terminal display switch. Second, four levels of log tables are stored in the memory. Third, high-level log information is stored on the NVM to avoid losing important log records in case of power failure; Fourth, the log is sent to the remote server for storage, collection and collation through the SYSLOG message. The SYSLOG submodule in the system log module only implements the third part of the function to transmit the system log to the server.

37.3.2 SYSLOG configuration

The SYSLOG configuration command contains:

- Open the syslog server address
- Close the syslog server address
- Open the syslog protocol

Command	Description	CLI Mode
syslog open <server-ip>	Open the syslog server address; the parameter server-ip is the server IP address.	Configuration Mode
syslog close	Close the syslog server address	Configuration Mode
log syslog	Open the syslog protocol	Configuration Mode

37.3.3 SYSLOG Configuration Example

(1) Configuration

Configure the IP address of the syslog server as 192.168.0.201, and configure the switch as follows:

Switch#configure terminal

Switch(config)#syslog open 192.168.0.201

Switch(config)# log syslog

(2) Validate

Switch#show syslog

Syslog is opened!

server ip address: 192.168.0.201

udp destination port: 514

severity level: debugging

local device name: switch

38. IPv6 Basic Configuration

The switch supports basic IPv6 functions, including IPv6 Layer 2 forwarding and IPv6 ND functions. This chapter describes how to configure IPv6 and includes the following:

- Introduction to IPv6
- Configure basic functions of IPv6
- Configure IPv6 Neighbor Discovery Protocol
- IPv6 display and maintenance

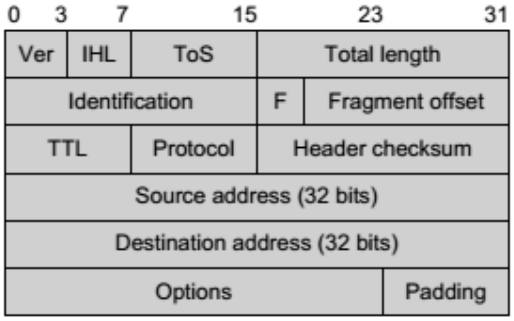
38.1 Introduction to IPv6

IPv6 (Internet Protocol Version 6, Internet Protocol Version 6) is the second generation standard protocol of the network layer protocol, and is also called IPng (IP Next Generation, the next generation Internet). It is a set of specifications designed by IETF (Internet Engineering Task Force) and an upgraded version of IPv4. The most significant difference between IPv6 and IPv4 is that the length of the IP address has increased from 32 bits to 128 bits.

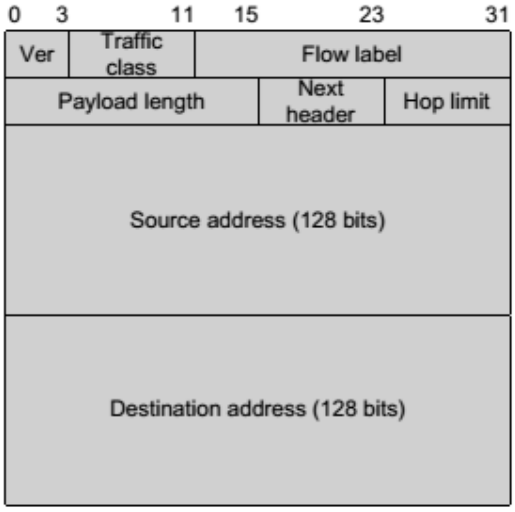
38.1.1 IPv6 Protocol Features

(1) Simplified header format

The length of the IPv6 basic header is reduced by reducing or moving some fields in the IPv4 header into the extended header. IPv6 uses a fixed-length basic packet header, which simplifies the processing of IPv6 packets by forwarding devices and improves the forwarding efficiency. Although the IPv6 address is four times as long as the IPv4 address, the IPv6 basic header is only 40 bytes long, which is twice as long as the IPv4 header (excluding the options field).



IPv4 header



Basic IPv6 header

(2) Sufficient address space

The length of source address and destination address of IPv6 is 128 bits (16 bytes). It can provide more than 3.4×1038 possible address spaces, which can fully meet the needs of multi-level address division, as well as the address allocation of public networks and private networks within institutions.

(3) Hierarchical address structure

The address space of IPv6 adopts a hierarchical address structure, which is conducive to rapid routing lookup, and can effectively reduce the system resources occupied by the IPv6 routing table with the help of routing aggregation.

(4) Automatic address configuration

To simplify host configuration, IPv6 supports both stateful and stateless address configuration:

1) Stateful address configuration refers to obtaining an IPv6 address and related information from a server (such as a DHCP server);

2) Stateless address configuration means that the host automatically configures the IPv6 address and related information according to its own link layer address and the prefix information issued by the router.

At the same time, the host can also form a link local address according to its own link layer address and default prefix (FE80:/10) to realize communication with other hosts on the link.

(5) Built-in security

IPv6 uses IPSec as its standard extension header, which can provide end-to-end security features. This feature also provides a standard for solving network security problems and improves the interoperability between different IPv6 applications.

(6) Support QoS

The Flow Label field of the IPv6 packet header identifies the flow, allowing the device to identify the packet in a certain flow and provide special processing.

(7) Enhanced neighbour discovery mechanism

The neighbour discovery protocol of IPv6 is implemented through a set of ICMPv6 (Internet Control Message Protocol for IPv6) messages, and manages the interaction of information between neighbor nodes (i.e., nodes on the same link). It replaces ARP (Address Resolution Protocol), ICMPv4 router discovery, and ICMPv4 redirect messages, and provides a range of other features.

(8) Flexible extended message header

IPv6 cancels the option field in the IPv4 header and introduces a variety of extended headers, which not only improves the processing efficiency, but also greatly enhances the flexibility of IPv6 and provides a good scalability for IP protocol. The option field in the IPv4 header is only 40 bytes at most, while the size of the IPv6 extension header is only limited by the size of the IPv6 packet.

38.1.2 IPv6 Address Introduction

(1) IPv6 address representation

IPv6 addresses are represented as a series of 16-bit hexadecimal numbers separated by colons (:). Each IPv6 address is divided into 8 groups, the 16 bits of each group are represented by 4 hexadecimal numbers, and the groups are separated by colons, for example, 2001:0000: 130F: 0000:0000: 09C0: 876a: 130B.

In order to simplify the representation of the IPv6 address, the "0" in the IPv6 address can be processed as follows:

1) The leading "0" in each group can be omitted, that is, the above address can be written as 2001:0: 130F: 0:0:9 C0: 876A: 130B.

2) If the address contains two or more consecutive groups of 0, it can be replaced by a double colon ":", that is, the above address can be written as 2001:0: 130F: 9 C0: 876 A: 130B.

Notice:

The double colon ":" can only be used once in an IPv6 address, otherwise the number of zeros represented by the ":" will not be determined when the device changes the "::" to a zero to recover a 128-bit address.

An IPv6 address consists of two parts: an address prefix and an interface identifier. The address prefix corresponds to the network number field portion of the IPv4 address, and the interface identifier corresponds to the host number portion of the IPv4 address.

The address prefix is expressed as: IPv6 address/prefix length. Where the IPv6 address is any of the forms listed previously, and the prefix length is a decimal number indicating how many of the leftmost bits of the IPv6 address are the address prefix.

(2) IPv6 address classification

IPv6 has three main types of addresses: unicast address, multicast address and anycast address.

- **Unicast address:** It is used to uniquely identify an interface, similar to the unicast address of IPv4. Datagrams sent to a unicast address are delivered to the interface identified by that address.
- **Multicast address:** It is used to identify a group of interfaces (usually belonging to different nodes), similar to the multicast address of IPv4. Datagrams sent to a multicast address are delivered to all interfaces identified by that address.
- **Anycast address:** Used to identify a group of interfaces (usually belonging to different nodes). A datagram sent to an anycast address is delivered to the interface from the group of interfaces identified by that address that is closest (as measured by the routing protocol in use) to the source node.

There is no broadcast address in IPv6, and the function of broadcast address is realized by multicast address.

The IPv6 address type is specified by the first few bits of the address (called the format prefix). The correspondence between the main address type and the format prefix is shown in Table 1-1 below.

Table 1-1 Correspondence between Address Type and Format Prefix

	Address Type	Format Prefix (Binary)	IPv6 prefix identification
Unicast addr	No address specified	00...0(128 bits)	::/128
	Loopback addr	00...1(128 bits)	::1/128
	Link-local addr	1111111010	FE80::/10
	Site Local Address	1111111011	FEC0::/10
	Global unicast addr	Other forms	-
Multicast addr		11111111	FF00::/8
Anycast addr		From the unicast address space, using the format of a un icast addr	

(3) Types of unicast addr

There are many types of IPv6 unicast addresses, including global unicast addresses, link-local addresses, and site-local addresses.

1) The global unicast address is equivalent to the IPv4 public network address and is provided to the network service provider. This type of address allows aggregation of routing prefixes, limiting the number of global routing table entries.

2) **Link-local addresses** are used for communication between nodes on a link-local in Neighbor Discovery Protocol and Stateless Autoconfiguration. Datagrams that use link-local addresses as source or destination addresses are not forwarded to other links.

3) **Site-local addresses** are similar to private addresses in IPv4. Datagrams that use the site-local address as the source or destination address will not be forwarded to other sites outside the site (equivalent to a private network).

4) **Loopback address:** The unicast address 0:0:0:0 (abbreviated as: 1) is called a loopback address and cannot be assigned to any physical interface. Its function is the same as the loopback address in IPv4, that is, the node is used to send IPv6 messages to itself.

5) **Unspecified address:** The address ":" is called an unspecified address and cannot be assigned to any node. Before the node obtains a valid IPv6 address, the address can be filled in the source address field of the IPv6 message sent, but it cannot be used as the destination address in the IPv6 message.

(4) Multicast addr

The multicast addresses shown in Table 1-2 are reserved for special purposes

Table 1-2 Reserved IPv6 Multicast Addresses List

address	application
FF01::1	All node multicast address in node local scope
FF02::1	Link local range all node multicast addr
FF01::2	Node Local Scope All Routers Multicast Addr
FF02::2	Link local scope all rout multicast addr
FF05::2	All route multicast addresses in that site-local ran

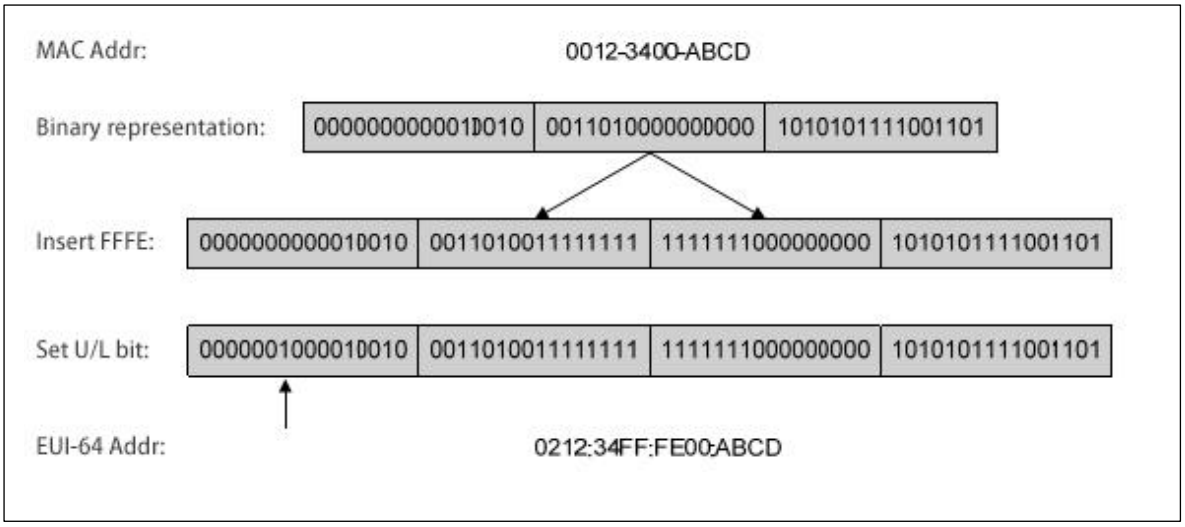
There is another type of multicast address: the solicited-node address. The address is mainly used for obtaining the link layer address of the neighbor node on the same link and realizing duplicate address detection. Each unicast or anycast IPv6 address has a corresponding requested node address. The format is:

FF02:0:0:0:0:1:FFXX:XXXX

Where FF02: 0:0:0:1: FF is a 104-bit fixed format, and XX: XXXX is the last 24 bits of a unicast or anycast IPv6 address.

(5) Interface identifier in IEEE EUI-64 format

The interface identifier in an IPv6 unicast address is used to identify a unique interface on a link. Currently, IPv6 unicast addresses basically require an interface identifier of 64 bits. The interface identifier in the IEEE EUI-64 format varies from the link layer address (MAC address) of the interface. Because the interface identifier in an IPv6 address is 64 bits and the MAC address is 48 bits, the hexadecimal number FFFE (1111111111111110) needs to be inserted in the middle of the MAC address (after the 24th bit from the high order). To ensure that the interface identifier derived from the MAC address is unique, also set the Universal/Local (U/L) bit (bit 7 from the high order) to "1". The resulting set of numbers is used as the interface identifier in EUI-64 format.



38.1.3 Introduction of IPv6 Neighbour Discovery Protocol

IPv6 neighbour discovery protocol uses five types of ICMPv6 messages to implement the following functions: address resolution, neighbour reachability verification, duplicate address detection, router discovery/prefix discovery, address autoconfiguration, and redirection.

The types and functions of ICMPv6 messages used by the neighbour discovery protocol are shown in Table 38.1.3 below.

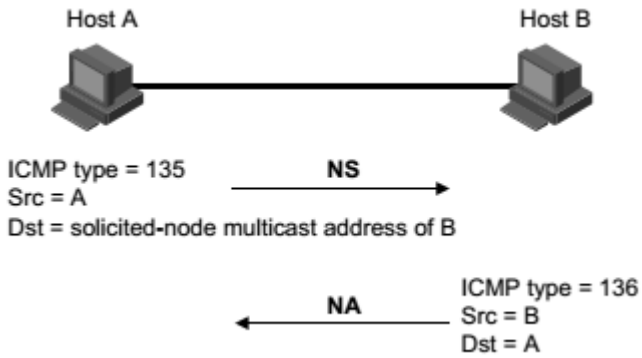
Table 38.1.3 ICMPv6 Message Types and Functions Used by Neighbour Discovery Protocol

ICMPv6 message	Type No.	Action
Neighbour Solicitation	135	Gets the link layer address of the neighbour
		Verify whether the neighbour is reachable
		Perform duplicate address detection
Neighbour Advertisement	136	Respond to NS message
		When the link layer changes, the node actively sends an NA message to notify the neighbour nodes of the change information of the node
Router Solicitation	133	After the node is started, the node sends a request to the router through an RS message to request a prefix and other configuration information for automatic configuration of the node
Router Advertisement	134	Respond to the RS message
		If the RA message is not suppressed, the router will periodically issue the RA message, which includes the prefix information option and some flag bit information
Redirect	137	When certain conditions are met, the default gateway sends a redirection message to the source host, so that the host reselects a correct next hop address to send subsequent messages.

The main functions provided by the Neighbour Discovery Protocol are as follows:

(1) Address resolution

Obtain the link layer address of the neighbour node on the same link (the same as the ARP function of IPv4), which is realized by the neighbour request message NS and the neighbour advertisement message NA. As shown in the following figure, Node A wants to obtain the link layer address of Node B.



- Node A sends an NS message in a multicast manner. The source address of the NS message is the interface IPv6 address of node A, the destination address is the multicast address of the requested node of node B, and the message content includes the link layer address of node A.
- after receiving the NS message, the node B judges whether the destination address of the message is the multicast address of the requested node corresponding to its own IPv6 address. If so, node B can learn the link-layer address to node A and return an NA message in unicast mode with its own link-layer address.
- Node A can obtain the link layer address to node B from the received NA message.

(2) Verify whether the neighbour is reachable

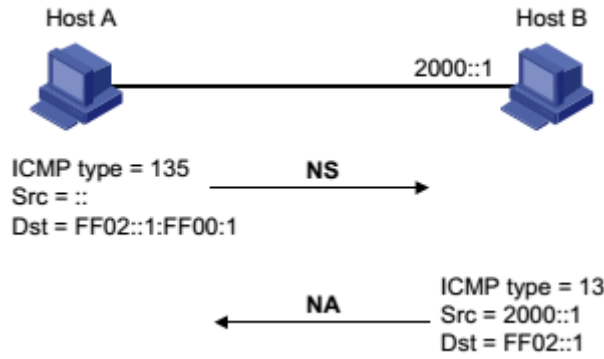
After the link layer address of the neighbour node is obtained, whether the neighbour node is reachable may be verified through the neighbour solicitation message NS and the neighbour advertisement message NA.

- The node sends the NS message, where the destination address is the IPv6 address of the neighbour node.
- if the confirmation message of the neighbour node is received, the neighbour is considered to be reachable, otherwise, the neighbour is considered to be unreachable.

(3) Duplicate address detection

When a node acquires an IPv6 address, it needs to use the duplicate address detection function to determine whether the address has been used by other nodes (similar to the free ARP function of IPv4). Duplicate address detection can be achieved through NS and NA, as shown in Figure 1-4.

Figure 1-4 Duplicate Address Detection Diagram



1) Node A sends an NS message, where the source address of the NS message is an unspecified address:, the destination address is the multicast address of the requested node corresponding to the IPv6 address to be detected, and the message content includes the IPv6 address to be detected.

2) If Node B is already using this IPv6 address, a NA message is returned. It contains its own IPv6 address.

3) When node A receives the NA message from node B, it knows that the IPv6 address has been used. Otherwise, the address is not used, and Node A can use the IPv6 address.

(4) Router discovery/prefix discovery and address auto-configuration

Router discovery/prefix discovery means that the node obtains the prefix of the neighbor router and the network where it is located, as well as other configuration parameters, from the received RA message.

Address stateless auto-configuration means that the node automatically configures the IPv6 address according to the information obtained by router discovery/prefix discovery. Router discovery/prefix discovery is achieved by means of router solicitation messages RS and router advertisement messages RA, The specific process is as follows:

- When the node is started, it sends a request to the router through the RS message, requesting the prefix and other configuration information for the configuration of the node.
- The router returns an RA message that includes the prefix information option (the router also issues RA messages periodically).
- the node automatically configures the IPv6 address and other information of the interface by using the address prefix and other configuration parameters in the RA message returned by the router.
- The prefix information option includes not only the information of the address prefix, but also the preferred lifetime and valid lifetime of the address prefix. After receiving the RA message sent periodically, the node will update the preferred lifetime and valid lifetime of the prefix according to the message.
- During the valid lifetime, the automatically generated address can be used normally; after the valid lifetime expires, the automatically generated address will be deleted.

(5) Redirection function

When a host starts up, it may have only one default route to the default gateway in its routing table. When certain conditions are met, the default gateway will send an ICMPv6 redirect message to the source host to notify the host to select a better next hop to send subsequent packets (the function is the same as that of the IPv4 ICMP redirect message).

When the following conditions are met, the device will send an ICMPv6 redirection message that redirects the host:

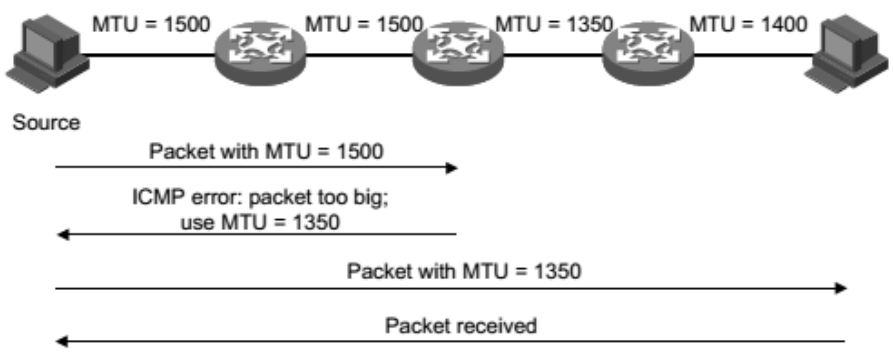
- the interfaces for receiving and forwarding the data message are the same interface;
- The selected route itself has not been created or modified by the ICMPv6 redirect message;
- The selected route is not the default route;
- The forwarded IPv6 data packet does not contain a routing extension header.

38.1.4 IPv6 PMTU discovery

The links through which the message passes in the transmission path from the source end to the destination end may have different MTUs. In IPv6, when the length of the packet is greater than the MTU of the link, the fragmentation of the packet will be carried out at the source end, thus reducing the processing pressure of the intermediate forwarding equipment and making rational use of network resources.

The purpose of the PMTU (Path MTU) discovery mechanism is to find the minimum MTU on the path from the source to the destination. The working process of PMTU is shown in Figure 1-5.

Figure 1-5 Working Process of PMTU Discovery



1) The source host uses its own MTU to fragment the message, and then sends the message to the destination host.

2) When the intermediate forwarding device receives the message and forwards it, if it finds that the MTU value supported by the interface that forwards the message is less than the length of the message, it will discard the message and return an ICMPv6 error message to the source, which contains the MTU of the interface that failed to forward.

3) after receiving the error message, the source host will use the MTU carried in the message to re-fragment the message and send it.

4) repeat that process until the destination end host receive the message so as to determine the minimum MTU in the path of the message from the source end to the destination end.

38.1.5 Protocol Specification

The protocol specifications related to the IPv6 foundation are:

- RFC 1881：IPv6 Address Allocation Management
- RFC 1887：An Architecture for IPv6 Unicast Address Allocation
- RFC 1981：Path MTU Discovery for IP version 6
- RFC 2375：IPv6 Multicast Address Assignments
- RFC 2460：Internet Protocol, Version 6 (IPv6) Specification.
- RFC 2461：Neighbour Discovery for IP Version 6 (IPv6)
- RFC 2462：IPv6 Stateless Address Autoconfiguration
- RFC 2463：Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6 (IPv6) Specification
- RFC 2464：Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526：Reserved IPv6 Subnet Anycast Addresses
- RFC 3307：Allocation Guidelines for IPv6 Multicast Addresses
- RFC 3513：Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3596：DNS Extensions to Support IP Version 6

38.2 Introduction to basic IPv6 configuration tasks

Configure basic functions of IPv6

Configure IPv6 Neighbour Discovery Protocol

Configure PMTU discovery

Configure ICMPv6 message sending

38.3 Configure basic functions of IPv6

38.3.1 Configure IPv6 unicast address

IPv6 global unicast addresses are obtained by manual assignment.

IPv6 link-local addresses are obtained in two ways:

- Automatic generation: when the VLAN port is UP, the device automatically generates a link local address for the interface according to the link local address prefix (FE80:/10) and the link layer address of the interface;
- Manual designation: The user manually configures the IPv6 link-local address.

Command	Description	CLI Mode
ipv6 address <ipv6-address>/<prefix-length>	Specify the IPv6 address manually. By default, link-local address are automatically generated unde layer 3 interfaces based on that MAC address of the VLAN interface.	Configuration Mode

38.4 Configure IPv6 Neighbour Discovery Protocol

38.4.1 Configure relevant parameters of RA message

The user can configure whether the interface sends the RA message and the time interval for sending the RA message according to the actual situation. At the same time, the user can configure the relevant parameters in the RA message to notify the host. When the host receives the RA message, it can use these parameters to operate accordingly. Parameters in configurable RA messages and their meanings are shown in Table 1-4.

Parameter	Description
Cur Hop Limit	When the host sends an IPv6 message, it will use this parameter value to fill the Hop Limit field in the IPv6 message header. At the same time, the parameter value is also used as the value of the Hop Limit field in the device response message
Prefix Information	After the host on the same link receives the prefix information i ssued by the device, it can perform operations such as stateless automatic configuration.
Managed address configura tion flag bit（M flag）	Used to determine whether a host acquires an IPv6 address using stateful autoconfiguration. If this bit is set to 1, the host will obtain an IPv6 address through stateful autoconfiguration (such as a DHCP server); otherwise, the host will obtain an IPv6 address through stateless autoconfiguration, which generates an IPv6 address based on its link-layer address and the prefix information published by the router
Other configuration flag bit （O flag）	Used to determine if a host uses stateful autoconfiguration to obtain information other than an IPv6 address. If the Other Configuration flag bit is set to 1, the host will obtain additional information other than the IPv6 address through stateful autoconfiguration (for example, DHCP server); otherwise, it will obtain additional information through stateless auto configuration.
Router Life time	Time used to set the router that issued the RA message as the default router for the host. The host can determine whether to take the router issuing the RA message as the default router according to the router lifetime parameter value in the received RA message.
Retrans Timer	After the device sends the NS message, it resends the NS message if it does not receive a response within the specified time interval.
Reachable Time	After the neighbour reachability detection confirms that the neighbour is reachable, the device considers that the neighbour is reachable within the set reachability time; after the set reachability time is exceeded, if a message needs to be sent to the neighbour, the device will reconfirm whether the neighbour is reachable.
Link MTU	The MTU option is used in the RA message to ensure that all n odes on the link use the same MTU value, primarily when the n odes may not know the MTU of the link. Other Neighbour Discovery messages must be silent. Ignore this option.

Configure hop count limit

Command：ipv6 nd cur-hop-limit value

View Mode: VLAN Interface Mode

Default configuration: By default, the router is limited to 64 hop

Unsuppress RA Message Posting

Command：ipv6 nd send-ra

View Mode: VLAN Interface Mode

Default configuration: By default, RA messages are suppressed from being published

Configure the maximum time interval and minimum time interval for RA message publishing

Command：ipv6 nd max-ra-interval value

View Mode: VLAN Interface Mode

Default configuration: By default, the maximum interval for RA message publishing is 600 second

Command：ipv6 nd min-ra-interval value

View Mode: VLAN Interface Mode

Default configuration: By default, the minimum time interval for RA message publishing is 198 seconds

Notice:

- When the RA message is issued periodically, the interval between two adjacent times is the interval between the maximum time interval and the minimum time interval, and a value is randomly selected between the maximum time interval and the minimum time interval as the interval for issuing the RA message periodically.
- The configured minimum time interval shall be less than or equal to 0.75 times of the maximum time interval.

Configure prefix information in RA message

Command：ipv6 nd prefix X:X::X:X/M (valid-lifetime preferred-lifetime (off-link | no-autoconfig))

View Mode: VLAN Interface Mode

Default configuration: By default, the prefix information in the RA message is not configured. At this time, the IPv6 address of the interface that sends the RA message is used as the prefix information in the RA message.

Set the managed address configuration flag bit

Command：ipv6 nd managed-config-flag

View Mode: VLAN Interface Mode

Default configuration: By default, the managed address flag bit is 0, that is, the host obtains the IPv6 address through stateless autoconfiguration.

Set other configuration flag bit

Command：ipv6 nd other-config-flag

View Mode: VLAN Interface Mode

Default configuration: By default, the other configuration flag bit is 0, that is, the host obtains other information through stateless automatic configuration.

Configure the router lifetime in the RA message

Command：ipv6 nd ra-lifetime value

View Mode: VLAN Interface Mode

Default configuration: By default, the router lifetime in the RA message is 1800 seconds.

Configuring neighbour request message retransmission time interval

Command：ipv6 nd base retrans-timer value

View Mode: Configuration Mode

Default configuration: By default, the interface sends NS messages at an interval of 1000 milliseconds

Configure the retransmission interval of the router in the RA message

Command：ipv6 nd retrans-timer value

View Mode: VLAN Interface Mode

Default configuration: By default, the value of the Retrans Timer field in the RA message issued by the interface is 0

Configures the time to keep a neighbour reachable

Command：ipv6 nd base reachable-time value

View Mode: Configuration Mode

Default configuration: By default, the interface remains reachable for 30000 milliseconds.

Configures the time to keep a neighbour reachable

Command：ipv6 nd reachable-time value

View Mode: VLAN Interface Mode

Default configuration: By default, the value of the Reachable Timer field in the RA message published by the interface is 0.

Configure Link MTU Size

Command：ipv6 nd link-mtu value

View Mode: VLAN Interface Mode

Default configuration: By default, the value of the link MTU field in the RA message issued by the interface is 0.

When the source host sends a message from an interface, it will compare the MTU of the interface with the Link MTU. If the length of the message is greater than the minimum value of the two, the minimum value will be used to fragment the message.

38.4.2 The number of times a Neighbour Solicition message is sent when duplicate address detection is configured

After obtaining the IPv6 address, the interface will send a neighbour solicitation message for duplicate address detection. If no response is received within the specified time (configured by the IPv6 nd retrans-timer command), the interface will continue to send the neighbour solicitation message. If no response is received after the number of times of sending reaches the set number, the address is considered to be available.

.

Command	Description	CLI Mode
ipv6 nd dad attempts <value>	By default, the number of times of sending neighbor solicitation messages during duplicate address detection is 1. When the value is 0, duplicate address detection is prohibited	Configuration Mode

38.5 IPv6 Static Route Configuration

Command	Description	CLI Mode
ipv6 route <X:X::X:X/M> (<X:X::X:X> | <ifName>) <distance>	Configure IPv6 Static Routine	Configuration Mode

38.6 IPv6 display and maintenance

After the above configuration is completed, execute the show command in the privileged view to display the operation of IPv6 after configuration, and verify the effect of configuration by viewing the display information.

Command	Description	CLI Mode
show ipv6 ndp nc	Show Neighbor Information	Privileged Mode
show ipv6 interface (<ifName>) brief	Displays IPv6 information for interfaces that can be configured with IPv6 addresses	Privileged Mode
show ipv6 route (database)	Displaying IPv6 Route	Privileged Mode

39 MLD SNOOPING Configuration

In man/Internet, when the same data packet is sent to multiple receivers in the network by unicast, the number of packets to be sent will increase linearly with the increase of the number of receivers due to the need to copy the packet to each receiving endpoint, which will increase the overall burden of the host, switching routing equipment and network bandwidth resources. Efficiency is greatly affected. With the increasing demand of multipoint video conference, video on demand and group communication applications, multicast has increasingly become a popular transmission mode in multipoint communication in order to improve resource utilization.

The switch implements the MLD SNOOPING function to serve multicast applications. MLD SNOOPING monitors the MLD packets on the network to realize the dynamic learning of IPV6 multicast MAC address.

This chapter describes the concept and configuration of MLD SNOOPING, mainly including the following contents:

- Introduction to MLD SNOOPING
- MLD SNOOPING configuration
- SNOOPING Configuration Example

39.1 Introduction to MLD SNOOPING

In the traditional network, multicast packets are treated as broadcast in a subnet, which is easy to cause network traffic and network congestion. When MLD SNOOPING is implemented on the switch, MLD SNOOPING can dynamically learn the IPV6 multicast MAC address and maintain the output port list of the IPV6 multicast MAC address, so that the multicast data stream is only sent to the output port, which can reduce the network traffic.

This section mainly includes the following contents:

- MLD SNOOPING process
- Layer-2 dynamic multicast
- Join a group
- Leave a group

39.1.1 MLD SNOOPING process

MLD SNOOPING is a Layer 2 network protocol that monitors MLD protocol packets passing through the switch, maintains a multicast group according to the receiving port, VLAN ID, and multicast address of these MLD protocol packets, and then forwards these MLD protocol packets. Only the ports joined in the multicast group can receive the multicast data stream, thus reducing the network traffic and saving the network bandwidth.

The multicast group includes the multicast group address, member port, VLAN ID, and Age time.

The formation of MLD SNOOPING multicast group is a learning process. When a port of the switch receives an MLD REPORT packet, MLD SNOOPING generates a new multicast group, and the port receiving the MLD REPORT packet is added to the multicast group. When the switch receives an MLD QUERY packet, if the multicast group already exists in the switch, the port that received the MLD QUERY also joins the multicast group. Otherwise, just forward the MLD QUERY packet. MLD SNOOPING also supports the Done mechanism of MLD V2. If fast-leave is configured as ENABLE for MLD SNOOPING, its receiving port can immediately leave the multicast group when receiving the Done packet of MLD V2; If the fast-leave-timeout is configured, the multicast group waits for this time to expire before leaving the multicast group.

MLD SNOOPING has two update mechanisms. One is the Done mechanism described above. In most cases, MLD SNOOPING uses age time to delete expired multicast groups. When a multicast group joins the MLD SNOOPING, the joining time is recorded. When the multicast group remains in the switch for more than a configured age time, the switch will delete the multicast group.

When a port receives a Done protocol packet, the port will be immediately deleted from the multicast group to which it belongs, which may affect the continuity of network data streams, because a HUB or a network device without MLD SNOOPING function may be connected to the port, and many devices receiving multicast data streams are connected to the device. When one device sends Done, it may affect other devices to receive the multicast data stream. The Fast-leave-timeout mechanism can prevent this from happening. A leave-waiting time is configured through the Fast-leave-timeout mechanism. After receiving the leave packet, the port waits for the Fast-leave-timeout long time before deleting it from the multicast group to which it belongs. It is possible to guarantee the continuity of the network multicast stream.

39.1.2 Layer-2 dynamic multicast

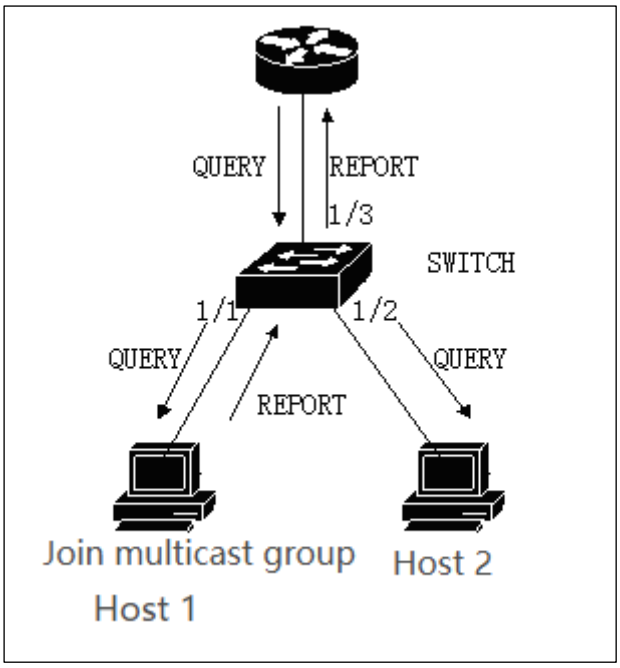
The multicast MAC address entries in the layer 2 hardware multicast forwarding table can be learned dynamically by MLD SNOOPING. The IPV6 multicast MAC address is learned dynamically through MLD SNOOPING.

When the switch closes the MLD SNOOPING, the layer 2 hardware multicast forwarding table is in the unregistered forwarding mode, the multicast MAC address cannot be dynamically learned, there is no entry in the layer 2 hardware multicast forwarding table, and all layer 2 multicast data streams are treated as broadcasts.

When the network has a multicast environment, in order to effectively control the multicast traffic of the network, the switch can open the MLD SNOOPING, at this time, the layer 2 hardware multicast forwarding table is in the register forwarding mode, and the switch can learn the multicast MAC address by monitoring the MLD protocol packet on the network. Only the layer 2 multicast flows matching the entries in the layer 2 hardware multicast forwarding table can be forwarded.

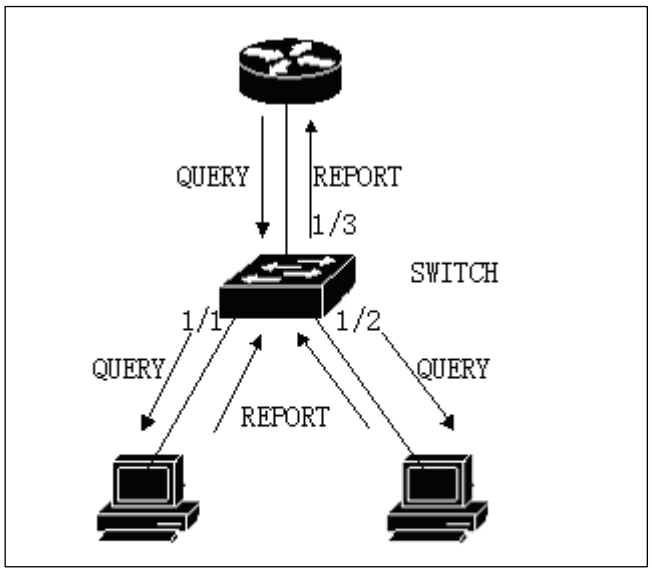
39.1.3 Join a group

When a host wants to join a multicast group, the host sends an MLD REPORT packet that specifies the multicast group the host wants to join. When the switch receives an MLD QUERY packet, the switch will forward the packet to all other ports in the same VLAN. When the host under the port that wants to join the multicast group receives the MLD QUERY packet, it will return an MLD REPORT packet. When the switch receives an MLD REPORT packet, a layer 2 multicast entry is created, and the port that receives the MLD QUERY packet and the port that receives the MLD REPORT packet are added to the layer 2 multicast entry and become its output ports.



As shown in the figure above, all the devices are in a subnet, and the VLAN of the subnet is assumed to be 2. The router runs the MLDv2 protocol and sends MLD QUERY packets periodically. Host 1 wants to join the multicast group ff15: 1. When the switch receives the MLD QUERY packet from port 1/3, it records the port and forwards the packet to ports 1/1 and 1/2. Host 1 sends back an MLD REPORT packet after receiving the MLD QUERY packet, and host 2 does not send the MLD REPORT packet because it does not want to join the multicast group. When the switch receives the MLD REPORT packet on port 1/1, it forwards the packet out query port 1/3 and creates a Layer 2 multicast entry (assuming the entry does not exist) that includes the following:

Layer 2 multicast addr	VLAN ID	List of output ports
33:33:00:00:00:01	2	1/1， 1/3



The condition in the above figure is the same as that in Figure 1. Host 1 has joined the multicast group ff15: 1, and now host 2 wants to join the multicast group ff15: 1. When host 2 receives the MLD query packet and returns an MLD REPORT packet, the switch will forward the packet from query port 1/3 after receiving the MLD REPORT from port 1/2, and add the packet port 1/2 to the layer 2 multicast entry. The layer 2 multicast entry becomes:

Layer 2 multicast addr	VLAN ID	List of output ports
33:33:5e:00:00:01	2	1/1，1/2，1/3

39.1.4 Leave a group

In order to form a stable multicast environment, a device running MLD (such as a router) will send an MLD QUERY packet to all hosts at regular intervals. The host that has joined the multicast group or wants to join the multicast group receives the MLD QUERY and sends back an MLD REPORT.

If a host wants to leave a multicast group, there are two ways: active departure and passive departure. Active leave means that the host sends an MLD leave packet to the router, and passive leave means that the host does not return the MLD REPORT after receiving the MLD QUERY from the router.

Corresponding to the way the host leaves the multicast group, there are two ways for the port on the switch to leave the layer 2 multicast entry: timeout leaving and receiving MLD done packet leaving.

When the switch does not receive an MLD report packet of a multicast group from a port for a certain time, the port is removed from the corresponding layer 2 multicast entry, and if the layer 2 multicast entry has no port, the layer 2 multicast entry is deleted.

When the fast-leave configuration of the switch is ENABLE, if a port receives an MLD LEAVE packet of a multicast group, the port is removed from the corresponding layer 2 multicast entry. If the layer 2 multicast entry has no port, the layer 2 multicast entry is deleted.

Fast-leave is generally used when a port is connected to a host. If there is more than one host under a port, the fast-leave-timeout waiting time can be configured to ensure the continuity and reliability of the multicast stream in the network.

39.2 MLD SNOOPING configuration

39.2.1 MLD SNOOPING default configuration

MLD SNOOPING is off by default, and the Layer 2 hardware multicast forwarding table is in unregistered forwarding mode.

Fast-leave is off by default.

Fast-leave-timeout is 300 seconds.

The default age time of the multicast group REPORT port is 400 seconds.

The default age time of the multicast group QUERY port is 300 seconds.

39.2.2 Opening and closing MLD SNOOPING

The MLD SNOOPING protocol can be turned on globally or individually for some VLANs; only when the MLD SNOOPING is turned on globally, can the MLD SNOOPING of a VLAN be turned on or off.

Open global MLD SNOOPING

Switch#configure terminal

Switch(config)#ipv6 mld snooping

Open MLD SNOOPING for a VLAN

Switch#configure terminal

Switch(config)#ipv6 mld snooping vlan <vlan-id>

Turn off global MLD SNOOPING

Switch#configure terminal

Switch(config)#no ipv6 mld snooping

Turn off MLD SNOOPING for one VLAN

Switch#configure terminal

Switch(config)#no ipv6 mld snooping vlan <vlan-id>

39.2.3 Configuration Lifetime

Configure the lifetime of a multicast group

Switch#configure terminal

Switch(config)#ipv6 mld snooping group-membership-timeout <interval> vlan <vlan-id>

Interval is in milliseconds.

Configuring the Lifetime of a Query Group

Switch#configure terminal

Switch(config)#ipv6 mld snooping query-membership-timeout <interval> vlan <vlan-id>

Interval is in milliseconds.

39.2.4 Configuring fast-leave

Start fast-leave for one VLAN

Switch#configure terminal

Switch(config)#ipv6 mld snooping fast-leave vlan <vlan-id>

Close fast-leave

Switch#configure terminal

Switch(config)#no ipv6 mld snooping fast-leave vlan <vlan-id>

Configure the fast-leave wait times

Switch#configure terminal

Switch(config)# ipv6 mld snooping fast-leave-timeout <interval> vlan <vlan-id>

Restore default fast-leave wait times

Switch#configure terminal

Switch(config)#no ipv6 mld snooping fast-leave-timeout vlan <vlan-id>

39.2.5 Configure MROUTER

Configure a static query port

Switch#configure terminal

Switch#interface ge1/6

Switch(config-ge1/6)#ipv6 mld snooping mrouter vlan [vlan-id]

39.2.6 Configure the startup VLAN querier

Configure to enable the querier feature for VLAN 1

Switch#configure terminal

Switch(config)#ipv6 mld snooping querier vlan 1

39.2.7 Display Information

Display MLD SNOOPING configuration information
Switch#show ipv6 mld snooping

Displays configuration information for a VLAN
Switch#show ipv6 mld snooping vlan <vlan-id>

Displays aging information for a report multicast group
Switch#show ipv6 mld snooping age-table group-membership

Display aging information for QUERY
Switch#show ipv6 mld snooping age-table query-membership

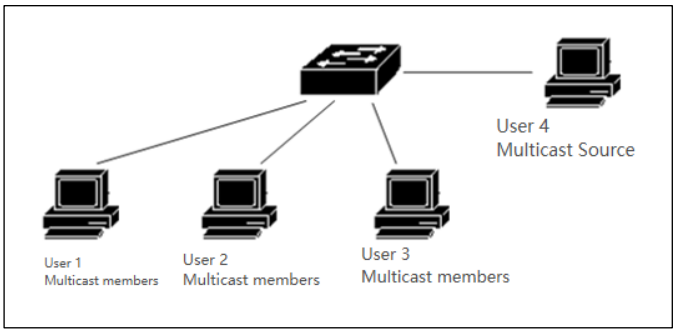
Displays forwarding information for a multicast group
Switch#show ipv6 mld snooping forwarding-table

Display MROUTER information
Switch#show ipv6 mld snooping mrouter

Displays the current configuration of the system, including the MLD SNOOPING configuration
Switch#show running-config

39.3 MLD SNOOPING Configuration Example

Enable the MLD SNOOPING function on the switch. User 1, User 2, and User 3 can join a specific multicast group.



Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 200

Switch(config)#ipv6 mld snooping

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 200

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 200

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode access

Switch(config-ge1/3)#switchport access vlan 200

Switch(config)#ipv6 mld snooping group-membership-timeout 60000 vlan 200

40. PoE Configuration

The switch supports the POE function, mainly including the following contents:

- Introduction to POE
- Configure POE

40.1 Introduction to POE

PoE (Power over Ethernet, also known as remote power supply) refers to the remote power supply of a device through an Ethernet interface by using a twisted pair to connect an external PD (Powered Device) device (such as an IP phone, a wireless AP, a network camera, etc.).

（1） Benefits of PoE

- Reliable: centralized power supply, convenient backup
- that connection is simple and convenient: the network terminal doe not need an external pow supply and only needs one network cable.
- Standard: It conforms to IEEE 802.3 AF and 802.3 at standards, and uses the global unified power interface.
- Wide application prospect: it can be used for IP phone, wireless AP (Access Point), portable device charger, card reader, network camera, data acquisition, etc.

（2）**POE system composition**

- PoE system includes PoE power supply, PSE and PD.
- PoE power supply
- The PoE power supply supplies power to the whole PoE system, which is divided into two types: external power supply and built-in power supply.
- PSE
- PSE (Power Sourcing Equipment, Power Supply Equipment) is the board (daughter card). Each PSE independently manages the PoE interface in the board (daughter card). The PSE finds, detects, classifies, and supplies power to the PD on the line of the PoE interface. When the PD is detected to be unplugged, the PSE stops supplying power. Ethernet interfaces with PoE power supply are called PoE interfaces, including FE and GE.
- PD
- An PD is a device that receives power from the PSE. The standard PD is a PD device conforming to the IEEE 802.3 AF and the 802.3 at standards. While receiving the PoE power supply, the PD device is allowed to be connected to other power supplies for power redundancy backup.

40.2 Configure POE

The POE configuration consists of the following three parts:

- Manual POE configuration
- POE policy configuration
- PD query configuration

40.2.1 Manual POE configuration

The commands for manual POE configuration are as follows:

- Turn on or off the POE power supply of the interface.
- Display POE information

Command	Description	CLI Mode
[no] poe enable	Turn on or off the POE power supply of the interface, and the power supply state of the interface is on by default.	Interface Configuration Mode
show poe	Displays POE information for all interfaces.	User mode or privileged user model

40.2.2 POE policy configuration

Commands for POE policy configuration are as follows:

- Open or close the POE policy of the interface
- Set the POE policy entry of the interface
- Display POE policy information

Command	Description	CLI Mode
[no] poe policy enable	Turn the interface POE policy on or off. The default interface POE policy is off.	Interface Configuration Mode
[no] poe policy shutdown clock <clock-value> week-day <day-value>	Sets or removes a POE policy entry for an interface. This command can be set multiple times. By default, no POE policy entry is set. Clock-value is the time or time range in 24-hour format. If the value is 1, it means 1 o'clock (between 1 o'clock and 2 o'clock). If the value is 20-23, it means 20 o'clock to 23 o'clock (between 20 o'clock and 0 o'clock). Day-value is the day of the week, indicating a certain day or a certain number of consecutive days, such as 3 for Wednesday, 1-7 for Monday to Sunday. A POE policy can take effect only if the interface's POE policy is turned on.	Interface Configuration Mode
show poe policy <if-name>	Displays POE policy information for an interface	User mode or privileged user mode

40.2.3 PD query configuration

The command for the PD query configuration is as follows:

- Set the IP address of PD
- Set the time interval for querying PD
- Set the timeout times for querying PD
- Set the start time of PD
- Display PD information

Command	Description	CLI Mode
poe pd-ip-address <ip-address> no poe pd-ip-address	Sets or clears the IP address of the PD to which the interface is connected. By default, the IP address of the PD is not configured. If the IP address of the PD is configured, the system will query the IP address periodically. If the PD does not respond for a given number of times, the system will restart the PD through the POE control.	Interface Configuration Mode
poe pd-query-interval <interval> no poe pd-query-interval	Set the PD query interval. The default PD query interval is 5 seconds.	Interface Configuration Mode
poe pd-timeout-number <number> no poe pd-timeout-number	Set the timeout times of PD query. The default timeout times of PD query is 3.	Interface Configuration Mode
poe pd-boot-time <time> no poe pd-boot-time	Set the startup time of PD. The default startup time of PD is 120 seconds.	Interface Configuration Mode
show poe pd-information	Displays information for all configured PDs	User mode or privileged user model

41. GVRP Configuration

This chapter covers the following：

- Introduction to GVRP
- Configure GVRP
- Display GVRP

41.1 Introduction to GVRP

GVRP is defined in the IEEE 802.1P standard and allows control of 802.1Q VLANs.

GVRP switches can exchange VLAN configuration information with each other, trim unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected over 802.1Q trunks.

GVRP uses GID and GIP, which provide a description of the general state mechanism and a common information propagation mechanism for GARP-based applications, respectively. GVRP only runs on 802.1Q trunk links. GVRP cuts out the trunk link so that only the active VLAN is transmitted on the trunk connection. Before GVRP can add a VLAN to the trunk, it first receives a join message from the switch. GVRP update information and timers can be changed. GVRP ports have several modes of operation, controlling how they trim VLANs. GVRP has the ability to dynamically add and manage VLANs for the VLAN database.

In other words, GVRP supports the propagation of VLAN information between devices. In GVRP, you can manually configure the VLAN information for one switch, and all other switches in the network can dynamically learn about those VLANs. The endpoint can plug into any switch and connect to the desired VLAN. In order for a terminal to use GVRP, a GVRP-compliant Network Interface Card (NIC) needs to be installed. GVRP-compliant NICs can be configured to join to the desired VLAN and then plugged into a GVRP-enabled switch. A communication connection is established between the NIC and the switch, and VLAN connectivity is implemented between the two.

41.2 Configure GVRP

The main configurations of GVRP include:

- Enable GVRP
- Check out GVRP

In a configuration task, you must enable global GVRP before you can enable port GVRP.

41.2.1 Enable GVRP settings

command	Description	Configuration mode
set gvrp enable | disable	Enable/de-enable all VLAN GVRPs globally	Global configuration mode
set gvrp applicant state active |normal	Enable the global GVRP applicant status	Global configuration mode
set gvrp dynamic-vlan-creation enable | disable	Enable/de-enable global dynamic VLANs	Global configuration mode
Set gvrp registration{fixed | forbidden | normal} <if-name>	Configure the multicast mode for API registration	Global configuration mode
set gvrp timer {join | leave | nleaveall} <time-value>	Configure the time of various timers	Global configuration mode
set port gvrp enable <if-name>	Enable GVRP on the port	Global configuration mode
set port gvrp disable <if-name>	Go to enable the GVRP function on the port	Global configuration mode

41.2.2 View GVRP information

After the preceding configuration is completed, run the show command in privileged mode to display the running status of GVRP after configuration, and verify the effect of the configuration by viewing the display information.

Command	Description	Configuration mode
show gvrp configuration	View GVRP configurations	Privileged mode
show gvrp machine	View the GVRP state machine information	Privileged mode
show gvrp statistics vlanid	View the GVRP statistics of a specific VLANID	Privileged mode
show gvrp timer <ifname>	View the timer information for a specific port	Privileged mode

This Page Left Blank Intentionally

This Page Left Blank Intentionally

Case Communications

www.casecomms.com