

Switch Product Operation Manual

Version：V1.2

Release Date : 20220422

Content

Chapter 1 Access Switch 1
1.1 CLI 1
1.1.1 Command Syntax 2
1.1.2 Help of Command Line 3
1.1.3 Display history Command of Command Line 4
1.2 Manage Users 4
1.2.1 System Default User 5
1.2.2 Add User 5
1.2.3 Change Password 6
1.2.4 Modify User's Privilege Level 7
1.2.5 Delete User 7
1.2.6 Display Users 8
1.2.7 Display Users 8
1.2.8 Kick off Online Telnet Users 8
1.3 Remote Authentication Configure 9
1.3.1 Enable RADIUS/TACACS+ 9
1.3.2 Display Authentication Method 9
1.3.3 TACACS+ Remote Server Configuration 9
1.3.4 Dsiplay TACACS+ Information 10

Chapter 2 System Management 11
2.1 System Maintenance 11
2.1.1 Display System Status Information 11
2.1.2 Configure the System Clock 11
2.1.3 Configure System Host Name 12
2.1.4 Trace Route Command 12
2.1.5 Port Loopback Test Command 13
2.1.6 Line Detection VCT Command 14
2.1.7 Management IP Address Configuration 15
2.1.8 Telnet User Limit for Login Privileged User View 16
2.1.9 CPU-CAR Command 17
2.2 Configuration Management 19
2.2.1 Save Configurations 19
2.2.2 Erase Configurations 19
2.2.3 Execute save Configuration 19
2.2.4 Show save Configurations 20
2.2.5 Show Running Configurations 20
2.3 Load Files and Upgrade Programs Online 21
2.3.1 Upload and Download Files by TFTP 21
2.3.2 Upload and Download Files by FTP 22
2.3.3 Download Files by Xmodem 23
2.4 Reboot Switch 24
Chapter 3 Port Configuration 25
3.1 Ethernet Port Configuration Overview 25
3.2 Configure Ethernet Port 25
3.2.1 Enter Interface Configuration Mode 25
3.2.2 Enter Interface Range Mode 25
3.2.3 Basic Port Configuration 26
3.2.4 Link Type of Ethernet Ports 27

3.2.5 Configure Default VLAN 28
3.2.6 Add Port to a Vlan 28
3.2.7 Dsiplay Port Information 29
3.2.8 Display and Clear Port Statistics 30
Chapter 4 Port Mirroring 31
4.1 Port Mirroring Overview 31
4.2 Configure Port Mirroring 31
4.2.1 Configure Port Mirroring 31
4.2.2 Configure the Mirror Destination Port 32
4.2.3 Configure the Mirror Source Port 32
4.2.4 Display Port Mirroring 33
Chapter 5 Link Aggregation 34
5.1 Link Aggregation Overview 34
5.1.1 Introduction to LACP 35
5.1.2 Operation Key (O-Key) 35
5.1.3 Static Aggregation Group 36
5.1.4 Dynamic LACP Aggregation Group 37
5.2 Redundancy of Interconnected Device 40
5.3 Load-balancing Policy 40
5.4 Configure Link Aggregation 40
5.4.1 Link AggregationConfiguration List 40
5.4.2 Configure a Static Aggregation Group 41
5.4.3 Configure Dynamic LACP 42
5.4.4 Display and Maintain LACP 43
Chapter 6 Port Isolation 45
6.1 PortIsolation Overview 45
6.2 Configure Port Isolation 45
6.2.1 Add/remove Isolated Ports 45
6.2.2 Display Port Isolation Configuration 46

Chapter 7 Storm-Control 47
7.1 Storm-Control Overview 47
7.2 Configure Storm-Control 47
7.2.1 Configure Storm-Control 47
7.2.2 Storm-Control Monitor and Maintenance 48
Chapter 8 VLAN 49
8.1 VLAN Overview 49
8.1.1 VLAN Principles 50
8.2 Configure 802.1Q VLAN 52
8.2.1 802.1Q VLAN Configuration List 52
8.2.2 Create and Modify VLAN 52
8.2.3 Delete Port Members from a VLAN 53
8.2.4 Delete VLAN 54
8.2.1 Configure Interface Default VLAN ID 54
8.2.2 Configure Interface VLAN Mode 55
8.2.3 VLAN Attributes Based on Hybrid Interface 56
8.2.4 VLAN Attributes Based on Trunk Interface 57
8.2.5 Configure Port Priority 58
8.2.6 Configure Ingress Filtering 58
8.2.7 Configure Types of Interface Acceptable-frame 59
8.2.8 Display VLANconfiguration 60
8.3 Configure MAC-Based VLAN 60
8.3.1 MAC-Based VLAN Overview 60
8.3.2 ConfigureMAC-Based VLAN 61
8.4 Configure Protocol-Based VLAN 61
8.4.1 Protocol-Based VLAN Overview 61
8.4.2 ConfigureProtocol-Based VLAN 62
8.5 Configure IP-subnet VLAN 63
8.5.1 IP-subnet VLAN Overview 63

8.5.2 ConfigureIP-subnet VLAN 63
Chapter 9 QinQ 65
9.1 QinQ Overview 65
9.1.1 Understanding QinQ 65
9.1.2 Implementations of QinQ 66
9.1.3 Modification of TPID Value of QinQ Frames 67
9.2 Configure QinQ 68
9.2.1 QinQ Configuration Task List 69
9.2.1 Configure BASIC QinQ 69
9.2.2 Configure Flexible QinQ 69
9.2.3 Display QinQ configuration 70
Chapter 10 MAC Address Table 71
10.1 MAC Address Table Overview 71
10.2 Configure MAC Address Table 71
10.2.1 MAC Address Table Configuration Task List 72
10.2.2 Configure the Aging Time 72
10.2.3 Add MAC Address Table by Manual 72
10.2.4 Display MAC Address Table 73
10.2.5 Enable/Disable MAC Learning 74
10.2.6 Quantity Limitation on MAC Address Learning Table 75
Chapter 11 STP 76
11.1 STP Overview 76
11.1.1 Protocol Packets of Spanning-Tree 76
11.1.2 Basic Concepts in Spanning-Tree 76
11.1.3 Spanning-Tree Interface States 78
11.2 How Spanning-Tree Works 80
11.3 Implement RSTP on Ethernet Switch 84
11.4 Configure RSTP 85
11.4.1 RSTP Configuration Task List 85

11.4.2 Enable RSTP and Configure the Working Mode 86
11.4.3 Configure STP Bridge Priority 86
11.4.4 Configure Time Parameter 87
11.4.5 Configure STP Path Cost 88
11.4.6 Configure STP Port Priority 88
11.4.7 Configure STP Mcheck 89
11.4.8 Configure STP Point-to-Point Mode 89
11.4.9 Configure STP Portfast 90
11.4.10 Configure STP Transit Limit 90
11.4.11 RSTP Monitor and Maintenance 90
Chapter 12 MSTP 92
12.1 MSTP Overview 92
12.2 Configure MSTP 92
12.2.1 Enable MSTP and Configure the Working Mode 92
12.2.2 Configure MSTP Timer Parameter Values 93
12.2.3 Configure MSTP Identifier 94
12.2.4 Configure MSTP Bridge Priority 94
12.2.5 ConfiConfigure Root Port Protection 95
12.2.6 Configure Digest Snooping Port 95
12.2.7 Configure Port mCheck Function 96
12.2.8 Configure MSTP Instance Is Enabled 97
12.2.9 Display and Maintain MSTP 97
Chapter 13 Remote-loop-detect 98
13.1 Remote-loop-detect Overview 98
13.2 Configure Remote-loop-detect 98
13.2.1 Enable Remote-loop-detect 98
13.2.2 Configure the Processing Policy 99
13.2.3 Configure the Interval Timer 99
13.2.4 Configure the Recovery Timer 100

13.2.5 Display Remote-loop-detect Configuration 100
Chapter 14 ACL 101
14.1 ACL Overview 101
14.1.1 ACL Overview 101
14.2 ACL Configuration 102
14.2.1 ACL Configuration List 102
14.2.2 Configure Match Order 102
14.2.3 Configure Time Range 104
14.2.4 Configure Basic ACL 106
14.2.5 Configure Extended ACL 108
14.2.1 Configure Layer 2 ACL 111
14.2.2 Activate ACL 113
14.2.3 Display and Debugging ACL 114
Chapter 15 QOS 116
15.1 QOS Overview 116
15.1.1 Traffic 117
15.1.2 Traffic Classification 117
15.1.3 Priority 117
15.1.4 Access Control List 120
15.1.5 Packet Filtration 121
15.1.6 Flow Monitor 121
15.1.7 Interface Speed Limitation 121
15.1.8 Redirection 122
15.1.9 Priority Mark 122
15.1.10 Choose Interface Outputting Queue for Packet 122
15.1.11 Queue Scheduler 122
15.1.12 Cos-map Relationship of Hardware Priority Queue and Priority of IEEE802.1p Protocol 124
15.1.13 Flow Mirror 124

15.1.14 Statistics Based on Flow 124
15.1.15 Copy Packet to CPU 124
15.2 Configure QOS 125
15.2.1 QoS Configuration List 125
15.2.2 Configure Flow Monitor 126
15.2.3 ConfigureTwo Rate Three Color Marker 126
15.2.4 Configure Interface Line Rate 127
15.2.5 Configure Packet Redirection 127
15.2.6 Configure Traffic Copy to CPU 127
15.2.7 Configure Traffic Priority 128
15.2.8 Configure Queue-Scheduler 128
15.2.9 Configure Cos-map Relationship of Hardware Priority Queue and Priority of IEEE802.1p Protocol 129
15.2.10 Configure Mapping Relationship between DSCP and 8 Priority in IEEE 802.1p 130
15.2.11 Configure Flow Statistic 132
15.2.12 Configure Flow Mirror 132
15.2.13 Display and Maintain QoS 133
Chapter 16 SSH 135
16.1 SSH Overview 135
16.2 Configure SSH Server 135
16.3 Log in Switch from SSH Client 136
Chapter 17 SNMP 137
17.1 SNMP Overview 137
17.2 Configure SNMP-Agent 138
17.2.1 SNMP-Agent Configuration List 138
17.2.2 Configure the Basic Parameters 138
17.2.3 Configure the Community Name 140
17.2.4 Configure the Views 140

17.2.5 Configure the Group 141
17.2.6 Configure the User 142
17.2.7 Display SNMP-Agent Configuration 142
Chapter 18 Info-center 154
18.1 Info-center Overview 154
18.2 Configure Info-center 154
18.2.1 Info-center Configuration List 154
18.2.2 Enabling/Disabling the Info-center for the Equipment 155
18.2.3 Configure the Function of Display the Sequence Number in Info-center Outputs 156
18.2.4 Configure the Time Stamp Type in Info-center Outputs 157
18.2.5 Configure the Function of Outputting Info-center Information to Terminals 157
18.2.6 Configure the Function of Outputting Info-center Information to the History Buffer 159
18.2.7 Configure the Function of Outputting Info-center Information to the Flash Storage 160
18.2.8 Configure the Function of Outputting Info-center Information to the Log Host 162
18.2.9 Configure the Function of Outputting Info-center Information to the SNMP Agent 164
18.2.10 Configure the Module Debugging Function 165
Chapter 19 L3 Base Function 167
19.1 L3 Base Function Overview 167
19.2 Configure L3 Base Function 167
19.2.1 L3 Base Function Configuration List 167
19.2.2 Planning VLANs and Creating L3 Interfaces 168
19.2.3 Configure the Forwarding Mode 168
19.2.4 Creating VLAN Interfaces for Common VLANs 169
19.2.5 Creating SuperVLAN Interfaces and Adding VLANs to the

SuperVLAN 170
19.2.6 Configure IP Addresses for VLAN or SuperVLAN Interfaces171
19.2.7 Configure an IP Address Range for VLAN or SuperVLAN Interfaces 172
19.2.8 Configure the ARP Proxy 173
19.2.9 Display VLAN and SuperVLAN Interface Information 174
19.2.10 Configure URPF 175
19.2.11 Disabling the Function of Sending ICMP Packets with an Unreachable Destination Host on Interfaces 176
Chapter 20 ARP 177
20.1 ARP Overview 177
20.2 Configure ARP 177
20.2.1 ARP Configuration List 177
20.2.2 Add/Delete ARP 178
20.2.3 Bind dynamic Arp to Static 178
20.2.4 Display ARP Entry 178
20.2.5 Configure ARP Aging-time 178
Chapter 21 ARP Spoofing and Flood 180
21.1 ARP Spoofing and Flood Attack Overview 180
21.1.1 ARP against ARP Flood 182
21.2 Configure ARP Anti-Spoofing 183
21.2.1 ARP Anti-Spoofing Configuration List 183
21.2.2 Configure Anti-Spoofing 183
21.2.3 Configure ARP Packet Source MAC Address Consistency Check 184
21.2.4 Configure Anti-Gateway-Spoofing 184
21.3 Configure against ARP Flood 184
21.3.1 ARP against ARP Flood Configuration List 184
21.3.2 Configure against ARP Flood 185

21.3.3 Display and Maintain Against ARP Flood 185
Chapter 22 DHCP-Relay 186
22.1 DHCP-Relay Overview 186
22.2 Configure DHCP-Relay 187
22.2.1 DHCP-Relay Configuration List 187
22.2.2 Configure DHCP Server Group 188
22.2.3 Configure DHCP Relay to Support Option60 188
22.2.4 Enable the DHCP Relay Function 189
22.2.5 Configure DHCP Option82 190
Chapter 23 DHCP Snooping 193
23.1 DHCP Snooping Overview 193
23.2 Configure DHCP Snooping 194
23.2.1 DHCP Snooping Configuration List 194
23.2.2 Enable DHCP Snooping 194
23.2.3 Configure DHCP Snooping Trust port 195
23.2.4 Configure Max Clients Number 195
23.2.5 Configure Link-Down Operation 196
23.2.6 Configure IP-Source-Guard 197
23.2.7 DHCP Snooping Display and Maintenance 198
Chapter 24 DHCP-Server 199
24.1 DHCP-Server Overview 199
24.2 Configure DHCP-Server 199
24.2.1 DHCP-Server Configuration List 199
24.2.2 Configure IP Pool 200
24.2.3 Configure IP Pool Gateway 200
24.2.4 Configure IP Pool Range 201
24.2.5 Enable/Disable IP Address 201
24.2.6 Configure IP Pool Lease 201
24.2.7 Configure the DNS Server Address of DHCP Server 202

24.2.8 Configure the DHCP Server to Assign WINS Server Addresses 202
24.2.9 Display IP Pool Configuration 203
24.2.10 Configure Dhcp-client Bind 203
Chapter 25 IGMP Snooping 205
25.1 IGMP Snooping Overview 205
25.2 IGMP Snooping Configuration 205
25.2.1 IGMP Snooping Configuration List 205
25.2.2 Enable IGMP Snooping 206
25.2.3 Configure IGMP Snooping Timer 207
25.2.4 Configure IGMP-snooping Fast-leave 207
25.2.5 Configure Number of Multicast Group Allowed Learning 208
25.2.6 Configure IGMP Snooping Querier 208
25.2.7 Configure IGMP Snooping Multicast Learning Strategy 210
25.2.8 Configure IGMP Snooping Router-Port 210
25.2.9 Configure IGMP Snooping Port Multicast VLAN 211
25.2.10 Configure Host Port Record MAC Functions 211
25.2.11 Configure Port of Dropped Query Packets 212
25.2.12 Configure Port of Discarded Report Packets 212
25.2.13 Configure Multicast Preview 213
25.2.14 Configure Profile of Black and White List 213
25.2.15 Display and Maintenance of IGMP Snooping 214
Chapter 26 MLD Snooping 216
26.1 MLD Snooping Overview 216
26.2 MLD Snooping 216
26.2.1 MLD Snooping Configuration List 216
26.2.2 Start MLD Snooping 217
26.2.3 Configure MLD Snooping Timer 217
26.2.4 Configure Fast-leave Port 217

26.2.5 Maximum Number of Learning Multicast Configuration Port218
26.2.6 Configure MLD Snooping Multicast Learning Strategies 219
26.2.7 Configure MLD-Snooping querier 220
26.2.8 Configure Routing Port 221
26.2.9 Multicast VLAN Port Configuration 221
26.2.10 Display and Maintenance of MLD Snooping 222
Chapter 27 Static Multicast Table 223
27.1 Static Multicast Table Overview 223
27.2 Configure Static Multicast Table 223
27.2.1 Static Multicast GroupConfiguration List 223
27.2.2 Create a Static Multicast Group 223
27.2.3 Add a Port to the Multicast Group 224
27.2.4 Create a Static Multicast Group based on Group IP 224
27.2.5 Display and Maintenance of Static Multicast Table 225
Chapter 28 IGMP 226
28.1 IGMP Overview 226
28.2 Configure IGMP 226
28.2.1 IGMP Configuration List 227
28.2.2 Enable Multicast Routing Protocol 227
28.2.3 Enable IGMP Protocol 228
28.2.4 Configure IGMP Version 228
28.2.5 Configure IGMP General Query Interval 229
28.2.6 Configure Last-Member-Query-Interval 230
28.2.7 Configure Robustness Variable of IGMP Querier 230
28.2.8 Configure the Maximum Number of the Multicast Group Added to the Interface 231
28.2.9 Configure IGMP Maximum Query Response Time 232
28.2.10 Configure Multicast Group Filter Function 233
28.2.11 Establish Static IP Multicast Table 233

28.2.12 Configure Static Multicast Group 234
28.2.13 Configure IGMP Proxy 235
28.2.14 Configure IGMP SSM Mapping 236
28.2.15 Configure SSM-Mapping static group address mapping rule236
28.2.16 IGMP Display and Maintenance 237
Chapter 29 PIM 238
29.1 PIM Overview 238
29.1.1 Principles of PIM-DM 238
29.1.2 Principles of PIM-SM 241
29.1.3 Principles of PIM-SSM 242
29.2 Configure PIM 243
29.2.1 PIM Configuration List 243
29.2.2 Basic PIM Configuration 243
29.2.3 Advanced PIM Configuration 243
Chapter 30 SNTP 247
30.1 SNTP Overview 247
30.1.1 SNTP Operation Mechanism 247
30.2 Configure SNTP Client 248
30.2.1 SNTP Client Configuration List 248
30.2.2 Enable SNTP Client 248
30.2.3 Modifying SNTP Client Operating Mode 249
30.2.4 Configure SNTP Sever Address 249
30.2.5 Modifying Broadcast Transfer Delay 249
30.2.6 Configure Multicast TTL 250
30.2.7 Configure Interval Polling 250
30.2.8 Configure Overtime Retransmist 250
30.2.9 Configure Valid Servers 251
30.2.10 Configure MD5 Authentication 251
30.2.11 Display and Maintain SNTP Client 252

Chapter 31 802.1X 253
31.1 802.1X Overview 253
31.1.1 Architecture of 802.1X 253
31.1.2 Rule of 802.1x 255
31.2 Configure AAA 257
31.2.1 Configure RADIUS Server 258
31.2.2 Configure Local User 258
31.2.3 Configure Domain 259
31.2.4 Configure RADIUS Features 259
31.3 Configure 802.1X 261
31.3.1 Configure EAP 261
31.3.2 Enable 802.1x 262
31.3.3 Configure 802.1x Parameters for a Port 262
31.3.4 Configure Re-Authentication 263
31.3.5 Configure Watch Feature 263
31.3.6 Configure User Features 264
Chapter 32 LLDP 265
32.1 LLDP Overview 265
32.1.1 LLDP Fundamentals 265
32.1.2 LLDP Timer 265
32.2 Configure LLDP 266
32.2.1 LLDP Configuration List 266
32.2.2 Enable LLDP 266
32.2.3 ConfigureLLDP Hello-Time 266
32.2.4 ConfigureLLDP Hold-Time 267
32.2.5 ConfigureLLDP Packet Transferring and Receiving Mode on Port 267
32.2.6 Configure LLDP Management Address 268
32.2.7 LLDP Display and Debugging 268

Chapter 33 PPPoE Plus 269
33.1 PPPoE Plus Overview 269
33.2 ConfigurePPPoE Plus 269
33.2.1 PPPoE PlusConfiguration List 269
33.2.2 Enable PPPoE Plus 269
33.2.3 ConfigureOption Content 270
33.2.4 PPPoE Plus Monitor and Maintenance 271
Chapter 34 CFM 272
34.1 CFM Overview 272
34.1.1 CFM Concepts 272
34.1.2 CFM Main Function 273
34.2 Configure CFM 274
34.2.1 CFM Configuration List 275
34.2.2 Maintain Field Configuration 275
34.2.3 Configuration and Maintenance Level Domain Name 275
34.2.4 Configure Maintain Set 276
34.2.5 Configure Name and Associated VLAN to Maintain Set 277
34.2.6 Configure MEPs 277
34.2.7 Configure Remote Maintenance Endpoint 278
34.2.8 Configure MIPs 279
34.2.9 Configure Continuity Detection 279
34.2.10 Configure Loopback 280
34.2.11 ConfigureLink Tracking 281
34.2.12 Display and Maintenance of CFM 281
Chapter 35 EFM 283
35.1 EFM Overview 283
35.1.1 EFM Main Function 283
35.1.2 EFM Protocol Packets 285
35.2 Configure EFM 285

35.2.1 EFM Configuration List 285
35.2.2 EFM Basic Configuration 286
35.2.3 Configure EFM Timer Parameter 287
35.2.4 Configure Remote Failure Indication 288
35.2.5 Configure Link Monitoring Capabilities 288
35.2.6 Enabling Remote Loopback 290
35.2.7 Rejecting Remote Loopback Requests Initiated by Remote 290
35.2.8 Initiating a Remote Loopback Request 291
35.2.9 Starting Remote Access Function MIB Variable 291
35.2.10 MIB Variable Access Requests Initiated by Remote 292
35.2.11 Display and Maintenance of EFM 293
Chapter 36 ERRP 294
36.1 ERRP Overview 294
36.1.1 Concept Introduction 294
36.1.2 Protocol Message 298
36.1.3 Operate Principle 300
36.1.4 Multi-loop Intersection Processing 304
36.2 Configure ERRP 304
36.2.1 ERRP Configuration List 304
36.2.2 Enable/Disable ERRP 305
36.2.3 Configure Time Parameter 305
36.2.4 Configure Domain 306
36.2.5 Configure Work Mode 306
36.2.6 Configure Control VLAN 307
36.2.7 Configure the Ring 308
36.2.8 Enable/Disable ERRP Ring 309
36.2.9 Configure the Query Solicit Function 309
36.2.10 Configure the Topology Discovery Function 310
36.2.11 Display and Maintenance of ERRP 311

Chapter 37 ERPS 312
37.1 ERPS Overview 312
37.1.1 ERPS Basic Conception 312
37.1.2 ERPS Ring Protection Mechanism 315
37.2 Configure ERPS 317
37.2.1 ERPS Configuration List 317
37.2.2 Enable/Disable ERPS 317
37.2.3 Configure ERPS Instance 318
37.2.4 Configure Connectivity Detection of ERRP Link 319
37.2.5 Configure ERPS Related Timers 319
37.2.6 ERPS Display and Maintenance 320
Chapter 38 FlexLink 321
38.1 FlexLink Overview 321
38.1.1 Basic Concept of Flex Links 321
38.1.2 Operating Mechanism of Flex Link 322
38.2 Configure FlexLinks 325
38.2.1 FlexLinks Configuration List 325
38.2.2 Configure FlexLinks group 326
38.2.3 Configure FlexLinks Preemption Mode 326
38.2.4 Configure FlexLinks Preemption Delay 327
38.2.5 Configure FlexLinks MMU 328
38.2.6 FLexLinks Monitor and Maintenance 328
Chapter 39 Monitorlink 329
39.1 Monitorlink Overview 329
39.1.1 Monitor Link Group 329
39.1.2 Monitor Link Mechanism 331
39.2 Configure Monitor Link 333
39.2.1 MonitorLink Configuration List 333
39.2.2 Configure MonitorLink Group 333

39.2.3 MonitorLink Monitor and Maintenance 334
Chapter 40 L3 Base Function Configuration 335
40.1 L3 Base Function Overview 335
40.2 ConfigureL3 Base Function 335
40.2.1 L3 Base Function Configuration List 335
40.2.2 Planning VLANs and Creating L3 Interfaces 336
40.2.3 Configure the Forwarding Mode 336
40.2.4 Creating VLAN Interfaces for Common VLANs 337
40.2.5 Creating SuperVLAN Interfaces and Adding VLANs to the SuperVLAN 338
40.2.6 Configure IP Addresses for VLAN or SuperVLAN Interfaces 339
40.2.7 Configure an IP Address Range for VLAN or SuperVLAN Interfaces 340
40.2.8 Configure the ARP Proxy 341
40.2.9 Display VLAN and SuperVLAN Interface Information 342
40.2.10 Configure URPF 343
40.2.11 Disabling the Function of Sending ICMP Packets with an Unreachable Destination Host on Interfaces 344
Chapter 41 Static Route Configuration 345
41.1 Static Route Overview 345
41.2 Configure Static Route 345
41.2.1 Static Route Configuration List 345
41.2.2 Adding/Deleting a Static Route 345
41.2.3 Display Routing Entries 346
Chapter 42 RIP 349
42.1 RIP Overview 349
42.2 Configure RIP 351
42.2.1 RIP Configuration List 351
42.2.2 Enabling RIP 352

42.2.3 Specifying the IP Network Segment to Run RIP 352
42.2.4 Configurethe Passive interface 353
42.2.5 Specifying the RIP Version for an Interface 353
42.2.6 Configure Default Metric Value 355
42.2.7 Enabling the Route Aggregation Function 355
42.2.8 Configure RIP Packet Authentication 356
42.2.9 Configure Split Horizon 356
42.2.10 Setting an Additional Routing Metric 357
42.2.11 Defining a Prefix List 358
42.2.12 Configure Route Redistribution 359
42.2.13 Configure Route Filtering 360
42.2.14 Display RIP Configuration 361
Chapter 43 OSPF 363
43.1 OSPF Overview 363
43.2 Configure OSPF 365
43.2.1 OSPF Configuration List 365
43.2.2 Enable OSPF 365
43.2.3 Configure OSPF Parameter 365
43.2.4 Configure OSPF Interface 366
43.2.5 Configure OSPF Area 371
Chapter 44 BGP 375
44.1 BGP Overview 375
44.2 Configure BGP 378
44.2.1 BGP Configuration List 378
44.2.2 Enable BGP 378
44.2.3 Configure BGP Peers 379
44.2.4 Configure BGP Parameters 381
44.2.5 Monitoring and Maintain BGP 383
Chapter 45 BFD 384

45.1 BFD Overview 384
45.2 Configure BFD 384
45.2.1 BFD Configuration List 384
45.2.2 Enable BFD 384
45.2.3 Configure BFD Parameters and Mode 385
45.2.4 Display and Maintain BFD Configurations 387
Chapter 46 VRRP 388
46.1 VRRP Overview 388
46.2 Configure VRRP 389
46.2.1 VRRP Configuration List 389
46.2.2 Enable VRRP 389
46.2.3 Configure VRRP Parameters 390
46.2.4 Displays and Maintain VRRP Configurations 393
Chapter 47 DLF-Control 394
47.1 DLF-Control Overview 394
47.2 Configure DLF-Control 394
47.2.1 DLF-Control Configuration List 394
47.2.2 Configure DLF-forward unicast 394
47.2.1 Configure DLF-forward multicast 395
47.2.2 Displays and Maintain DLF-forward Configurations 395
Chapter 48 SLF-Control 396
48.1 SLF-Control Overview 396
48.2 Configure SLF-Control 396
48.2.1 SLF-Control Configuration List 396
48.2.2 Configure SLF-forward unicast 396
48.2.3 Displays and Maintain SLF-forward Configurations 397
Chapter 49 BPDU-Discard 398
49.1 BPDU-Discard Overview 398
49.2 Configure BPDU-Discard 398

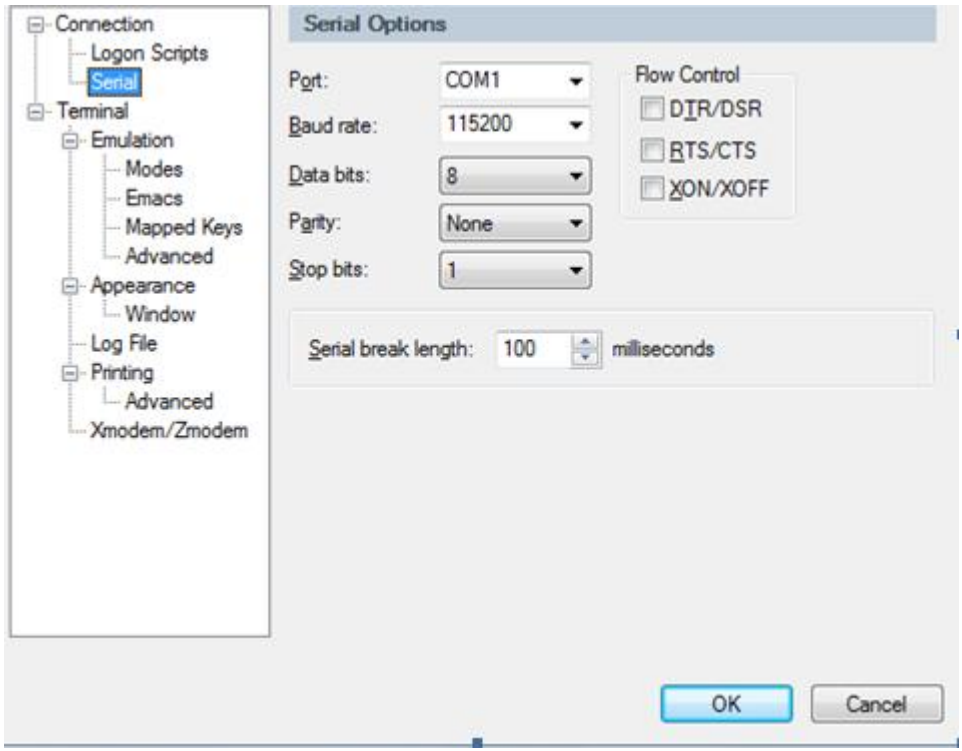
49.2.1 BPDU-Discard Configuration List 398
49.2.2 Configure BPDU-Discard 398
49.2.3 Displays and Maintain BPDU-Discard Configurations 399
Chapter 50 BPDU-Tunnel 400
50.1 BPDU-Tunnel Overview 400
50.2 Configure BPDU-Tunnel 401
50.2.1 BPDU-tunnel Configuration List 401
50.2.2 Configure BPDU-Tunnel Packet 401
50.2.3 Configure BPDU-Tunnel Destination MAC 401
50.2.4 Displays and Maintain BPDU-Tunnel Configuration 402
Chapter 51 Local-Switch 403
51.1 Local-Switch Overview 403
51.2 Configure Local-Switch 403
51.2.1 Local-switch Configuration List 403
51.2.2 Enable local-switch 403
51.2.3 Displays and Maintain Local-switch Configurations 404
Chapter 52 Port&CPU Utilization Alarm 405
52.1 Port&CPU Utilization Alarm Overview 405
52.2 Configure Port&CPU Utilization Alarm 405
52.2.1 Port & CPU Utilization Alarm Configuration List 405
52.2.2 Configure Port Utilization Alarm 406
52.2.3 Configure CPU Utilization Alarm 406
52.2.4 Display and Debugging Device Utilization Alarm 407

Chapter 1 Access Switch

1.1 CLI

You can access Switch in the following ways:

1.Perform local configuration through the Console port, the serial port baud rate is 115200, set as shown in the figure below：



2、Local or remote configuration by Telnet/SSH；

3、Provide FTP, TFTP, Xmodem services to facilitate users to upload and download files.

1.1.1 Command Syntax

The login verification of the system console of this Switch is mainly used to verify the identity of the operating user. The matching identification of the name and password to allow or deny the user's login.

Step 1: When entering the command line interface, the following login prompt appears:

Login:

Please enter the login user name, press Enter, and then enter the password:

*****

After entering the correct login password, you can enter the normal user view:

Switch>

There are two different permissions, one for administrator permissions and the other for ordinary user permissions.

Ordinary users can only view and have no right to modify, but the administrator can manage and configure the Switch.

If you log in as a system administrator, you will enter the privileged user view:

Switch>enable

Step 2：After typing the complete command, press Enter

E.g：

!The user does not need to enter parameters

[Switch]quit

"quit" is a command without parameters. After typing this command, press Enter to execute the command.

!Need to enter parameters

[Switch]vlan 100

The command keyword is vlan and the parameter value is 100.

1.1.2 Help of Command Line

There is a built-in syntax help in the command line interface. In any command mode, type "?" or use the help command to get all the commands in the command mode and their brief descriptions.

E.g：

1.Type "?" directly in the privileged user view

<Switch>?

Commands of system mode:

---

clear clear erps-ring's statistics

cls clear screen

display display running system information

2．Type "?" immediately after the keyword

[Switch]interf?

interface

3. Type a space after the command line string and add "?"

[Switch]stp ?

forward-time config delaytime

hello-time config hellotime

max-age config max agingtime

priority config priority

<enter> The command end.

4. Parameter range or format

[Switch]stp forward-time ?

INTEGER<4-30> delaytime: <4-30>(second)

5. Prompt for the end of the command line

[Switch] stp ?

<enter> The command end.

1.1.3 Display history Command of Command Line

Command line interface provides the function similar to that of DosKey. The commands entered by users can be automatically saved by the command line interface and you can invoke and execute them at any time later. History command buffer is defaulted as 100. That is, the command line interface can store 100 history commands for each user, you can type "up arrow" or "Ctrl+P", and access the next command can type "down arrow" or "Ctrl+N".

1.2 Manage Users

The system provides two user permissions：

-Admin administrator

-Normal user

The normal users can only be in the user's mode after logging in the Switch so they can only check the basic information about operation and statistics; administrator can enter each configuration mode to check and manage the system.

1.2.1 System Default User

There is an internal username with password called Super-administrator. It processes the superior priority in the Switch to manage both the users and the Switch.

The username of Super-administrator is admin and its initial password is admin. It is suggested modifying the password after the initial-logging in. This username and its administrator privilege cannot be deleted and modified.

1.2.2 Add User

Operation	Command	Remarks
Enter super user view	**enable**	
Enter global configuration mode	**system-view**	
Add Account	**terminal user username** [**privilege** level] { **password** encryption-type password }	
display user	**display terminal user**	

username：the username of the newly added user，The length is 1 to 32 characters, must be characters, and cannot contain'/',':','*','?','\\','<','>','|',""

privilege：User authority, the value range is 0～15. 0～1 means normal user; 2～15 means administrator

encryption-type：The value is 0 or 7, 0 means that the password is set in plain text, and 7 means that the password is set in cipher text

password：Login password, the length is 1-16 characters.

Example:

!Create the administrator user “test”, the password is test, and the privilege level is 15

[Switch]username test privilege 15 password 0 test

Notice:

Username is not case sensitive, password is case sensitive；

Only the system administrator admin user can delete user accounts, other users cannot delete users；

The system administrator admin can modify the password of himself or other users, and other administrator users can only modify their own passwords；

1.2.3 Change Password

Operation	Command	Remarks
Enter super user view	**enable**	
Enter global configuration mode	**system-view**	
Change password	**terminal user change-password**	

Example:

!Change the password of user “test” to 1234

[Switch] terminal user change-password

please input you login password : ********

please input username :test

Please input user new password :****

Please input user comfirm password :****

change user test password success.

1.2.4 Modify User's Privilege Level

Operation	Command	Remarks
Enter super user view	**enable**	
Enter global configuration mode	**system-view**	
Modify user Privilege Level	**terminal user username** [**privilege** *level*] { **password** *encryption-type password* }	

Example:

!Modify the privilege of the existed user “test” to 1, and the password totest

[Switch] terminal user test privilege 1 password 0 test

1.2.5 Delete User

Operation	Command	Remarks
Enter super user view	**enable**	
Enter global configuration mode	**system-view**	
Delete user	**undo terminal user** *username*	

Example:

!Delete user “test”

[Switch]undo terminal username test

1.2.6 Display Users

Operation	Command	Remarks
Display user	**display terminal user** [*username*]	

【Example】

！Display the information of user ”test”

[Switch]display terminal user test

1.2.7 Display Users

Operation	Command	Remarks
Display user	**display login-users**	

【Example】

！Display the information of user ”test”

[Switch]display login-users

1.2.8 Kick off Online Telnet Users

Operation	Command	Remarks
Enter super user view	**enable**	
Kick off online telnet users	**remote-stop** username	

【Example】

！Kick off online telnet users “test”

<Switch>remote-stop test

1.3 Remote Authentication Configure

User accounts can be stored in the local database of the Switch or in RADIUS/TACACS+ server，The system uses the local database by default.

Notice：

The admin user only supports the authentication method of the local database.

1.3.1 Enable RADIUS/TACACS+

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable Radius/Tacacs	**user-auth** { local | { radius *radiusname* { pap | chap } [local] } } | { tacacs+ [author] [account] [local] }	The default is local authentication

1.3.2 Display Authentication Method

Operation	Command	Remarks
Display authentication method	**display user-auth**	

1.3.3 TACACS+ Remote Server Configuration

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Configure Tacacs+Remote Server	**tacacs+** { priamary | secondary } **server** *ipaddress* [key *keyvalue*] [port *portnum*] [timeout *timevalue*]	

1.3.4 Dsiplay TACACS+ Information

Operation	Command	Remarks
Dsiplay TACACS+ information	**display tacacs+**	

Chapter 2 System Management

2.1 System Maintenance

2.1.1 Display System Status Information

Operation	Command	Remarks
Display version information	**display version**	
Display user information	**display terminal user**	
Display logged-in user information	**display login-users**	
Display system memory information	**display memory**	
Display system clock	**display time**	
Display system CPU utilization	**display cpu-info**	

【Example】

！Display system version

[Switch]display version

2.1.2 Configure the System Clock

Operation	Command	Remarks
Enter super user view	**enable**	
Set system clock	**time** HH:MM:SS YYYY/MM/DD	
Enter global configuration mode	**system-view**	

Set clock timezone	**time** zone*name hour minute*	
display system time	**display time**	

【Example】

！Set the system clock to 8:30: 0 on October 1, 2020

[Switch]time 08:30:0 2020/10/01

2.1.3 Configure System Host Name

Operation	Command	Remarks
Enter super user view	**enable**	
Enter global configuration mode	**system-view**	
Configure the host name	**SW** *SW*	
Delete the host name	**undo SW**	

【Example】

！Set the host name to Switch-ABCD

[Switch]SW Switch-ABCD

[Switch-ABCD]

2.1.4 Trace Route Command

Support tracert command and check network connection. The tracert command can be executed in any view：

Operation	Command	Remarks
Tracert test	**tracert** [-u | -c] [-p *udpport* | -f *first_ttl* | -h *maximum_hops* | -w *time_out*] *target_name*	

【Parameter Description】

-u： Send udp message;

-c： Send echo message of icmp;

-p udpport：The destination port , the value range is 1-65535, the default port is 62929;

-f first_ttl：The initial ttl value, the value range is 1-255, the default value is 1;

-h maximum_hops：The maximum ttl value, the value range is 1-255, the default value is 30;

-w time_out：The timeout period for waiting for a response, the value range is 10-60 seconds, and the default value is 10 seconds;

target_name：Destination host or router address

【Example】

！Trace the route that can reach 192.168.1.2

<Switch>tracert 192.168.1.2

2.1.5 Port Loopback Test Command

The system supports port loopback test function, used to test the internal and external connectivity of the port：

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Loopback test on all ports	**loopback** { **internal** | **external** }	

Enter interface view	**interface** { {ethernet *interface-num* } | interface-name }	
Lloopback test on a single port	**loopback** { **internal** | **external** }	

2.1.6 Line Detection VCT Command

VCT is used to detect network cable normal (NORMAL), open circuit (OPEN), short circuit (SHORT), impedance mismatch (IMPEDANCE MISMATCH) and other error conditions.

The normal connection of the network cable is NORMAL, the disconnection of the network cable is OPEN, and the short circuit of the network cable is SHORT. Impedance mismatch (IMPEDANCE MISMATCH) generally occurs when two network cables with different impedances are connected together. If an error is found, the location of the error can be detected. The longest detection distance of VCT is 181 meters for 100M ports and 175 meters for Gigabit ports：

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Perform VCT detection on all ports	**vct run**	
Enter interface view	**interface** { { ethernet*interface-num* } | interface-name }	
Perform VCT detection on a single port	**vct run**	

【Example】

！VCT test on Ethernet port 1

[Switch-ethernet-0/1]vct run

Notice:

VCT detection is only for Cat 5 Ethernet ports and does not support VCT detection on optical fiber ports.

2.1.7 Management IP Address Configuration

You can restrict the host IP address or a certain network segment that log in to the Switch's web, telnet, snmp agent, and other IP addresses other than the matching configuration cannot manage the Switch.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure management IP address restrictions	**login-acl** { **web** | **snmp** | **telnet** } *ip-address wildcard*	
Remove management IP address restrictions	**undo login-acl** { all | { web | snmp | telnet { all | *ip-address wildcard* }}}	
Display management IP address restriction configuration information	**display login-acl**	

【Example】

！The configuration only allows addresses in the network segment 192.168.0.0/255.255.0.0 to access the Switch through telnet

[Switch] login-acl telnet 192.168.0.1 0.0.255.255

[Switch]undo login-acl telnet 0.0.0.0 255.255.255.255

！Display the configuration of the management ip address restriction：

[Switch]display login-acl

2.1.8 Telnet User Limit for Login Privileged User View

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure the number of Telnet users	**telnet-server limit** *limit-num*	
Remove the limit on the number of users logging in to Telnet	**undo telnet-server limit**	
Display Telnet user limit configuration information	**display telnet-server**	

【Example】

！Configure to allow only two Telnet users to enter privileged user view at the same time

[Switch] telnet-server limit 2

2.1.9 CPU-CAR Command

CPU-CAR is mainly used to set the rate at which the CPU receives packets to limit the number of packets sent to the CPU per second.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure CPU-CAR	**cpu-car** *target_rate*	
Restore the default CPU-CAR Value	**undo cpu-car**	
Display CPU-CAR	**display cpu-car**	

【Example】

！Set the rate of cpu receives packets to 100pps

[Switch]cpu-car 100

2.1.10 SSL

SSL (Secure Socket Layer) Provide transport layer security services (according to the 7-layer protocol, it can also be considered as the session layer)，First developed by Netscape (1995), it was widely used in Web and other security services, and later adapted to the Internet standard TLS (TLS1.0, RFC2246, similar to SSL3.0)

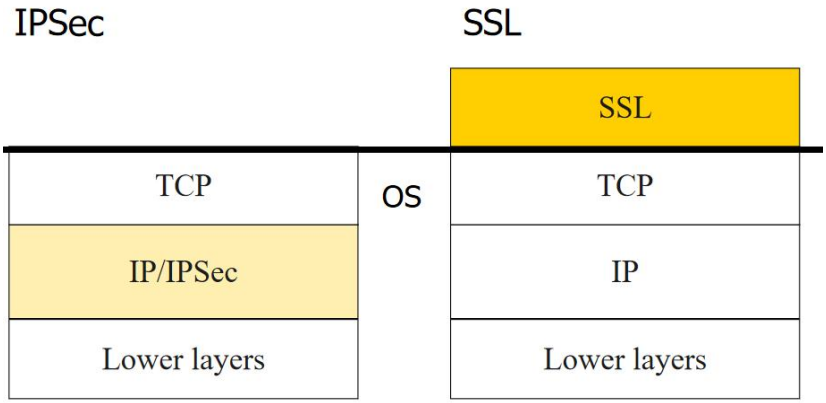
Independent of application layer

The transport layer uses TCP to provide reliable services

SSL can be divided into two layers:

SSL handshake protocol: used to exchange security information before establishing a secure connection between the client and the server

SSL recording protocol (low): determine the data security transmission mode



Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure SSL	**http enable ssl**	The default is http mode
Restore the default	**http disable**	
Display CPU-CAR	**display http**	

【Example】

[Switch]display http

Web Server status:

Running:TRUE

Port:80

[Switch]http enable ssl



2.2 Configuration Management

2.2.1 Save Configurations

After modified the configurations, you should same them so that these configurations can take effect next time it restarts. Use the following commands to save configurations.

Operation	Command	Remarks
Enter super user view	**enable**	
Save configurations	**save current-config**	

2.2.2 Erase Configurations

If you need to reset to factory default, you can use the following commands to erase all configurations. After erased, the device will reboot automatically.

Operation	Command	Remarks
Enter super user view	**enable**	
Erase configuration	**clear save-config**	

2.2.3 Execute save Configuration

Operation	Command	Remarks

Enter super user view	**enable**	
Execute save configuration	**update current-config**	

2.2.4 Show save Configurations

Use the following command to display the configurations you have saved.

Operation	Command	Remarks
Show configuration	**display save-config** [*module-list*]	

【Example】

! Display all contents of the configuration file

<Switch>display save-config

! Display the contents of GARP and OAM modules in the configuration file

<Switch>display save-config garp oam

2.2.5 Show Running Configurations

Operation	Command	Remarks
Show running configurations	**display current-config** [*module-list*] [perlines*num*]	

【Example】

! Display all configuration information

<Switch>display current-config

! Display configuration information for vlan

<Switch>display current-config vlan

2.3 Load Files and Upgrade Programs Online

2.3.1 Upload and Download Files by TFTP

Operation	Command	Remarks
Enter super user view	**enable**	
upload files	**upload** { configuration | info-center } tftp *tftpserver-ip filename*	configuration is the system save configuration file. info-center is the system log file
download file	l**oad** { configuration | host | bootrom } tftp *tftpserver-ip filename*	configuration is the system save configuration file. application is the device upgrade host program. whole-bootrom is the bootrom program for the device

tftpserver-ip is the IP address of the TFTP server, and filename is the name of the file to be uploaded. Before entering the command, open the TFTP server and set the destination path for the file upload.

【Example】

！Upload the configuration file by TFTP and name the configuration file config.txt

<Switch>upload configuration tftp 192.168.1.100 config.txt

After the upload is successful, the file config.txt in the computer with the IP address of

192.168.1.100 saves the current configuration.

！Download the configuration file config.txt by TFTP,

<Switch>load configuration tftp 192.168.1.100 config.txt

After downloading successfully and restarting the system, the system will use the new configuration file config.txt

！Upload the log file by TFTP and name the log file log.txt

<Switch>upload info-center tftp 192.168.1.100 log.txt

！Download the upgrade file host.bin by TFTP

<Switch>load host tftp 192.168.1.100 host.bin

After downloading successfully and restarting the system, host.bin will run.

！Download the bootrom program boot.bin by TFTP

<Switch>load bootrom tftp 192.168.1.100 boot.bin

2.3.2 Upload and Download Files by FTP

Operation	Command	Remarks
Enter super user view	**enable**	
upload files	**upload** { configuration | info-center } ftp *ftpserver-ip filename usename password*	
download file	**load** { configuration | host | bootrom } ftp *ftpserver-ip filename usename password*	

ftpserver-ip is the IP address of the FTP server, and filename is the name of the file to be

uploaded. username and userpassword are the username and password set in the FTP server. Before entering the command, you should open the FTP server, and set the user name, password, and the destination path of the file upload.

【Example】

！Upload the configuration file by FTP and name the configuration file config.txt

<Switch>upload configuration ftp 192.168.1.100 config.txt admin 123

！Download configuration files by FTP

<Switch>load configuration ftp 192.168.1.100 config.txt admin 123

！Download the upgrade file host.bin by ftp

<Switch>load host ftp 192.168.1.100 host.bin admin 123

！Upload the log file by FTP and name the log file log.txt

<Switch>upload info-center ftp 192.168.1.100 log.txt admin 123

！Download the bootrom program boot.bin by FTP

<Switch>load bootrom ftp 192.168.1.100 boot.bin admin 123

2.3.3 Download Files by Xmodem

Operation	Command	Remarks
Enter super user view	**enable**	
download file	l**oad** { configuration | host | bootrom } xmodem	

After entering the command, select "Transfer" ->"Send File" in the HyperTerminal menu, and enter the full path and file name of the file in the "File Name" column of the "Send File" dialog box that pops up, and the "Protocol" drop-down Select Xmodem in the list, and then click the

[Send] button.

【Example】

！Download the host program by Xmodem

<Switch>load application xmodem

2.4 Reboot Switch

Operation	Command	Remarks
Enter super user view	**enable**	
Restart the Switch immediately	**reboot**	
Enter system view	**system-view**	
Auto restart at specified time	**auto-reboot** { in { minutes *min* | hours *hour* } | at { *YYYY/MM/DD hh:mm:ss* | *hh:mm:ss* daily | *hh:mm:ssweekday* weekly } }	
Cancel scheduled automatic restart	**undo auto-reboot**	

【Example】

！Set to restart at 03:30:30 on May 15, 2020

[Switch]auto-reboot at 03:30:30 2020/05/15

！Set to restart at 03:30:30 every Monday morning

[Switch]auto-reboot at 03:30:30 mon weekly

Chapter 3 Port Configuration

3.1 Ethernet Port Configuration Overview

The gigabit port of the Switch supports 10/100/1000Base-T. The port can work in half-duplex and full-duplex modes. It can negotiate with other network equipment to determine the working mode and rate, and automatically select the most suitable working mode and rate. Simplified system configuration and management. The 10G optical port supports 1000M, 10000Mbps full-duplex speed mode. The PON port has a fixed rate and does not support rate configuration

3.2 Configure Ethernet Port

3.2.1 Enter Interface Configuration Mode

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode.	**interface** { { ethernet *interface-num* } | interface-name }	

3.2.2 Enter Interface Range Mode

Operation	Command	Remarks
Enter global mode	**system-view**	
Enter interface range	**interface range** { { ethernet	

mode.	*interface-list* } | *interface-name* }	

【Example】

！Enter interface range configuration mode, this range includes Ethernet 1~3

[Switch]interface range ethernet 0/0/1 to e 0/0/3

[Switch-port-range]

3.2.3 Basic Port Configuration

Operation	Command	Remarks
Enter global mode	**system-view**	
Enter interface mode	**interface** { { ethernet *interface-num* } | *interface-name* }	
Disable specific port	**shutdown**	
Enable specific port	**undo shutdown**	
Configure speed of a port	**speed** { 10 | 100| 1000 | 10000 | auto }	
Configure default duplex of a port	**undo speed**	
Configure duplex of a port	**duplex** { full | half }	
Configure priority of a port	**priority** *priority-num*	
Configure default priority of a port	**undo priority**	
Configure port description	**description** *description-list*	
Delete port description	**undo description**	
Enable ingress filtering	**ingress filtering**	

Disable ingress filtering	**undo ingress filtering**	
Enable ingress acceptable-frame	**ingress acceptable-frame** { all | tagged }	
Disable ingress acceptable-frame	**undo ingress acceptable-frame**	
Enable Ethernet port flow control	**flow-control**	
Disable Ethernet port flow control	**undo flow-control**	
Display port flow control function	**display flow-control** interface [ethernet *interface-num*]	

3.2.4 Link Type of Ethernet Ports

An Ethernet port can operate in one of the three link types:

Access: An access port only belongs to one VLAN, normally used to connect user device.

Trunk: A trunk port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs and is generally used to connect another Switch. The packet sent from this port can be with or without the tag label.

Hybrid: A hybrid port can belong to multiple VLANs, can receive, or send packets for multiple VLANs, used to connect either user or network devices. It allows packets of multiple VLANs to be sent with or without the tag label

Operation	Command	Remarks
Enter global mode	**system-view**	
Enter interface mode	**interface** { { ethernet *interface-num* } | *interface-name* }	

Set port link type	**port mode** { trunk | hybrid | access }	
Configure default link type	**undo port mode**	The default port type is Hybrid

【Example】

！Set Ethernet port 1 as a trunk port

[Switch-ethernet-0/0/1]port mode trunk

3.2.5 Configure Default VLAN

Operation	Command	Remarks
Enter global mode	**system-view**	
Enter interface mode.	**interface** { { ethernet *interface-num* } | *interface-name* }	
Set port default vlan id	**port default vlan** *vlan-id*	
Restore port default vlan id	**undo port default vlan**	

【Example】

！Set the default VLAN ID of Ethernet 0/1 to 5

[Switch-ethernet-0/0/1] port default vlan 5

3.2.6 Add Port to a Vlan

Operation	Command	Remarks
Enter global mode	**system-view**	

Enter interface mode	**interface** { { ethernet *interface-num* } | *interface-name* }	
Configure the port mode as access	**port mode access**	
Add the Access port to the specified vlan	**port default vlan** *vlan-id*	
Configure the port mode as Hybrid	**port mode hybrid**	
Add Hybrid port to specific VLAN and keep the packet VID	**port hybrid tagged vlan** { all | *vlan-list* }	
Add Hybrid port to specific VLAN and strip the packet VID	**port hybrid untagged vlan** { all | *vlan-list* }	
Delete Hybrid port from specific VLAN	**undo port hybrid vlan** { all | *vlan-list* }	
Configure the port mode as Trunk	**port mode trunk**	
Add Trunk port to specific VLAN	**port trunk allowed vlan** { all | *vlan-list* }	
Delete Trunk port from specific VLAN	**undo port trunk allowed vlan** { all | *vlan-list* }	

3.2.7 Dsiplay Port Information

Operation	Command	Remarks
Display port information	**display interface** [ethernet *interface-num* }]	
Display summary information of all ports	**display interface brief**	
Display port sfp information	**display interface sfp** [ethernet	

	interface-num }]	

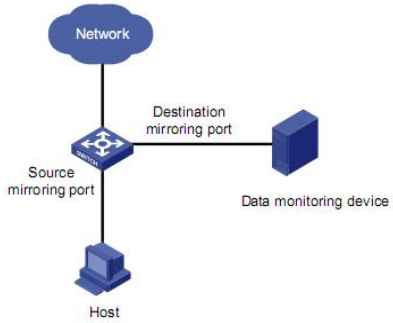
3.2.8 Display and Clear Port Statistics

Operation	Command	Remarks
Display port statistics	**display statistics interface** [ethernet *interface-num* }]	
Display all port statistics	**display statistics interface brief**	
Display real-time sending and receiving rates and band utilization	**display utilization interface**	
Enter global mode	**system-view**	
Clear port statistics	**clear interface** [ethernet *interface-num* }]	
Enter interface mode	**interface** { { ethernet *interface-num* } | *interface-name* }	
Clear port statistics	**clear interface**	

Chapter 4 Port Mirroring

4.1 Port Mirroring Overview

Mirroring refers to the process of copying packets that meet the specified rules to a destination port. Generally, a destination port is connected to a data detect device, which users can use to analyze the mirrored packets for monitoring and troubleshooting the network.



4.2 Configure Port Mirroring

4.2.1 Configure Port Mirroring

The source port is specified and whether the packets to be mirrored are ingress or egress is specified: ingress: only mirrors the packets received via the port; egress: only mirrors the packets sent by the port; both: mirrors the packets received and sent by the port at the same time.

The destination port is specified.

4.2.2 Configure the Mirror Destination Port

Operation	Command	Remarks
Enter global mode	**system-view**	
Configure destination port (so called monitor port)	**mirror group** *group-id* **destination-interface ethernet** *interface-num*	
Delete destination monitor port	**undo mirror group** { all | group-id **destination-interface ethernet** interface-num }	

4.2.3 Configure the Mirror Source Port

Operation	Command	Remarks
Enter global mode	**system-view**	
Configure source port	**mirror group** group-id **source-interface** { ethernet | cpu } *interface-list* { both | egress | ingress }	
Delete source monitor port	**undo mirror group** { all | *group-id* source-interface { cpu | *interface-list* } }	

【Example】

！Configure Ethernet ports 1 and 2 as mirror source ports

[Switch] mirror group 1 source-interface ethernet 0/0/1 to ethernet 0/0/2 both

4.2.4 Display Port Mirroring

Operation	Command	Remarks
Display port mirroring	**display mirror group** { all | *group-id* }	

【Example】

！Display port mirroring

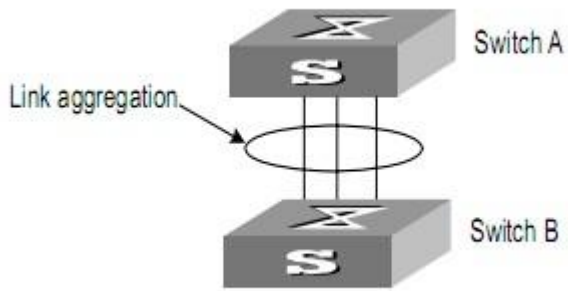
<Switch>display mirror group all

Chapter 5 Link Aggregation

5.1 Link Aggregation Overview

Link aggregation means aggregating several ports together to form an aggregation group, so as to implement outgoing/incoming load sharing among the member ports in the group and to enhance the connection reliability.

Depending on different aggregation modes, aggregation groups fall into two types: static LACP and dynamic LACP. Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups.



For the member ports in an aggregation group, their basic configuration must be the same. The basic configuration includes STP, QoS, VLAN, port attributes, and other associated settings.

- STP configuration, including STP status (enabled or disabled), link attribute (point-to-point

or not), STP priority, maximum transmission speed, loop prevention status.

- QoS configuration, including traffic limiting, priority marking, default 802.1p priority, traffic monitor, traffic redirection, traffic statistics, and so on.
- VLAN configuration, including permitted VLANs, and default VLAN ID, tag vlan list for hybrid port and allowed vlan list for trunk port.

Port attribute configuration, including port rate, duplex mode, and link type (Trunk, Hybrid or Access). The ports for a static aggregation group must have the same rate and link type, and the ports for a dynamic aggregation group must have the same rate, duplex mode (full duplex) and link type.

5.1.1 Introduction to LACP

The purpose of link aggregation control protocol (LACP) is to implement dynamic link aggregation and disaggregation. This protocol is based on IEEE802.3ad and uses LACPDUs (link aggregation control protocol data units) to interact with its peer.

After LACP is enabled on a port, LACP notifies the following information of the port to its peer by sending LACPDUs: priority and MAC address of this system, priority, number and operation key (it is so called O-Key) of the port. Upon receiving the information, the peer compares the information with the information of other ports on the peer device to determine the ports that can be aggregated with the receiving port. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group.

5.1.2 Operation Key (O-Key)

An operation key of an aggregation port is a configuration combination generated by system depending on the configurations of the port (rate, duplex mode, other basic configuration, and administrative key) when the port is aggregated.

1) The ports in the same aggregation group must have the same operation key (O-Key) and administrative key (A-Key).

2) The administrative key (A-Key) and operation key (O-Key) of an LACP-enable aggregation port is equal to its aggregation group ID+1.

3) The administrative key (A-Key) and operation key (O-Key) of an LACP-enable aggregation port cannot be modified.

4) The operation key (O-Key) which is contained in LACPDU of an LACP-enable aggregation port is the same as its peer.

5.1.3 Static Aggregation Group

1) Introduction to Static Aggregation

A static aggregation group is manually created. All its member ports are manually added and can be manually removed. Each static aggregation group must contain at least one port. When a static aggregation group contains only one port, you cannot remove the whole aggregation group unless you remove the port.

LACP is disabled on the member ports of static aggregation groups, and enabling LACP on such a port will not take effect.

2) Port status of Static Aggregation Group

A port in a static aggregation group is only in one state: on, which means the port in a static

aggregation group must transceive packets. There can be at most 8 ports in a static aggregation group.

5.1.4 Dynamic LACP Aggregation Group

1) Introduction to Dynamic LACP Aggregation Group

A dynamic LACP aggregation group is also manually created. All its member ports are manually added and can be manually removed. Each dynamic aggregation group must contain at least one port. When a dynamic aggregation group contains only one port, you cannot remove the whole aggregation group unless you remove the port.

LACP is enabled on the member ports of dynamic aggregation groups, and disabling LACP on such a port will not take effect.

2) Mode of Dynamic Aggregation Group

The mode of dynamic aggregation group can be active or passive. It is manually set by users. The dynamic aggregation group in active mode will actively send LACPDUs; group in passive mode will only response LACPDUs passively. When interconnecting with another device, static mode can only interconnect with static mode; active mode can interconnect with both active and passive mode, but passive mode can only interconnect with active mode. The default mode is ACTIVE.

3) Port Status of Dynamic Aggregation Group

A port in a dynamic aggregation group can be in one of the three states: bundle (bndl), standby, and no-bundle (no-bndl). In dynamic aggregation group, only bundled ports can transceive LACP protocol packets; others cannot.

Note:

In an aggregation group, the bundled port with the minimum port number serves as the master port of the group, and other bundled ports serve as member ports of the group.

No-bundled ports are the ports which fail to form link aggregation with other ports in the dynamic aggregation.

There is a limit on the number of bundled ports in an aggregation group. Therefore, if the number of the member ports that can be set as bundled ports in an aggregation group exceeds the maximum number supported by the device, the system will negotiate with its peer end, to determine the states of the member ports according to the port IDs of the preferred device (that is, the device with smaller system ID). The following is the negotiation procedure:

1) Compare device IDs (system priority + system MAC address) between the two parties. First compare the two system priorities, then the two system MAC addresses if the system priorities are equal. The device with smaller device ID will be considered as the preferred one.

2) Compare port IDs (port priority + port number) on the preferred device. The comparison between two port IDs is as follows: First compare the two port priorities, then the two port numbers if the two port priorities are equal; the port with the smallest port ID is the bundled port and the left ports are standby ports.

4) Configure System Priority

LACP determines the bundled and standby states of the dynamic aggregation group members according to the priority of the port ID on the end with the preferred device ID.

The device ID consists of system priority and system MAC address, that is, device ID = system priority + system MAC address.

When two device IDs are compared, the system priorities are compared first, and the system MAC addresses are compared when the system priorities are the same. The device with smaller device ID will be considered as the preferred one.

Note:

Changing the system priority of a device may change the preferred device between the two parties, and may further change the states (bundled or standby) of the member ports of dynamic aggregation groups.

5) Configure Port Priority

LACP determines the bundled and standby states of the dynamic aggregation group members according to the port IDs on the device with the preferred device ID. When the number of members in an aggregation group exceeds the number of bundled ports supported by the device in each group, LACP determines the bundled and standby states of the ports according to the port IDs. The ports with superior port IDs will be set to bundled state and the ports with inferior port IDs will be set to standby state.

The port ID consists of port priority and port number, that is, port ID = port priority + port number. When two port IDs are compared, the port priorities are compared first, and the port numbers are compared if the port priorities are the same. The port with smaller port ID is considered as the preferred one.

5.2 Redundancy of Interconnected Device

LACP provides link redundancy mechanism to guarantee the redundancy conformity of the two interconnected devices and user can configure the redundant link which is realized by system and port priority. The steps are as following:

Step 1 Selection reference. The two devices know the LACP sys-id and system MAC address of each other through LACPDUs exchanges. The system priorities are compared first, and the system MAC addresses are compared when the system priorities are the same. The device with smaller device ID will be considered as the preferred one.

Step 2 Redundant link. The port priorities are compared first, and the port numbers are compared if the port priorities are the same. The port with smaller port ID is considered as the preferred one.

5.3 Load-balancing Policy

Load-balancing policy is specific physical link selection strategy when sending packets, which can be source MAC, destination MAC, source and destination MAC, source IP, destination IP, and source and destination IP. The default strategy is source MAC.

5.4 Configure Link Aggregation

5.4.1 Link AggregationConfiguration List

Configuration Task	Description	Detailed Configuration

Configure a Static Aggregation Group	Required	5.4.2
Configure a Dynamic LACP Aggregation Group	Required	5.4.3
Display and Maintain Link Aggregation Configuration	Optional	5.4.4

5.4.2 Configure a Static Aggregation Group

You can create a static aggregation group, or remove an existing static aggregation group (before that, all the member ports in the group are removed).

You can manually add/remove a port to/from a static aggregation group, and a port can only be manually added/removed to/from a static aggregation group.

Perform the configuration in global configuration mode.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Create a static aggregation group	**channel-group** *channel-group-number*	*channel-group-number* ranges from 0 to 51.
Configure load-balancing policy	**channel-group load-balance { dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac }**	
Enter interface configuration mode	**Interface ethernet** *interface-num*	
Enter interface range configuration mode	**interface range ethernet** *interface-list*	
Add a port to the aggregation group	**channel-group** *channel-group-number* **mode on**	

Delete a port from an aggregation group	**undo channel-group** *channel-group-number*	
Back to global configuration mode	**quit**	
Delete a static aggregation group	**undo channel-group** *channel-group-number*	

5.4.3 Configure Dynamic LACP

You can manually add/remove a port to/from a dynamic aggregation group, and a port can only be manually added/removed to/from a dynamic aggregation group.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Create a dynamic aggregation group	**channel-group** *channel-group-number*	*channel-group-number* ranges from 0 to 51
Configure load-balancing policy	**channel-group load-balance { dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac }**	Src-mac by default
Configure system priority	**lacp system-priority** *priority*	32768 by default
Enter interface configuration mode	**Interface thernet** *interface-num*	
Enter interface range configuration mode	**interface range ethernet** *interface-list*	
Add a port to the aggregation group	**channel-group** *channel-group-number* **mode** { **active | passive** }	
Configure port priority	**lacp port-priority** *priority*	128 by default
Delete a port from an aggregation group	**undo channel-group** *channel-group-number*	

Back to global configuration mode	**quit**	
Delete a dynamic aggregation group	**undo channel-group** *channel-group-number*	

5.4.4 Display and Maintain LACP

After the above configuration, execute the display command in any mode to display the running status after the link aggregation configuration and verify your configuration.

Operation	Command	Remarks
Display system LACP ID	**display lacp sys-id**	System LACP-ID consists of 16-bit system priority and 48-bit system MAC.
Display port member info of the aggregation group	**display lacp internal** [*channel-group-number*]	
Display neighbor port info of the aggregation group	**display lacp neighbor** [*channel-group-number*]	
Display packet statistics of the aggregation group	**display statistics channel-group** [*channel-group-id*]	
Display packet statistics of the aggregation group by dynamic	**display statistics dynamic channel-group**	
Display utilization statistics of the aggregation group	**display utilization channel-group**	

Clear packet statistics of the aggregation group	**clear channel-group** [*channel-group-id*]	

Chapter 6 Port Isolation

6.1 PortIsolation Overview

To implement Layer 2 isolation, you can add different ports to different VLANs. However, this will waste the limited VLAN resource. With port isolation, the ports can be isolated within the same VLAN. Thus, you need only to add the ports to the isolation group to implement Layer 2 isolation. This provides you with more secure and flexible networking schemes.

On the current device:

- Currently, only one isolation group is supported on a device, which is created automatically by the system as isolation group. The user cannot remove the isolation group or create other isolation groups.
- The number of the ports an isolation group can contain is total port number-1. Because isolated ports are downlink ports. There should be at least one uplink port.

Note:

When a port in an aggregation group is configured as the member of isolation group, the other ports of the aggregation group will not be downlink ports.

6.2 Configure Port Isolation

6.2.1 Add/remove Isolated Ports

Add a port to port-isolation group. The isolated port members cannot communicate with each other, but can only communicate with un-isolated port.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface range configuration mode	**interface range** *interface-list*	
Configure port isolation	**port-isolation uplink ethernet** *interface-num*	
Delete uplink port	**undo port-isolation** [uplink ethernet *interface-num*]	

6.2.2 Display Port Isolation Configuration

Operation	Command	Remarks
Display isolate-port configuration	**display port-isolation**	Display isolate-port configuration

Chapter 7 Storm-Control

7.1 Storm-Control Overview

When there is loop or malicious attacker in the network, there will be plenty of packets, which occupy the bandwidth and even affect the network. Storm-control will avoid too much packets appear in the network. Restrict the speed rate of port receiving broadcast/multicast/unknown unicast packets and unknown unicast packets received by all ports. By default, Broadcast storm control is Enable; Multicast storm control is Disable; Unicast storm control is Disable.

7.2 Configure Storm-Control

7.2.1 Configure Storm-Control

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface** [range] { { ethernet *interface-list* } | *interface-name* }	
Configure storm-control type and rate	**storm-control** { broadcast | multicast | unicast } { disable | pps *target-rate*}}	
Delete port storm	**undo storm-control** { broadcast | multicast | unicast }	

7.2.2 Storm-Control Monitor and Maintenance

Operation	Command	Remarks
Display Storm-control	**display storm-control interface** [ethernet *interface-list*]]	

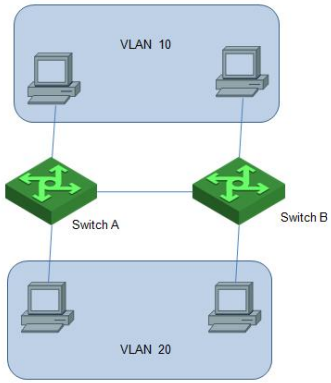
Chapter 8 VLAN

8.1 VLAN Overview

Virtual Local Area Network (VLAN) groups the devices of a LAN logically but not physically into segments to implement the virtual workgroups. IEEE issued the IEEE 802.1Q in 1999, which was intended to standardize VLAN implementation solutions.

Through VLAN technology, network managers can logically divide the physical LAN into different broadcast domains. Every VLAN contains a group of workstations with the same demands. The workstations of a VLAN do not have to belong to the same physical LAN segment.

With VLAN technology, the broadcast and unicast traffic within a VLAN will not be forwarded to other VLANs, therefore, it is very helpful in controlling network traffic, saving device investment, simplifying network management and improving security.



A VLAN can span across multiple Switches, or even routers. This enables hosts in a VLAN to be dispersed in a looser way. That is, hosts in a VLAN can belong to different physical network segment.

Compared with the traditional Ethernet, VLAN enjoys the following advantages.

1) Broadcasts are confined to VLANs. This decreases bandwidth utilization and improves network performance.

2) Network security is improved. VLANs cannot communicate with each other directly. That is, a host in a VLAN cannot access resources in another VLAN directly, unless routers or Layer 3 Switches are used.

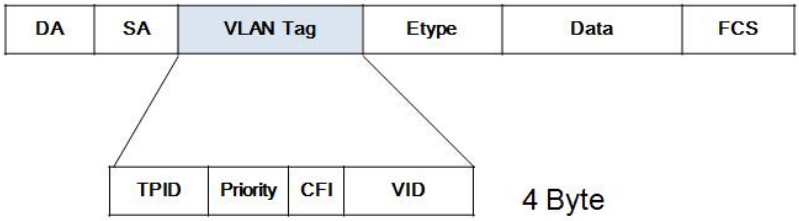
3) Network configuration workload for the host is reduced. VLAN can be used to group specific hosts. When the physical position of a host changes within the range of the VLAN, you need not change its network configuration.

8.1.1 VLAN Principles

VLAN tags in the packets are necessary for the Switch to identify packets of different VLANs. The Switch works at Layer 2 (Layer 3 Switches are not discussed in this chapter) and it can identify the data link layer encapsulation of the packet only, so you can add the VLAN tag field into only the data link layer encapsulation if necessary.

In 1999, IEEE issues the IEEE 802.1Q protocol to standardize VLAN implementation, defining the structure of VLAN-tagged packets.

IEEE 802.1Q protocol defines that a 4-byte VLAN tag is encapsulated after the destination MAC address and source MAC address to display the information about VLAN.



As shown in Figure 1-2, a VLAN tag contains four fields, including TPID (Tag Protocol Identifier), priority, CFI (Canonical Format Indicator), and VID (VLAN ID).

TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100.

Priority is a 3-bit field, referring to 802.1p priority. Refer to section “QoS & QoS profile” for details.

CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format in different transmission media. This field is not described in detail in this chapter.

VID (VLAN ID) is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

VLAN ID identifies the VLAN to which a packet belongs. When the Switch receives an un-VLAN-tagged packet, it will encapsulate a VLAN tag with the default VLAN ID of the inbound port for the packet, and the packet will be assigned to the default VLAN of the inbound port for transmission. For the details about setting the default VLAN of a port, refer to section “02-Port Configuration”

8.2 Configure 802.1Q VLAN

8.2.1 802.1Q VLAN Configuration List

Configuration Task	Description	Detailed Configuration
Create and Modify VLAN	Required	8.2.2
Delete Port Members from a VLAN	Optional	8.2.3
Delete VLAN	Optional	8.2.4
Configure Interface Default vlan ID	Optional	8.2.5
Configure Interface VLAN Mode	Optional	8.2.6
VLAN Attributes Based on Hybrid Interface	Optional	8.2.7
VLAN Attributes Based on Trunk Interface	Optional	8.2.8
Configure Port Priority	Optional	8.2.9
Configure Ingress Filtering	Optional	8.2.10
Configure Types of Interface acceptable-frame	Optional	8.2.11
Display VLANconfiguration	Optional	8.2.12

8.2.2 Create and Modify VLAN

Switch supports 4094 VLANs.

Perform following commands in privilege mode.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Create a vlan and enter vlan configuration mode	**vlan** *vlan-list*	
Add port member to a vlan	**port ethenet** *interface-num*	
Configure vlan description	**description** *vlan-name*	By default, vlan description is empty.
Display the related information about VLAN	**display vlan** { *vlan-id* | brief }	

Note： If the VLAN to be created exists, enter the VLAN mode directly. Otherwise, create the VLAN first, and then enter the VLAN mode.

Vlan-id allowed to configure is in the range of 1 to 4094. Vlan-list can be in the form of discrete number, a sequence number, or the combination of discrete and sequence number, discrete number of which is separate by comma, and sequence number of which is separate by subtraction sign, such as: 2, 5, 8, 10-20.

8.2.3 Delete Port Members from a VLAN

Perform following commands in privilege mode.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Create a vlan and enter vlan configuration mode	**vlan** *vlan-list*	
Delete port member from VLAN	**undo port** { **all | ethernet** *interface-num* }	
Display the related information	**display vlan** { *vlan-id* | brief }	

about VLAN		

8.2.4 Delete VLAN

Perform following commands in privilege mode.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Delete VLAN	**undo vlan** { *vlan-list* | all }	
Display the related information about VLAN	**display vlan** { *vlan-id* | brief }	

8.2.1 Configure Interface Default VLAN ID

Perform following commands in privilege mode.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter Interface configuration mode	**interface ethernet** *interface-num*	
Configure interface pvid	**port default vlan** *vlan-id*	
Configure interface default pvid	**undo port default vlan**	Vlan1 by default
Display interface detailed configurations	**display interface ethernet** *interface-num*	

Display interface brief configurations	**display interface brief ethernet** [*interface-num*]	

8.2.2 Configure Interface VLAN Mode

Interface VLAN mode can be divided into three types according to the different process modes the interface performs on tag label:

Access: the interface only belongs to one vlan, and it usually is used to connect the terminal device.

Trunk: the interface can be able to receive and forward multiple vlans. When the packet is forwarded, the default vlan packet will not carry the tag whereas the other vlan will carry the tag, and the tag is applied to the Switch interface.

Hybrid: the interface can be able to receive and forward multiple vlans, and it allows multiple vlans to carry the tag or not carry the tag.

Interface VLAN mode	**Processing on receiving message**		**Processing on forwarding message**
	Untag	**Tag**	
Access	Receive it and add a tag of pvid to it.	If the VLAN ID of the packet is a VLAN that the port allows to pass through, the packet will	If the VLAN ID carried in a packet is the VLAN ID that the port allows to pass through, the VLAN tag will be striped and the packet will be forwarded.
Hybrid			1. If the VLAN ID carried in the packet is the UNTAG VLAN ID the port allows to pass through, the VLAN tag will be striped and the packet will be forwarded. 2. If the VLAN ID carried in the packet is the TAG VLAN ID the port allows to

		be accepted. Otherwise, the packet will be discarded.	pass through, the VLAN tag will remain and the packet will be forwarded.
Trunk			When the VLAN ID carried in a packet is the VLAN ID that the port allows to pass through:: 1. If the VLAN ID is not consistent with the port PVID, VLAN tag will be remained and the packet will be forwarded. 2. If the VLAN ID is consistent with the port PVID, VLAN tag will be stripped and the packet will be forwarded.

Configure interface vlan mode

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter Interface configuration mode	**interface ethernet** *interface-num*	
Configure interface vlan mode	**port mode {** access | hybrid | trunk **}**	Hybrid by default.

8.2.3 VLAN Attributes Based on Hybrid Interface

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter Interface configuration mode	**interface ethernet** *interface-num*	
Configure interface vlan mode	**port mode hybrid**	

Allow the specified vlan to pass through this hybrid port	**port hybrid** { **tagged** | **untagged** } **vlan** { *vlan-list* | *all* }	"tagged" means that the vlan packet carries tag; "untagged" means that the vlan packet does not carry tag;
Does not allow the specified vlan to pass this hybrid port	**undo port hybrid vlan** *vlan-list*	

8.2.4 VLAN Attributes Based on Trunk Interface

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter Interface configuration mode	**interface ethernet** *interface-num*	
Configure interface vlan mode	**port mode trunk**	
Allow the specified vlan to pass through this trunk port	**port trunk allowed vlan** { *vlan-list* | *all* }	

Do not allow the specified vlan to pass through this trunk port	**undo port trunk allowed vlan** { *vlan-list* | *all* }	

8.2.5 Configure Port Priority

If Switch receives a untagged packet, system will add a vlan tag to the packet in which the vid value in the tag is the PVID value and the priority value is the port priority value.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter Interface configuration mode	**interface ethernet** *interface-num*	
Configure port priority	**priority** *value*	
Restore default priority	**undo priority**	0 by default
Display the port detailed configurations	**display interface ethernet** *interface-num*	
Display the port brief configurations	**display interface brief ethernet** [*interface-num*]	

8.2.6 Configure Ingress Filtering

By default, interface will check whether the receiving packet belongs to the vlan, if it does, the

interface will perform the forward processing. Otherwise, it will discard the packet. This process is called ingress filtering. Switch will enable this function by default and this function is allowed to be disabled.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter Interface configuration mode	**interface ethernet** *interface-num*	
Configure ingress filtering	[**undo**] **ingress filtering**	Enabled by default
Display the configuration information	**Displayress** [**interface** *interface-num*]	

8.2.7 Configure Types of Interface Acceptable-frame

By default, regardless of any type of packet (tag or untag) received by the Switch, it is allowed to change the port to receive only tag packets.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter Interface configuration mode	**interface ethernet** *interface-num*	
Configure interface priority	**ingress acceptable-frame** { **all** | **tagged** }	“all” means it can receive the tag packets and untag packets;

		“tagged” means it can only receive the tag packets.
Display the configuration information	**display ingress** [**interface** *interface-num*]	

8.2.8 Display VLANconfiguration

Operation	Command	Remarks
Display VLANconfiguration by vlanid	**display vlan** [*vlan-id*]	
Display VLAN configuration by brief	**display vlan brief**	
Display VLAN configuration by interface	**display vlan interface** [ethernet*interface-num*]	

8.3 Configure MAC-Based VLAN

8.3.1 MAC-Based VLAN Overview

As noted earlier, a single port in the campus network has multiple services, and each service belongs to different VLANs. So the flexible configuration of VLAN under the Switch port to identify different services has become a key issue of the campus network management.

In order to solve the above-mentioned problems, the MAC-based VLAN is proposed. MAC (Media Access Control) address is burnt on a Network Interface Card (NIC), also known as the hardware address. It’s composed of 48 bits long (6 bytes), 16 hex digits.

MAC-based VLAN is another way to distinguish VLAN that tag of VLAN is added to packet according to the source MAC address. This is often in combination with security technologies (such as 802.1X) to achieve the purpose of the terminal's safety and flexible access.

8.3.2 ConfigureMAC-Based VLAN

Users should bind the terminal MAC address with VLAN via the command line, and the device will generate a corresponding MAC VLAN table.

The implementation of this approach is simple, only involved in access equipment. But in this way, it is necessary to manually configure the MAC VLAN of the terminal on terminal accessable ports. It was a big project.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure static vlan-mac table	**mac-vlan mac-address** *mac-address vlan* [*priority*]	
Delete vlan-mac table	**undo mac-vlan** [**mac-address** *mac-address*]	
Display vlan-mac table	**display vlan-mac-table** [*mac-address*]	

8.4 Configure Protocol-Based VLAN

8.4.1 Protocol-Based VLAN Overview

Protocol-based VLAN: the packet distributes different VLAN ID according to the receiving

protocol types and encapsulation formats. “Protocol types + encapsulation formats” is also called model agreement. One protocol vlan can be able to bind multiple model agreements. Different model agreements can be distinguished by the vlan-protocol table index. Agreement profile is referenced to the port, and then you can modify the packet vlan according to the model agreements.

Untagged packet processing (no vlan tag):

1. If the packet protocol types and encapsulation formats are conform to the model agreements, it will be tagged with the protocol vlan-id.
2. If the packet protocol types and encapsulation formats are not conforming to the model agreements, it will be tagged with the port default VLAN ID.

Tagged packet processing (has vlan tag):

1. If the packet protocol types and encapsulation formats are conform to the model agreements, the outer vlan information will be modified to be the protocol vlan-id.
2. If the packet protocol types and encapsulation formats are not conform to the model agreements, the processing mode will be the same as the port-based vlan.

This feature is mainly applied to bind the service type with VLAN, providing convenient management and maintenance.

There are two types’ configuration modes of protocol-based VLAN. Please choose the suitable one according to the equipment type.

8.4.2 ConfigureProtocol-Based VLAN

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Configure protocol profile	**protocol-vlan profile** *index* **frame-type** *eth-type*	
Delete protocol profile	**undo protocol-vlan profile** [*index*]	
Enter Interface configuration mode	**interface ethernet** *interface-num*	
Bind protocol-vlan profile	**protocol-vlan profile** *index* **vlan** *vlan-id* [priority *priority*]	
Undo bind protocol-vlan profile	**undo protocol-vlan profile** [*index*]	
Display protocol-vlan profile	**display protocol-vlan profile** [*index*]	
Display protocol-vlan profile bind	**display protocol-vlan interface** [ethernet *interface-num*]	

8.5 Configure IP-subnet VLAN

8.5.1 IP-subnet VLAN Overview

IP subnet-based vlan is divided according to packet source IP address and subnet mask. After device received packets from the interface, it will confirm the packets belonging to which VLAN and then automatically divide these packets to specified VLAN.

8.5.2 ConfigureIP-subnet VLAN

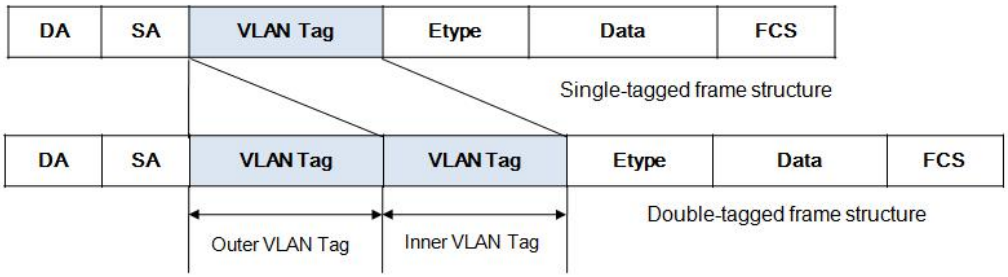
Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure ip-subnet-vlan table	**ip-subnet-vlan ipv4** *ip-address* **mask** *mask* **vlan** *vlanid* [priority *priority*]	
Delete ip-subnet-vlan table	**undo ip-subnet-vlan** [ipv4 *ip-address* mask *mask*]	
Enable the IP subnet-based VLAN	**ip-subnet-vlan precede**	
Disable the IP subnet-based VLAN	**undo ip-subnet-vlan precede**	
Display ip-subnet-vlan table	**display ip-subnet-vlan** [ipv4 *ip-address* mask *mask*]	

Chapter 9 QinQ

9.1 QinQ Overview

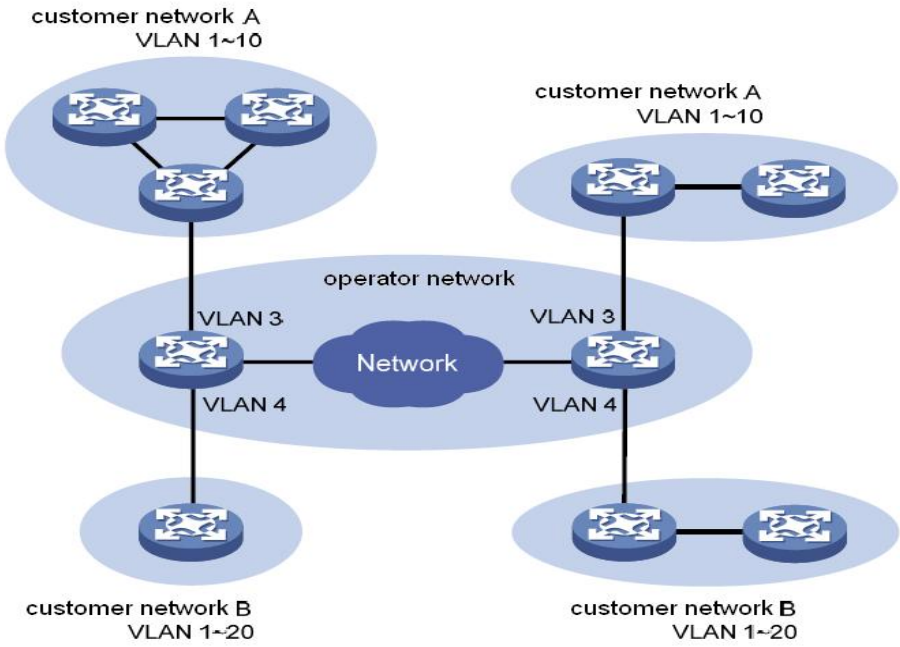
9.1.1 Understanding QinQ

In the VLAN tag field defined in IEEE 802.1Q, only 12 bits are used for VLAN IDs, so a Switch can support a maximum of 4,094 VLANs. In actual applications, however, a large number of VLANs are required to isolate users, especially in metropolitan area networks (MANs), and 4,094 VLANs are far from satisfying such requirements. shows the structure of 802.1Q-tagged and double-tagged Ethernet frames. The QinQ feature enables a device to support up to 4,094 x 4,094 VLANs to satisfy the requirement for the amount of VLANs in the MAN.



The port QinQ feature is a flexible, easy-to-implement Layer 2 VPN technique, which enables the access point to encapsulate an outer VLAN tag in Ethernet frames from customer networks (private networks), so that the Ethernet frames will travel across the service provider's backbone network (public network) with double VLAN tags. The inner VLAN tag is the customer network VLAN tag while the outer one is the VLAN tag assigned by the service

provider to the customer. In the public network, frames are forwarded based on the outer VLAN tag only, with the source MAC address learned as a MAC address table entry for the VLAN indicated by the outer tag, while the customer network VLAN tag is transmitted as part of the data in the frames.



9.1.2 Implementations of QinQ

There are two types of QinQ implementations: basic QinQ and Flexible QinQ.

1) Basic QinQ

Basic QinQ is implemented through VLAN VPN.

With the VLAN VPN feature enabled on a port, when a frame arrives at the port, the Switch will tag it with the port's default VLAN tag, regardless of whether the frame is tagged or untagged.

If the received frame is already tagged, this frame becomes a double-tagged frame; if it is an untagged frame, it is tagged with the port's default VLAN tag.

2) Flexible QinQ

Flexible QinQ is a more flexible, VLAN-based implementation of QinQ. If Flexible QinQ on port is enabled, Flexible QinQ can:

- For ingress packet, different outer vlan tag can be added according to different inner VLAN ID
- For ingress packet, new VLAN tag can take the place of some specific VLAN Tag
- For ingress packet, some VLAN can be transparent transmit.

For QinQ-enabled port, there are different handlings for different port type:

Uplink port: The Tag judgment on uplink port is based on the consistency between packet VID and configured global outer-tpid.

Custom port: The Tag judgment on customer port is based on the consistency between packet VID and inner-tpid. The default inner-tpid is 0x8100

9.1.3 Modification of TPID Value of QinQ Frames

A VLAN tag uses the tag protocol identifier (TPID) field to identify the protocol type of the tag. The value of this field, as defined in IEEE 802.1Q, is 0x8100. The device can identify whether there is corresponded VLAN Tag according to TPID. If configured TPID is the same as the corresponded field, packet is regarded as with VLAN Tag.

The systems of different vendors may set the TPID of the outer VLAN tag of QinQ frames to different values. For compatibility with these systems, the S5710-48 series Switches allow you to modify the TPID value so that the QinQ frames, when sent to the public network, carry the

TPID value identical to the value of a particular vendor to allow interoperability with the devices of that vendor.

The TPID in an Ethernet frame has the same position with the protocol type field in a frame without a VLAN tag. To avoid problems in packet forwarding and handling in the network, you cannot set the TPID value to any of the values in the table below.

Protocol type	**Value**
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E
GnLink	0x0765
GSTP	0X5524

9.2 Configure QinQ

9.2.1 QinQ Configuration Task List

Configuration Task	Description	Detailed Configuration
Configure BASIC QinQ	Required	9.2.2
Configure Flexible QinQ	Required	9.2.3
Display QinQ configuration	Optional	9.2.4

9.2.1 Configure BASIC QinQ

Perform following commands in privilege mode.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Enable basic QinQ	**qinq**	
Disable basic QinQ	**undo qinq**	

9.2.2 Configure Flexible QinQ

Perform following commands in privilege mode.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Modify outer TPID	**qinq** { inner-tpid | outer-tpid } *tpid-value*	
Add different outer VLAN Tag for different inner VID	**flexible-vlan insert** *start-vlan-id end-vlan-id service-vlan-idpriority*	

Configure vlan-swap	**flexible-vlan swap** *start-vlan-id end-vlan-id target-vlan-idpriority*	
Configure packet belonged to specified vlan range need not to add double VLAN Tag	**flexible-vlan pass-through** *start-vlan-id end-vlan-id*	

9.2.3 Display QinQ configuration

Operation	Command	Remarks
Display qinq configuration	**display flexible-vlan interface** [ethernet *interface-list*]	

Chapter 10 MAC Address Table

10.1 MAC Address Table Overview

The system maintains a MAC address table for forwarding packets. The entries in this table contain the device MAC addresses, VLAN IDs, and Switch port numbers. When a packet enters the Switch, the Switch looks up the MAC address table based on the destination MAC address of the packet and the VLAN ID of the packet. If the packet is found, the Switch sends the packets to the specified ports. Otherwise, Switch will broadcast the packets in this VLAN.

The system can be able to learn MAC address table. If the source MAC address of a received packet does not exist in the MAC address table, the system will add the source MAC address, VLAN ID, and port number of the received packet as a new entry to the MAC address table.

You can manually configure MAC address entries. The administrator can configure the MAC address table based on the actual network condition, that is, the administrator can add or modify static entries, permanent entries, blackhole entries, dynamic entries.

System provides MAC address aging function. If a device does not send any packets for a certain period of time, the system deletes the MAC address entries associated with the device. MAC address aging only takes effect on the learned MAC address or the MAC address entries which can be aged (the dynamic MAC address entries).

10.2 Configure MAC Address Table

10.2.1 MAC Address Table Configuration Task List

Configuration Task	Description	Detailed Configuration
Configure the Aging Time	Optional	10.2.2
Add MAC Address Table by Manual	Optional	10.2.3
Display MAC Address Table	Optional	10.2.4
Enable/Disable MAC Learning	Optional	10.2.5
Quantity Limitation on MAC Address Learning Table	Optional	10.2.6

10.2.2 Configure the Aging Time

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure the aging time of MAC address	**mac-address-table age-time** { *agetime* | disable }	*disable* means mac address will not be aged
Configure the default aging time of MAC address	**undo mac-address-table age-time**	300s by default
Display the aging time of MAC address	**display mac-address-table age-time**	
Display the aging time of MAC address	**display mac-address-table age-time**	

10.2.3 Add MAC Address Table by Manual

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure the static | permanent | dynamicmac-address	**mac-address-table** { **static** | **permanent** | **dynamic** } *mac-address* **interface ethernet** *interface-num* **vlan** *vlan-id*	

Configure the blackholemac-address	**mac-address-table blackhole** *mac-address* **vlan** *vlan-id*	
Delete the static | permanent | dynamicmac-address	**undo mac-address-table** [**dynamic** | **permanent** | **static**] *mac-address* **interface ethernet** *interface-num* **vlan** *vlan-id*	
Delete the blackholemac-address	**undo mac-address-table** [**blackhole** | **dynamic** | **permanent** | **static**] *mac-address* **vlan** *vlan-id*	
Delete the static | permanent | dynamicmac-address by port	**undo mac-address-table** [**static** | **permanent** | **dynamic**] **interface ethernet** *interface-num*	
Delete the blackholemac-address by port	**undo mac-address-table** [**blackhole** | **dynamic** | **permanent** | **static**] **vlan** *vlan-id*	
Delete all mac-address	**undo mac-address-table**	

10.2.4 Display MAC Address Table

Operation	Command	Remarks
Display all MAC address	**display mac-address-table**	
Display CPU MAC address	**display mac-address-table cpu**	
Display MAC address by mac	**display mac-address-table** *mac-address* [vlan *vlan-id*]	
Display MAC address by type	**display mac-address-table** { **static** |	

	dynamic | **permanent** | **blackhole** } [vlan *vlan-id*]	
Display MAC address by port	**display mac-address-table** { **static** | **dynamic** | **permanent** | **blackhole** } **interface ethernet** *interface-num* [vlan *vlan-id*]	
Display MAC address by vlan	**display mac-address-table vlan** *vlan-id*	

10.2.5 Enable/Disable MAC Learning

You can configure whether the device learns MAC addresses dynamically or not.

If MAC address learning is disabled under global configuration mode, all ports cannot learn MAC address; If you want to disable mac address learning on some ports, just enable MAC address learning under global configuration mode and disable MAC address learning on the port will be OK.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable global mac learning	**mac-address-table learning**	
Disable global mac learning	**undo mac-address-table learning**	
Enter interface configuration mode	**interface** { { ethernet *interface-num* } | interface-name }	
Enable mac learning	**mac-address-table learning**	

Disable mac learning	**undo mac-address-table learning**	
Display mac learning	**display mac-address learning** [interface ethernet [*interface-num*]]	

10.2.6 Quantity Limitation on MAC Address Learning Table

Under port configuration mode, you can configure the maximum number of learned MAC addresses on a port. By default, the number of MAC addresses learning table are unlimited.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter vlan configuration mode	**vlan** *vlan-id*	
Configure max-mac-count	**mac-address-table max-mac-count** *max-mac-count*	
Configure the default max-mac-count	**undo mac-address-table max-mac-count**	
Enter interface configuration mode	**interface** { { ethernet *interface-num* } | interface-name }	
Configure max-mac-count	**mac-address-table max-mac-count** *max-mac-count*	
Configure the default max-mac-count	**undo mac-address-table max-mac-count**	
Display the max-mac-count	**display mac-address max-mac-count** { interface ethernet [*interface-num*] | vlan *vlan-id* }	

Chapter 11 STP

11.1 STP Overview

Spanning Tree Protocol (STP) is applied in loop network to block some undesirable redundant paths with certain algorithms and prune the network into a loop-free tree, thereby avoiding the proliferation and infinite cycling of the packet in the loop network.

11.1.1 Protocol Packets of Spanning-Tree

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

STP identifies the network topology by transmitting BPDUs between STP-compliant network devices. BPDUs contain sufficient information for the network devices to complete the spanning tree calculation.

In STP, BPDUs come in two types:

Configuration BPDUs, used for calculating spanning trees and Maintain the spanning tree topology.

Topology change notification (TCN) BPDUs, used for notifying concerned devices of network topology changes, if any.

11.1.2 Basic Concepts in Spanning-Tree

Root Bridge

A tree network must have a root; hence the concept of “root bridge” has been introduced in STP.

There is one and only one root bridge in the entire network, and the root bridge can change alone with changes of the network topology. Therefore, the root bridge is not fixed.

Upon network convergence, the root bridge generates and sends out configuration BPDUs at a certain interval, and other devices just forward the BPDUs. This mechanism ensures topological stability.

Root Port

On a non-root bridge device, the root port is the port nearest to the root bridge. The root port is responsible for communication with the root bridge. A non-root-bridge device has one and only one root port. The root bridge has no root port.

Designated Bridge

For a device, Designated Bridge is the device directly connected with this device and responsible for forwarding BPDUs; For a LAN, Designated Bridge is the device responsible for forwarding BPDUs to this LAN segment.

Designated Port

For a device, Designated Port is the port through which the designated bridge forwards BPDUs to this device; For a LAN, Designated Port is the port through which the designated bridge forwards BPDUs to this LAN segment.

Path cost

Path cost is a reference value used for link selection in STP. By calculating the path cost, STP

selects relatively “robust” links and blocks redundant links, and finally prunes the network into loop-free tree structure.

11.1.3 Spanning-Tree Interface States

Each Layer 2 interface on a Switch using spanning tree exists in one of these states:

Disabled

The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

Blocking

The interface does not participate in frame forwarding.

Listening

The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.

Learning

The interface prepares to participate in frame forwarding.

Forwarding

The interface forwards frames.

An interface moves through these states:

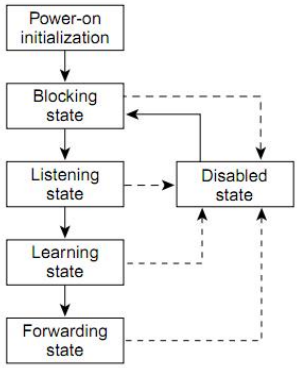
• From initialization to blocking

• From blocking to listening or to disabled

• From listening to learning or to disabled

• From learning to forwarding or to disabled

• From forwarding to disabled



When you power up the Switch, spanning tree is enabled by default, and every interface in the Switch, VLAN, or network goes through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

When the spanning-tree algorithm places a Layer 2 interface in the forwarding state, this process occurs:

1)The interface is in the listening state while spanning tree waits for protocol information to transition the interface to the blocking state.

2)While spanning tree waits the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.

3)In the learning state, the interface continues to block frame forwarding as the Switch learns end-station location information for the forwarding database.

4)When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

11.2 How Spanning-Tree Works

Spanning-Tree identifies the network topology by transmitting configuration BPDUs between network devices. Configuration BPDUs contain sufficient information for network devices to complete the spanning tree calculation. Important fields in a configuration BPDU include:

Root bridge ID: consisting of root bridge priority and MAC address.

Root path cost: the cost of the shortest path to the root bridge.

Designated bridge ID: designated bridge priority plus MAC address.

Designated port ID: designated port priority plus port name.

Message age: age of the configuration BPDU while it propagates in the network.

Max age: maximum age of the configuration BPDU maintained in the device.

Hello time: configuration BPDU interval.

Forward delay: forward delay of the port.

1) Specific calculation process of the STP algorithm

- Initial state

Upon initialization of a device, each port generates a BPDU with itself as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the local port.

- Selection of the optimum configuration BPDU

Each device sends out its configuration BPDU and receives configuration BPDUs from other devices.

The process of selecting the optimum configuration BPDU is as follows:

Step	Description
1	Upon receiving a configuration BPDU on a port, the device performs the following processing: If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device will discard the received configuration BPDU without doing any processing on the configuration BPDU of this port. If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device will replace the content of the configuration BPDU generated by the port with the content of the received configuration BPDU.
2	The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU.

- Selection of the root bridge

At network initialization, each STP-compliant device on the network assumes itself to be the root bridge, with the root bridge ID being its own device ID. By exchanging configuration BPDUs, the devices compare one another's root bridge ID. The device with the smallest root bridge ID is elected as the root bridge.

- Selection of the root port and designated ports

The process of selecting the root port and designated ports is as follows:

Selection of the root port and designated ports

Step	Description
1	A non-root-ridge device regards the port on which it received the optimum configuration BPDU as the root port.

2	Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of the rest ports. ● The root bridge ID is replaced with that of the configuration BPDU of the root port. ● The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost corresponding to the root port. ● The designated bridge ID is replaced with the ID of this device. ● The designated port ID is replaced with the ID of this port.
3	The device compares the calculated configuration BPDU with the configuration BPDU on the port of which the port role is to be defined, and does different things according to the comparison result: ● If the calculated configuration BPDU is superior, the device will consider this port as the designated port, and the configuration BPDU on the port will be replaced with the calculated configuration BPDU, which will be sent out periodically. ● If the configuration BPDU on the port is superior, the device will block this port without updating its configuration BPDU, so that the port will only receive BPDUs, but not send any, and will not forward data.

Once the root bridge, the root port on each non-root bridge and designated ports have been unsuccessfully elected, the entire tree-shaped topology has been constructed.

2) The BPDU forwarding mechanism in spanning-tree

Upon network initiation, every Switch regards itself as the root bridge, generates configuration BPDUs with itself as the root, and sends the configuration BPDUs at a regular interval of hello time.

- If it is the root port that received the configuration BPDU and the received configuration

BPDU is superior to the configuration BPDU of the port, the device will increase message age carried in the configuration BPDU by a certain rule and start a timer to time the configuration BPDU while it sends out this configuration BPDU through the designated port.

- If the configuration BPDU received on the designated port has a lower priority than the configuration BPDU of the local port, the port will immediately send out its better configuration BPDU in response.
- If a path becomes faulty, the root port on this path will no longer receive new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. In this case, the device will generate a configuration BPDU with itself as the root and sends out the BPDU. This triggers a new spanning tree calculation process so that a new path is established to restore the network connectivity.

However, the newly calculated configuration BPDU will not be propagated throughout the network immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data along the old path. If the new root port and designated port begin to forward data as soon as they are elected, a temporary loop may occur.

3) STP timers

STP calculations need three important timing parameters: forward delay, hello time, and max age.

- Forward delay is the delay time for device state transition. A path failure will cause re-calculation of the spanning tree, and the spanning tree structure will change

accordingly. However, the new configuration BPDU as the calculation result cannot be propagated throughout the network immediately. If the newly elected root port and designated ports start to forward data right away, a temporary loop is likely to occur. For this reason, as a mechanism for state transition in STP, a newly elected root port or designated port requires twice the forward delay time before transitioning to the forwarding state, when the new configuration BPDU has been propagated throughout the network.

- Hello time is the time interval at which a device sends hello packets to the surrounding devices to ensure that the paths are fault-free.
- Max age is a parameter used to determine whether a configuration BPDU held by the device has expired. A configuration BPDU beyond the max age will be discarded.

11.3 Implement RSTP on Ethernet Switch

The Ethernet Switch implements the Rapid Spanning Tree Protocol (RSTP), i.e., the enhancement of STP. The Forward Delay for the root ports and designated ports to enter forwarding state is greatly reduced in certain conditions, thereby shortening the time period for stabilizing the network topology.

To achieve the rapid transition of the root port state, the following requirement should be met: The old root port on this Switch has stopped data forwarding and the designated port in the upstream has begun forwarding data.

The conditions for rapid state transition of the designated port are:

- The port is an Edge port that does not connect with any Switch directly or indirectly. If the designated port is an edge port, it can Switch to forwarding state directly without immediately forwarding data.
- The port is connected with the point-to-point link, that is, it is the master port in aggregation ports or full duplex port. It is feasible to configure a point-to-point connection. However, errors may occur and therefore this configuration is not recommended. If the designated port is connected with the point-to-point link, it can enter the forwarding state right after handshaking with the downstream Switch and receiving the response.

The Switch that uses RSTP is compatible with the one using STP. Both protocol packets can be identified by the Switch running RSTP and used in spanning tree calculation.

11.4 Configure RSTP

11.4.1 RSTP Configuration Task List

Configuration Task	Description	Detailed Configuration
Enable STP and Configure the working mode	Required	11.4.2
Configure STP bridge priority	Optional	11.4.3
Configure Time Parameter	Optional	11.4.4
Configure STP Path Cost	Optional	11.4.5
Configure STP Port Priority	Optional	11.4.6
Configure STP mcheck	Optional	11.4.7
Configure STP point-to-point mode	Optional	11.4.8
Configure STP portfast	Optional	11.4.9

Configure STP transit limit	Optional	11.4.10
RSTP Monitor and Maintenance	Optional	11.4.11

11.4.2 Enable RSTP and Configure the Working Mode

After enabling STP globally, all ports will be defaulted to join the STP topology calculating by default. If some port is not allowed to take part in the STP calculation, administrator can use undo stp command in interface configuration mode to disable STP on this port.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable STP globally	**stp**	
Select STP mode	**stp mode rstp**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Enable/disable STP on port	[**undo**] **stp**	

Note：

When enable STP globally, the system is working under RSTP mode.

11.4.3 Configure STP Bridge Priority

The priority of bridge determines this Switch can be root or not. If this Switch is needed to be the root, the priority can be configured inferior.

By default, the Switch bridge priority is 32768.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure STP priority	**stp priority** *bridge-priority*	

11.4.4 Configure Time Parameter

There are three time parameters: Forward Delay, Hello Time and Max Age.

User can configure these three parameters for RSTP calculation.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure Hello-packet sending interval	**stp hello-time** *seconds*	
Configure STP forward-delay	**stp forward-time** *seconds*	
Configure STP max-age	**stp max-age** *seconds*	

Note:

Too long Hello Time may cause link failure thought by network bridge for losing packets of the link to restart accounting STP; too smaller Hello Time may cause network bridge frequently to send configuration packet to strengthen the load of network and CPU. Hello Time ranges from 1 to 10 seconds. It is suggested to use the default time of 2 seconds. Hello Time ≤ Forward Delay-2.

If Forward Delay is configured too small, temporary redundancy will be caused; if Forward Delay is configured too large, network will not be restored linking for a long time. Forward Delay ranges from 4 to 30 seconds. The default forward delay time, 15 seconds is suggested to use. Forward Delay≥Hello Time + 2.

Max Age is used to configure the longest aging interval of STP. Lose packet when over-timing. The STP will be frequently accounts and take crowded network to be link fault, if the value is too small. If the value is too large, the link fault cannot be known timely. Max Age is determined by diameter of network, and the default time of 20 seconds is suggested. 2*(Hello Time + 1) ≤

Max Age ≤ 2*(ForwardDelay – 1) When enable STP globally, the system is working under RSTP mode.

11.4.5 Configure STP Path Cost

Configure interface STP path cost and choose the path with the smallest path cost to be the effective path.

The path cost is related to the link speed rate. The larger the speed rate is, the less the cost is. STP can auto-detect the link speed rate of current interface and converse it to be the cost.

Configure port path cost will make STP re-calculating. The value of the path cost is 1-65535. It is suggested using the default vaule, which makes the STP to calculate the current port cost by itself. By default, the path cost is determined by the current port speed.

When the port is 10M, the default cost is 200,000; when the port is 100M, the default cost is 20,000; 1000M, 2,000.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Configure STP path cost	**stp cost** *path-cost*	

11.4.6 Configure STP Port Priority

Specify specified port in STP by Configure port priority. Generally, the smaller the value is, the superior the priority is, and the port will be more possible to be included in STP. If the priorities are the same, the port number is considered.

The smaller the value is, the superior the priority is, and the port is easier to be the root

interface. Change the port priority may cause the re-calculating of the STP. The port priority ranges from 0 to 255. The default port priority is 128.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Configure STP port priority	**stp port-priority** *port-priority*	

11.4.7 Configure STP Mcheck

Switch working under RSTP mode can be connected to Switch with STP. But when the neighbor is working under RSTP, the two connected ports are still work under STP mode. Mcheck is for force port sending RSTP packet to make sure the two neighbor ports can be working under RSTP. If yes, the working mode will turn to be RSTP.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Configure STP mcheck	**stp mcheck**	

11.4.8 Configure STP Point-to-Point Mode

In rstp, the requirement of interface quickly in transmission status is that the interface must be point to point link not media sharing link. It can be specified interface link mode manually and can also judge it by network bridge.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Enter interface configuration mode	**interface ethernet** *interface-num*	
Configure Switch auto-check the point-to-point	**stp point-to-point auto**	
Configure STP point-to-point mode forcetrue	**stp point-to-point forcetrue**	
Configure STP point-to-point mode forcefalse	**stp point-to-point forcefalse**	

11.4.9 Configure STP Portfast

Edge port is the port connecting to the host which can be in transmission status in very short time after linkup, but once the port receiving STP packet, it will shift to be non-edge port.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Configure STP portfast	**stp portfast**	

11.4.10 Configure STP Transit Limit

Restrict STP occupying bandwidth by restricting the speed of sending BPDU packet. The speed is determined by the number of BPDU sent in each hello time.

By default, port will send 3 BPDU packets in every Hello time interval.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Configure STP transit limit	**stp transit-limit** *transit-limit*	

11.4.11 RSTP Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Operation	Command	Remarks
Display STP interface	**display stp interface** [brief [ethernet *interface-num*]]	

Chapter 12 MSTP

12.1 MSTP Overview

The multiple spanning tree protocol (MSTP) overcomes the shortcomings of STP and RSTP. In addition to support for rapid network convergence, it also allows data flows of different VLANs to be forwarded along their own paths, thus providing a better load sharing mechanism for redundant links. For description about VLANs, refer to VLAN.

12.2 Configure MSTP

12.2.1 Enable MSTP and Configure the Working Mode

After the tree starts to give birth to a global default for all ports will participate in the spanning tree topology is calculated, if an administrator wants some of the port does not participate in the calculation of the production tree, or go to the specified port configuration mode, use the undo stp to disable the port Spanning Tree function.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Choice STP mode	**stp mode mstp**	
Enable STP	**stp**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Enable(disable) port STP	(**undo**) **stp**	

12.2.2 Configure MSTP Timer Parameter Values

MSTP timers include: forwarding delay, contracting cycle hello time, maximum aging time, and the maximum hops. Users can configure these three parameters on the Switch for MSTP spanning tree.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure bridge forward delay	**stp mst forward-time** *forward-time*	
Configure bridge hello time	**stp mst hello-time** *hello-time*	
Configure bridge max aging time	**stp mst max-age** *max-age*	
Configure bridge max hops	**stp mst max-hops** *max-hops*	

Notes:

- The Hello Time value is too long will lead to packet loss due to leaving the bridge that links the link failure, began to re-calculate the spanning tree; too short can cause the bridge Hello Time value configured to send messages frequently to increase the network and CPU burden. Hello Time value range is 1 to 10 seconds, recommended default value of 2 seconds. Hello Time must be less than equal to the Forward Delay 2.
- If the Forward Delay configuration is too small, may introduce temporary redundant paths; if the Forward Delay configuration is too large, the network may not be a long time to restore connectivity. Forward Delay value range is 4 to 30 seconds, it is recommended to use the default value of 15 seconds. Forward Delay time must be greater than equal to the Hello Time + 2.
- Max Age is used to set the MSTP protocol packet aging longest interval, if the timeout, it

discards the packet. If this value is too small, spanning tree will be more frequent, there may be network congestion mistaken link failure; If this value is too large, is not conducive to timely detection of link failures. Max Age of the range is 6 to 40 seconds. Max Age time value and the exchange of the network diameter. Recommended default value of 20 seconds. Max Age time must be greater than equal to 2 * (Hello Time + 1), less than or equal 2 * (Forward Delay-1).

12.2.3 Configure MSTP Identifier

MSTP configuration identifiers include: MSTP configuration name, MSTP revision level, and the MSTP instance and VLAN mapping, MSTP will have the same configuration identifier and the bridge connected to each other logically be treated as a virtual bridge.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure MSTP identifier name	**stp mst name** *name*	
Configure MSTP identifiers revision	**stp mst revision** *revision-level*	
Configure MSTP instance configuration and VLAN identifier mapping	**stp mst instance** *instance-num* **vlan** *vlan-list*	

12.2.4 Configure MSTP Bridge Priority

In MSTP, the bridge priority is based on the parameters of MSTI, the bridge priority together with port priority and port path cost determines the topology of each spanning tree instance, constitute the basis for link load balancing.

Switch bridge priority determines the size of this Switch is able to be selected as the spanning tree root bridge. By Configure the bridge priority of the smaller, you can specify a Switch to

become the spanning tree root bridge purposes.

By default, the Switch bridge priority is 32768.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure MSTP instance priority	**stp mst instance** *instance-num* **priority** *priority*	

12.2.5 ConfiConfigure Root Port Protection

As the maintenance of configuration errors or malicious network attacks, network valid root bridge may receive a higher priority configuration information, so the root bridge will lose the current status of the root bridge, causing changes in network topology errors .Assuming the original traffic is forwarded through the high-speed links, this is not legally change will lead to the original high-speed links are to low-speed traffic links, resulting in network congestion. Root protection function to prevent this from happening.

Root-protection function of the port, the port can only be kept for a specified port. Once this port received a high priority on the configuration information, status of the ports will be set to the Discarding state, not forwarding packets (equivalent to the link connected to this port is disconnected).When a long enough period of time does not receive better configuration message, the port will revert to the original state.

In MSTP, this function works for all instances.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configure the root port protection	**stp mst root-guard**	

12.2.6 Configure Digest Snooping Port

When a Switch port uses a proprietary spanning tree with Cisco and other Switch is connected, these manufacturers' Switches configured with the proprietary spanning tree protocol, even if the same MST region configuration, the Switch can't be achieved between the MSTP domain interoperability. Digest snooping feature such a situation. With the use of proprietary spanning tree protocol of the manufacturer's Switches connected to the port on the digest snooping feature, when receiving the manufacturer's Switches over to send a BPDU, the Switch that is from the same packet in an MST region, while the configuration summary record; when BPDU packets sent to these manufacturer's Switches, the Switch configuration summary to supplement it. This Switch is realized and the manufacturer's Switches in the MSTP region exchange.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configure digest snooping port	**stp mst config-digest-snooping**	

12.2.7 Configure Port mCheck Function

In order to flexibly control MSTP, you can open the DISABLE INSTANCE features, disable instance STP mode operating results with the implementation of no spanning-tree similar to the instance of the VLAN mapping of all connections on port forwarding state.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configuration port mcheck function	**stp mcheck**	

Note:

mcheck function is a prerequisite for the port must send BPDU packets, so only works on the

specified port.

12.2.8 Configure MSTP Instance Is Enabled

In order to flexibly control MSTP, you can open the DISABLE INSTANCE features, disable instance STP mode operating results with the implementation of no spanning-tree similar to the instance of the VLAN mapping of all connections on port forwarding state.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Disable MSTP instance	**stp mst disable instance** *instance-number*	
Enable MSTP instances	**undo stp mst disable instance** *instance-number*	

12.2.9 Display and Maintain MSTP

After completing the above configuration, can use the following command to view configuration. RSTP.

Operation	Command	Remarks
MSTP configuration information display identifier	**display stp mst config-id**	
Display spanning tree instance and port configuration information	**display stp mst instance** [brief [*instance-list*]]	

Chapter 13 Remote-loop-detect

13.1 Remote-loop-detect Overview

The device is connected with the client. If there is a loop in the client network, which will affect the entire network. Remote-loop-detect is to solve this problem. After the Remote-loop-detectis enabled on the Switch port, the Switch periodically sends a detection message. If the client network has a loop, the Switch receives the detection message from the Switch. In this case, the Switch considers that the client network exists loop, and the port connected to the client port according to the treatment strategy placed discarding or shutdown.

Some people may ask, the spanning tree can also be remote loop detection, why need Remote-loop-detect? This is because if the client network also has equipment to open spanning tree, the client network topology change easily affects the network of the room. The general networking is to connect the client port which does not open the spanning tree, with remote-loop-detectalternative.

13.2 Configure Remote-loop-detect

13.2.1 Enable Remote-loop-detect

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	

Enable remote-loop-detect	**stp remote-loop-detect interface** [ethernet [interface-list]]	
Disable remote-loop-detect	**undo stp remote-loop-detect interface** [ethernet [interface-list]]	
Enter the interface configuration mode.	**interface** { { ethernet *interface-num* } | interface-name }	
Enable remote-loop-detect	**stp remote-loop-detect**	
Disable remote-loop-detect	**undo stp remote-loop-detect**	

13.2.2 Configure the Processing Policy

When Remote-loop-detectdetects the existence of loop, there are two ways: one is discarding the port, the other is the port shutdown, and then periodically restores the port; the default use discarding.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Configure the processing policy	**stp remote-loop-detect action** { shutdown | discarding }	Discarding by default

13.2.3 Configure the Interval Timer

Operation	Command	Remarks

Enter the global configuration mode.	**system-view**	
Configure the processing policy	**stp remote-loop-detect interval-time** *interval-time*	5s by default

13.2.4 Configure the Recovery Timer

When Remote-loop-detectdetects that a loop exists and the shutdown command is used, the shutdown port periodically recovers the corresponding port. The default recovery period is 20 seconds and can be modified as needed. If it is configured as 60s, it means that it will not be automatically restored. User needs to manually run the shutdown / no shutdown command on the port. The port can re-linkup.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Configure the shutdown processing policy	**stp remote-loop-detect action shutdown**	
Configure the recovery time of the port	**stp remote-loop-detect recover-time** *recover-time*	

13.2.5 Display Remote-loop-detect Configuration

Operation	Command	Remarks
Displayremote-loop-detectConfiguration	**display stp remote-loop-detect interface** [ethernet [interface-list]]	

Chapter 14 ACL

14.1 ACL Overview

14.1.1 ACL Overview

As network scale and network traffic are increasingly growing, network security and bandwidth allocation become more and more critical to network management. Packet filtering can be used to efficiently prevent illegal users from accessing networks and to control network traffic and save network resources. Access control lists (ACL) are often used to filter packets with configured matching rules.

ACLs are sets of rules (or sets of permit or deny statements) that decide what packets can pass and what should be rejected based on matching criteria such as source MAC address, destination MAC address, source IP address, destination IP address, and port number.

When an ACL is assigned to a piece of hardware and referenced by a QoS policy for traffic classification, the Switch does not take action according to the traffic behavior definition on a packet that does not match the ACL.

ACL according to application identified by ACL numbers, fall into three categories,

Basic ACL: Source IP address

Extended ACL: Source IP address, destination IP address, protocol carried on IP, and other Layer 3 or Layer 4 protocol header information

Layer 2 ACL: Layer 2 protocol header fields such as source MAC address, destination MAC address, 802.1p priority, and link layer protocol type.

14.2 ACL Configuration

14.2.1 ACL Configuration List

Configuration Task	Description	Detailed Configuration
Configure Match Order	Optional	14.2.2
Configure Time Range	Optional	14.2.3
Configure Basic ACL	Required	14.2.4
Configure Extended ACL	Required	14.2.5
Configure Layer 2 ACL	Required	14.2.6
Activate ACL	Required	14.2.7
Display and Debugging ACL	Optional	14.2.8

14.2.2 Configure Match Order

An ACL consists of multiple rules, each of which specifies different matching criteria. These criteria may have overlapping or conflicting parts. This is where the order in which a packet is matched against the rules comes to rescue.

Two match orders are available for ACLs:

config: where packets are compared against ACL rules in the order in which they are configured.

auto: where depth-first match is performed. The term depth-first match has different meanings for different types of ACLs. Depth-first match for a basic ACL

For example, now Configure 2 types of ACL as below:

[Switch]acl 2000 deny any

Config ACL subitem successfully.

[Switch]acl 2000 permit 1.1.1.1 0

Config ACL subitem successfully.

1) If it is the configuration mode, sub-item 0 is the first command. You can see as below configuration:

[Switch]display acl config 1

Standard IP Access List 1, match-order is config, 2 rule:

0 deny any

1 permit 1.1.1.1 0.0.0.0

2) If it is the auto mode, sub-item 0 is the longest ACL match rule. You can see as below configuration:

[Switch]display acl config 1

Standard IP Access List 1, match-order is auto, 2 rule:

0 permit 1.1.1.1 0.0.0.0

1 deny any

Notes, ACL must enable. Switches must obey “first enable then active. Please refer to Chapter 1.6 for detailed configuration.

14.2.3 Configure Time Range

There are two kinds of configuration: configure absolute time range and periodic time range. Configure absolute is in the form of year, month, date, hour and minute. Configure periodic time range is in the form of day of week, hour and minute.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
new build time range and enter time range mode	**time-range** *name*	
Configure absolute start	**absolute start** *HH:MM:SS YYYY/MM/DD* [**end** *HH:MM:SS YYYY/MM/DD*]	
Configure periodic start	**periodic** *days-of-the-weekhh:mm:ss* **to** [*day-of-the-week*] *hh:mm:ss*	

Note:

Periodic time range created using the time-range time-name start-time to end-time days command. A time range thus created recurs periodically on the day or days of the week.

Absolute time range created using the time-range time-name {from time1 date1 [to time2 date2] | to time2 date2 } command. Unlike a periodic time range, a time range thus created does not recur. For example, to create an absolute time range that is active between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the time-range test from 00:00

01/01/2004 to 23:59 12/31/2004 command.

Compound time range created using the time-range time-name start-time to end-time days { from time1 date1 [to time2 date2] | to time2 date2 } command. A time range thus created recurs on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the time-range test 12:00 to 14:00 Wednesday from 00:00 01/01/2004 to 23:59 12/31/2004 command.

You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.

With no start time specified, the time range is from the earliest time that the system can express (that is, 00:00 01/01/1970) to the end time. With no end time specified, the time range is from the time the configuration takes effect to the latest time that the system can express (that is, 24:00 12/31/2100).

Up to 256 time ranges can be defined.

Configuration Examples

Create an absolute time range from 16:00, Jan 3, 2009 to 16:00, Jan 5, 2009

```
<Switch>system-view
[Switch]time-range b
Config time range successfully.
 [Switch-timerange-b]absolute start 16:00:00 2009/1/3 end 16:00:00 2009/1/5
Config absolute range successfully .
```

[Switch-timerange-b]display time-range name b

Current time is: 02:46:43 2009/01/31 Saturday
time-range: b (Inactive)

absolute: start 16:00:00 2009/01/03 end 16:00:00 2009/01/05

Create a periodic time range that is active from 8:00 to 18:00 every working day.

<Switch>system-view

[Switch]time-range b

Config time range successfully.
[Switch-timerange-b]periodic weekdays 8:00:00 to 18:00:00
Config periodic range successfully .
[Switch-timerange-b]display time-range name b
Current time is: 02:47:56 2009/01/31 Saturday

time-range: b (Inactive)

periodic: weekdays 08:00 to 18:00

14.2.4 Configure Basic ACL

Switch support ACL as below:

1)Basic ACL

2)Extended ACL

3)Layer 2 AC

Basic ACLs filter packets based on source IP address. They are numbered in the range 1 to 99. At most 99 ACL with number mark and at most 1000 ACL with name mark. At most 128 rules for each ACL at the same time. If you want to reference a time range to a rule, define it with the

time-range command first.

Follow these steps to configure a basic ACL.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Define sub-item match rule	**acl** *num* **match-order** { **config** | **auto** }	Bydefault ,system is config
Define basic ACL	**acl** *num* { **permit** | **deny** } { *source-IPv4/v6 source-wildcard* | **any** | **ipv6any** } [**time-range** *name*]	

Configure basic ACL based on name identification

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Define sub-item match rule	**acl standard** *name* **match-order** { **config** | **auto** }	by default,system is config
Define basic ACL and enter configuration mode	**acl standard** *name*	
Configure ACL rule	{ **permit** | **deny** } { *source-IPv4/v6 source-wildcard* | **any** | **ipv6any** } [**time-range** *name*]	

Configure Examples

!Define a basic ACL with number mark to deny packet with source IP 10.0.0.1

<Switch>system-view

[Switch]acl 1 deny 10.0.0.1 0

!Define a basic ACL with name mark to deny packet with source IP 10.0.0.2

<Switch>system-view

[Switch]acl standard stdacl

[Switch-std-nacl-stdacl]deny 10.0.0.2 0

14.2.5 Configure Extended ACL

Switch can define at most 100 extended ACL with the number ID (the number is in the range of 100 to 199), at most 1000 extended ACL with the name ID. It can define 128 sub-rules for an ACL (this rule can suit both ACL with name ID and number ID).

Follow these steps to configure a extended ACL.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	-
Define sub-item match rule	**acl** *num* **match-order** { **config** | **auto** }	by default ,system is config
Define extended ACL	**acl** *num* { **permit** | **deny** } [*protocol*] [**established**] { *source-IPv4/v6 source-wildcard* | **any** | **ipv6any** } [*port* [*portmask*]] { *dest- IPv4/v6 dest-wildcard* | **any** | **ipv6any** } [*port* [*portmask*]] { [**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*] } [**time-range** *name*]	required

Configure extended ACL based on name identification

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Define subitem match rule	**acl extended** *name* **match-order** { **config** | **auto** }	
		by

		default ,system is config
Define extended ACL and enter configuration mode	**acl extended** *name*	
Configure ACL rule	{ **permit** | **deny** } [*protocol*] [**established**] { *source-IPv4/v6 source-wildcard* | **any** | **ipv6any** } [*port* [*portmask*]] { *dest-IPv4/v6 dest-wildcard* | **any** | **ipv6any** } [*port* [*portmask*]] { [**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*] } [**time-range** *name*]	

Detailed parameters of extended ACL as below Table:

Parameters	Function	Remark
protocol	IP protocol type carried	A number in the range of 1 to 255. Represented by name, you can select GRE, ICMP, IGMP, IPinIP, OSPF, TCP, UDP
source-IPv4/v6	ACL rules specified the source address information	source-IPv4/v6 used to determine the packet's source IP address. Dotted decimal notation;
source-wildcard		sour-wildcard of 0 means

		that the host address
any		any source address.
dest-IPv4/v6	The purpose of ACL rules specified address information	dest-IPv4/v6 used to determine the packet destination address, in dotted decimal notation;
dest-wildcard | any		dest-wildcard is 0, the host address; Any is any destination address.
port	TCP / UDP port number	——
precedence	priority precedence message	IP precedence values range from 0 to 7
tos	tos priority packets	ToS priority ranges from 0 to 15
dscp	DSCP priority	Rule applies only to non-first fragment packet effective
	Level ranges from 0 to 63	
	fragment fragmentation information	
name	Create a time range	——

Configuration Examples

!Create extended ACL based on digital identification to deny the FTP packets with source

address 10.0.0.1 .
<Switch>system-view

[Switch]acl 100 deny tcp 10.0.0.1 0 ftp any

!Create extended ACL based on name identification to deny the FTP packets with source address 10.0.0.1.
<Switch>system-view
[Switch]acl extended extacl

[Switch-ext-nacl-extacl] deny tcp 10.0.0.2 0 ftp any

14.2.1 Configure Layer 2 ACL

Switch can define at most 100 layer 2 ACL with the number ID (the number is in the range of 200 to 299), at most 1000 layer 2 ACL with the name ID. It can define 128 sub-rules for an ACL (this rule can suit both ACL with name ID and number ID). Layer 2 ACL only classifies data packet according to the source MAC address, source VLAN ID, layer protocol type, layer packet received and retransmission interface and destination MAC address of layer 2 frame head of data packet and analyze the matching data packet.

Follow these steps to configure a Layer 2 ACL.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Define sub-item match rule	**acl** *num* **match-order** { **config** | **auto** }	by default ,system is config
Define Layer 2 ACL	**acl** *num* { **permit** | **deny** } [*protocol*] [**cos**	

	vlan-pri] **ingress** { { [*source-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** *interface-num*] } | **any** } **egress** { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-num* | **cpu**] } | **any** } [**time-range** *name*]	

Configure Layer 2 ACL based on name identification

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Define sub-item match rule	**acl link** *name* **match-order** { **config** | **auto** }	By default , system is config
Define Layer 2 ACL and enter configuration mode	**acl link** *name*	
Configure ACL rule	{ **permit** | **deny** } [*protocol*] [**cos** *vlan-pri*] **ingress** { { [*source-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** *interface- num*] } | **any** } **egress** { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-num* | **cpu**] } | **any** } [**time-range** *name*]	

Configuration Examples

!Create Layer 2 ACL based on digital identification to deny the MAC with ARP address 00:00:00:00:00:01.

<Switch>system-view

[Switch]acl 200 deny arp ingress 00:00:00:00:00:01 0 egress any

!Create Layer 2 ACL based on name identification to deny the MAC with ARP address 00:00:00:00:00:02.

<Switch>system-view

[Switch]acl link lnkacl

[Switch-link-nacl-lnkacl] deny arp ingress 00:00:00:00:00:02 0 egress any

14.2.2 Activate ACL

Switch obey the rule of "**First enable then active**"

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Active ACL	**access-group** [**ip-group** *name*|*num*] [**subitem** *num*] [**link-group** *name* | *num*] [**subitem** *num*]	

Configuration Examples

Switches only permit with source IP address 1.1.1.1

!Before configuration

[Switch]display acl config 1

Standard IP Access List 2, match-order is config, 2 rule:

0 deny any

1 permit 1.1.1.1 0.0.0.0

!Configuration steps

[Switch]access-group ip-group 1 subitem 1

Activate ACL successfully .

[Switch]access-group ip-group 1 subitem 0

Activate ACL successfully .

!Before configuration

[Switch]display acl config 1

Standard IP Access List 1, match-order is auto, 2 rule:

0 permit 1.1.1.1 0.0.0.0

1 deny any

!Configuration steps

[Switch]access-group ip-group 1

Activate ACL successfully .

Active ACL Binding

IP+MAC+Port binds through ACL binding active.

!Configuration request

MAC is 00:00:00:00:00:01, IP address of 1.1.1.1,the user can only enter from e0/0/1 mouth.

!Configuration steps

[Switch]acl 1 permit 1.1.1.1 0

[Switch]acl 200 permit ingress 00:00:00:00:00:01 0 interface ethernet 0/0/1 egress any

[Switch]acl 210 deny ingress any egress any

[Switch]access-group ip-group 1 link-group 200

[Switch]access-group link-group 210

14.2.3 Display and Debugging ACL

After finishing above configuration, you can see configuration as below commands.

Operation	Command	Remarks

Display ACL statistics	**display acl config statistic**	
Display ACL configuration	**display acl config** { **all**|*num* | **name** *name* }	
Display ACL runtime information	**display acl runtime** { **all** | *num* | **name** *name* }	

Chapter 15 QOS

15.1 QOS Overview

In traditional IP networks, packets are treated equally. That is, the FIFO (first in first out) policy is adopted for packet processing. Network resources required for packet forwarding is determined by the order in which packets arrive. All the packets share the resources of the network. Network resources available to the packets completely depend on the time they arrive. This service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, jitter, packet loss ratio, reliability, and so on.

With the fast development of computer networks, more and more networks are connected into Internet. Users hope to get better services, such as dedicated bandwidth, transfer delay, jitter voice, image, important data which enrich network service resources and always face network congestion. Internet users bring forward higher requirements for QoS. Ethernet technology is the widest network technology in the world recently. Now, Ethernet becomes the leading technology in every independent LAN, and many LAN in the form of Ethernet have become a part of internet. With the development of Ethernet technology, Ethernet connecting will become one of main connecting for internet users. To execute end-to-end QoS solution has to consider the service guarantee of Ethernet QoS, which needs Ethernet device applies to

Ethernet technology to provide different levels of QoS guarantee for different types of service flow, especially the service flow highly requiring delay and jitter.

15.1.1 Traffic

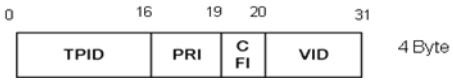
Traffic means all packets through Switch.

15.1.2 Traffic Classification

Traffic classification is to identify packets conforming to certain characters according to certain rules. It is the basis and prerequisite for proving differentiated services. A traffic classification rule can use the precedence bits in the type of service (ToS) field of the IP packet header to identify traffic with different precedence characteristics. A traffic classification rule can also classify traffic according to the traffic classification policy set by the network administrator, such as the combination of source address, destination address, MAC address, IP protocol, or the port numbers of the application. Traffic classification is generally based on the information in the packet header and rarely based on the content of the packet.

15.1.3 Priority

1) 802.1p priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet header does not need analysis but QoS must be assured at Layer 2. As shown in the chapter of VLAN configuration. Each host supported 802.1Q protocol forwards packets which are from Ethernet frame source address add a 4-byte tag header.

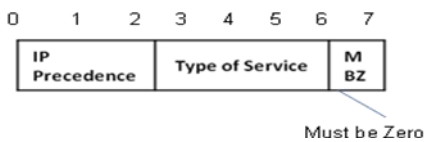


As shown in the figure above, PRI segment is 802.1p priority. It consists of 3bits whose range from 0~7. The three bits point the frame priority. The tag including 8 formats gives the precedence to forward the packets.

cos (decimal)	cos (binary)	Description
0	000	spare
1	001	background
2	010	best-effort
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

2) IP precedence, TOS precedence, and DSCP values

The TOS field in the IP header contains eight bits: the first three bits represent IP precedence; the subsequent four bits represent a ToS value and 1 bit with currently unused defaults 0. The four bits of TOS packets are grouped into four classes: the smallest time delay, maximum rate, highly reliability, minimum cost. Only 1 bit can be set, if the DSCP values equal 0, that means normal service.



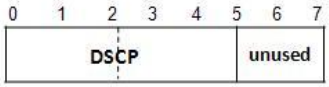
IP precedence contains 8 formats.

IP Precedence (decimal)	IP Precedence (binary)	Description
0	000	routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

TOS precedence contains 5 formats.

TOS (decimal)	TOS (binary)	Description
0	0000	normal
1	0001	min-monetary-cost
2	0010	max-reliability
4	0100	max-throughput
8	1000	min-delay

According to RFC 2474, the ToS field is redefined as the differentiated services (DS) field, where a DSCP value is represented by the first six bits (0 to 5) and ranges from 0 to 63. The remaining two bits (6 and 7) are reserved.



In a network in the Diff-Serve model, traffic is grouped into the following classes, and packets are processed according to their DSCP values

Expedited forwarding (EF) class: In this class, packets are forwarded regardless of link share of other traffic. The class is suitable for preferential services requiring low delay, low

packet loss, low jitter, and high bandwidth.

Assured forwarding (AF) class: This class is divided into four subclasses (AF 1 to AF 4), each containing three drop priorities for more granular classification. The QoS level of the AF class is lower than that of the EF class.

Class selector (CS) class: This class is derived from the IP ToS field and includes eight subclasses.

Best effort (BE) class: This class is a special CS class that does not provide any assurance. AF traffic exceeding the limit is degraded to the BE class. All IP network traffic belongs to this class by default.

DSCP (decimal)	DSCP (binary)	keys
0	000000	be
46	101110	ef
10	001010	af1
18	010010	af2
26	011010	af3
34	100010	af4
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7

15.1.4 Access Control List

To classify flow is to provide service distinctively which must be connected resource distributing. To adopt which kind of flow control is related to the stage it is in and the current load of the network. For example: monitor packet according to the promised average speed rate when the packet is in the network and queue scheduling manage the packet before it is out of the node.

15.1.5 Packet Filtration

Packet filtration is to filtrate service flow, such as deny, that is, deny the service flow which is matching the traffic classification, and permit other flows to pass. System adopts complicated flow classification to filtrate all kinds of information of service layer 2 packets to deny useless, unreliable, and doubtable service flow to strengthen network security.

Two key points of realizing packet filtration:

Step 1: Classify ingress flows according to some regulation;

Step 2: Filtrate distinct flow by denying. Deny is default accessing control.

15.1.6 Flow Monitor

In order to serve customers better with the limited network resources, QoS can monitor service flow of specified user in ingress interface, which can adapt to the distributed network resources.

15.1.7 Interface Speed Limitation

Interface speed limitation is the speed limit based on interface which limits the total speed rate of interface outputting packet.

15.1.8 Redirection

User can re-specify the packet transmission interface based on the need of its own QoS strategies.

15.1.9 Priority Mark

Ethernet Switch can provide priority mark service for specified packet, which includes: TOS, DSCP, 802.1p. These priority marks can adapt different QoS model and can be defined in these different models.

15.1.10 Choose Interface Outputting Queue for Packet

Ethernet Switch can choose corresponding outputting queue for specified packets.

15.1.11 Queue Scheduler

It adopts queue scheduler to solve the problem of resource contention of many packets when network congestion. There are three queue scheduler matchings: Strict-Priority Queue (PQ), Weighted Round Robin (WRR) and WRR with maximum delay.

1) PQ

PQ (Priority Queuing) is designed for key service application. Key service possesses an important feature, that is, require the precedent service to reduce the response delay when

network congestion. Priority queue divides all packets into 4 levels, that is, superior priority, middle priority, normal priority and inferior priority (3, 2, 1, 0), and their priority levels reduce in turn.

When queue scheduler, PQ precedently transmits the packets in superior priority according to the priority level. Transmit packet in inferior priority when the superior one is empty. Put the key service in the superior one, and non-key service (such as email)in inferior one to guarantee the packets in superior group can be first transmitted and non-key service can be transmitted in the spare time.

The shortage of PQ is: when there is network congestion, there are more packets in superior group for a long time, the packets in inferior priority will wait longer.

2) WRR

WRR queue scheduler divides a port into 4 or 8 outputting queues (S2926V-O has 4 queues, that is, 3, 2, 1, 0) and each scheduler is in turn to guarantee the service time for each queue. WRR can configure a weighted value (that is, w3, w2, w1, w0 in turn) which means the percentage of obtaining the resources. For example: There is a port of 100M. Configure its WRR queue scheduler value to be 50, 30, 10, 10 (corresponding w3, w2, w1, w0 in turn) to guarantee the inferior priority queue to gain at least 10Mbit/s bandwidth, to avoid the shortage of PQ queue scheduler in which packets may not gain the service.

WRR possesses another advantage. The scheduler of many queues is in turn, but the time for service is not fixed-if some queue is free, it will change to the next queue scheduler to make full use of bandwidth resources.

3) SP+ WRR

Superior priority or less priority use SP algorithm, others use WRR algorithm.

15.1.12 Cos-map Relationship of Hardware Priority Queue and Priority of IEEE802.1p Protocol

System will map between 802.1p protocol priority of packet and hardware queue priority. For each packet, system will map it to specified hardware queue priority according to 802.1p protocol priority of packet.

15.1.13 Flow Mirror

Flow mirror means coping specified data packet to monitor interface to detect network and exclude failure.

15.1.14 Statistics Based on Flow

Statistics based on flow can statistic and analyze the packets customer interested in.

15.1.15 Copy Packet to CPU

User can copy specified packet to CPU according to the need of its QoS strategies.

System realizes QoS function according to accessing control list, which includes: flow monitor, interface speed limit, packet redirection, priority mark, queue scheduler, flow mirror, flow statistics, and coping packet to CPU.

15.2 Configure QOS

15.2.1 QoS Configuration List

Configuration Task	Description	Detailed Configuration
Configure Flow Monitor	Required	15.2.2
Configure Two Rate Three Color Marker	Required	15.2.3
Configure Interface Line Rate	Required	15.2.4
Configure Packet Redirection	Required	15.2.5
Configure Traffic Copy to CPU	Required	15.2.6
Configure Traffic Priority	Required	15.2.7
Configure Queue-Scheduler	Optional	15.2.8
Configure Cos-map Relationship of Hardware Priority Queue and Priority of IEEE802.1p Protocol	Optional	15.2.9
Configure Mapping Relationship between DSCP and 8 Priority in IEEE 802.1p	Optional	15.2.10
Configure Flow Statistic	Required	15.2.11
Configure Flow Mirror	Required	15.2.12
Display and Maintain QoS	Optional	15.2.13

15.2.2 Configure Flow Monitor

Flow monitor is restriction to flow rate which can monitor the speed of a flow entering Switch. If the flow is beyond specified specification, it will take actions, such as dropping packet or reconfigure their priority.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Configure flow rate	**rate-limit** { **input** | **output** } { [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]] } *target-rate*	

15.2.3 ConfigureTwo Rate Three Color Marker

Two Rate Three Color Marker is defined in RFC 2698. There is 4 parameter for it: CIR, CBS, PIR and PBS.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Configure Two Rate Three Color Mode	**two-rate-policer mode** { color-aware | color-blind }	
Configure Two Rate Three Color pre-color	**two-rate-policer set-pre-color** *dscp-value* { green | red | yellow }	
Configure Two Rate Three Color Marker	**rate-limit input** { [**ip-group** { *acl-number* | *acl-name* } [**subitem** *subitem*]] [**link-group** { *acl-number* | *acl-name* } [**subitem** *subitem*]] } *target-rate* **two-rate-policercir** *cir* **cbs** *cbs* **pir** *pir* **pbs** *pbs* **conform-action** { copy-to-cpu | drop | set_dscp_value *dscp* | transmit exceed-action { copy-to-cpu | drop | set_dscp_value *dscp* | transmit } }	

	violate-action { copy-to-cpu | drop | set_dscp_value *dscp* | transmit } }	

15.2.4 Configure Interface Line Rate

Line-limit is the speed limit based on interface which restricts the total speed of packet outputting.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configure egress rate	**bandwidth egress kbps** *target-rate*	
Configure ingress rate	**bandwidth ingress kbps** *target-rate*	

15.2.5 Configure Packet Redirection

Packet redirection configuration is redirecting packet to be transmitted to some egress.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Configure packet redirection	**traffic-redirect** { [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]] } { [**interface** *interface-num* | **cpu**] }	

15.2.6 Configure Traffic Copy to CPU

Switch automatically copies to CPU after Configure traffic copy to CPU.

Operation	Command	Remarks

Enter globally configuration mode	**system-view**	
Configure traffic copy to CPU	**traffic-copy-to-cpu** { [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]] }	

15.2.7 Configure Traffic Priority

Traffic priority configuration is the strategy of remark priority for matching packet in ACL, and the marked priority can be filled in the domain which reflects priority in packet head.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Configure traffic priority	**traffic-priority** { [**ip-group** { *num* | *name*} [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]] } { [**dscp** *dscp-value*] [**cos** { *pre-value* | **from-ipprec** }] [**local-precedence** *pre-value*] }	

15.2.8 Configure Queue-Scheduler

When network congestion, it must use queue-scheduler to solve the problem of resource competition. System supports 3 kinds of queue-scheduler, that is SP, WRR and full SP+WRR. By default is SP in system.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Configure SP	**queue-scheduler** *group-number* **strict-priority**	

Configure WRR	**queue-scheduler** *group-number* **wrr** *queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight queue8-weight*	
Configure SP+WRR	**queue-scheduler** *group-number* **sp-wrr** *queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight queue8-weight*	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configure queue-scheduler on interface	**queue-scheduler** *group-number*	

15.2.9 Configure Cos-map Relationship of Hardware Priority Queue and Priority of IEEE802.1p Protocol

The cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol is one - to - one correspondence. Administrators change the cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol timely when the one-to-one correspondence shifting.

By default, the cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol as below:

802.1p	hardware priority queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Administrators also change the cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol according to the actual network.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Modify 802.1p and cos-map relationship of hardware priority queue	**queue-scheduler cos-map** *cos-map-group queue-number 802.1p-priority*	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configure cos-map on interface	**queue-scheduler cos-map** *cos-map-group*	

15.2.10 Configure Mapping Relationship between DSCP and 8 Priority in IEEE 802.1p

The same situation as 1.2.7, by default, the relation between DSCP and 8 priority in IEEE 802.1p as below:

SCP	hardware priority queue	DSCP	hardware priority queue	DSCP	hardware priority queue	DSCP	hardware priority queue
0	0	16	2	32	4	48	6
1	0	17	2	33	4	49	6
2	0	18	2	34	4	50	6
3	0	19	2	35	4	51	6
4	0	20	2	36	4	52	6
5	0	21	2	37	4	53	6
6	0	22	2	38	4	54	6
7	0	23	2	39	4	55	6
8	1	24	3	40	5	56	7
9	1	25	3	41	5	57	7
10	1	26	3	42	5	58	7
11	1	27	3	43	5	59	7
12	1	28	3	44	5	60	7
13	1	29	3	45	5	61	7
14	1	30	3	46	5	62	7
15	1	31	3	47	5	63	7

Administrators also change the mapping relationship between DSCP and 8 priority in IEEE 802.1p according to the actual network.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
save the relation between DSCP and 8 priority in IEEE 802.1p	**queue-scheduler dscp-map**	
Modify the relation between DSCP and 8 priority in IEEE 802.1p	**queue-scheduler dscp-map** *dscp-map-group dscp-value queue-number*	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configure cos-map on interface	**queue-scheduler dscp-map** *dscp-map-group*	

15.2.11 Configure Flow Statistic

Flow statistic configuration is used to statistic specified service flow packet. The statistic is accumulated value and reset to zero when re-Configure.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Configure flow staticstic	**traffic-statistic** { [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]] }	
reset to Zero	**clear traffic-statistic** { [**all** | [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]]] }	

15.2.12 Configure Flow Mirror

Flow mirror is copying the service flow which matches ACL rules to specified monitor interface to analyze and monitor packet.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Configure flow mirror	**mirrored-to** { [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]] } **interface** *interface-num*	

15.2.13 Display and Maintain QoS

After finishing above configuration, please use below commands to display the configuration.

Operation	Command	Remarks
Display all the informaion of QoS	**display qos-info all**	
Display QoS statistic	**display qos-info statistic**	
Display quue-scheduler mode and parameters	**display queue-scheduler**	
Display the cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol	**display queue-scheduler cos-map** [*cos-map-group*]	
Display the dscp-map relationship of hardware priority queue and priority of IEEE802.1p protocol	**display queue-scheduler dscp-map** [*dscp-map-group*]	
Display all QoS port configuration	**display qos-interface** [interface ethernet	

	interface-num] **all**	
Display rate-limit parameters	**display qos-interface** [interface ethernet *interface-num*] **rate-limit**	
Display interface line rate parameters	**display bandwidth** [interface ethernet *interface-num*]	
Display QoS interface statistic parameters	**display qos-interface statistic**	
Display traffic-priority parameters	**display qos-info traffic-priority**	
Display traffic-redirect parameters	**display qos-info traffic-redirect**	
Display packet redirection	**display qos-info traffic-statistic**	
Display information of traffic copy to CPU	**display qos-info traffic-copy-to-cpu**	

Chapter 16 SSH

16.1 SSH Overview

Secure Shell (SSH) can provide information security and powerful authentication to prevent such assaults as IP address spoofing, plain-text password interception when users log on to the Switch remotely through an insecure network environment.

SSH can take the place of the Telnet to provide safe management and configuration.

16.2 Configure SSH Server

A Switch, as a SSH server, can connect to multiple SSH clients. SSH clients can be both LAN users and WAN users. XXXX Switches can only SSH server and support SSH v2.

The following table describes SSH server configuration tasks.

Operation	Command	Remarks
Enterprivileged configuration mode	**enable**	
Configure the default key	**ssh-server key create** { rsa | dss | ecdsa }	
Clear configured key	**ssh-server key delete** { rsa | dss | ecdsa }	
Enter globally configuration mode	**system-view**	-
Enable SSH	**ssh-server**	By default, this function is disabled.

Disable SSH	**undo ssh-server**	
Config SSH User limit	**ssh-server limit** *max-num*	
Display SSH	**display ssh-server**	
Display SSH user limit	**display ssh-server limit**	

16.3 Log in Switch from SSH Client

To successfully establish SSH connection, pay attention to following points:

1) Create the connection between SSH client and server.

2) The version of client and server should be the same.

3) SSH function in server should be enabled.

Chapter 17 SNMP

17.1 SNMP Overview

SNMP (Simple Network Management Protocol) is an important network management protocol on TCP / IP networks, implementing network management by exchanging packets on the network. The SNMP protocol provides the possibility of centralized management of large networks. Its goal is to ensure the management information is transmitted between any two points. SNMP is convenient for the network administrator to retrieve information from any node on the network, make modifications, find faults, and complete fault diagnosis, capacity planning and report generation.

SNMP structure is divided into two parts: NMS and Agent. NMS (Network Management Station) is a workstation that runs client programs while Agent is a server-side software running on a network device. The NMS can forward GetRequest, GetNextRequest, and SetRequest packets to the Agent. Upon receiving the NMS request message, the agent performs Read or Write operations according to the packet type and generates a Response packet to return to the NMS. On the other hand, when the device encounters an abnormal event such as hot / cold start, the agent will forward a trap packet to NMS to report the events.

The system supports SNMP v1, SNMP v2c and SNMP v3. SNMP V1 provides a simple authentication mechanism, does not support the administrator-to-manager communications, and v1 Trap has no confirmation mechanism. V2c enhanced v1 management model (on

security), management information structure, protocol operation, manager and communication ability between managers to increase the creation and deletion of the table, the communication ability between managers, reducing the storage side of the agent. V3 implements the user authentication mechanism and packet encryption mechanism, which greatly improves the security of the SNMP protocol.

This function cooperates with the network management software to log on to the Switch and manage the Switch.

17.2 Configure SNMP-Agent

17.2.1 SNMP-Agent Configuration List

Configuration Task	Description	Detailed Configuration
Configure the Basic Parameters	Required	17.2.2
Configure the Community Name	Required	17.2.3
Configure the Views	Optional	17.2.4
Configure the Group	Optional	17.2.5
Configure the User	Optional	17.2.6
Display SNMP Configuration	Optional	17.2.7

17.2.2 Configure the Basic Parameters

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enable/disable SNMP Traps/informs	[**undo**] **snmp-agent enable** { informs | traps } [*notificationtype-list*]	
Configure sysContact	[**undo**] **snmp-agent scontact** *syscontact*	
Configure sysLocation	[**undo**] **snmp-agent location** *syslocation*	
Configure SW	[**undo**] **snmp-agent name** *SW*	
Configure maximum length of snmp protocol packets	[**undo**] **snmp-agent max-packet-length** *length*	
Configure host	[**undo**] **snmp-agent host** *host-addr* [version { 1 | 2c | 3 [auth | noauth | priv] }] *community-string* [udp-port *port*] [notify-type [*notifytype-list*]]	
Configure snmp trap-source	[**undo**] **snmp-agent trap-source** *ipaddress*	
Configure snmp-agent engineoid	[**undo**] **snmp-agent engineoid** { **local** *engineid-string* | **remote** *ip-address*	

	[*udp-port port-number*] *engineid-string* }	

17.2.3 Configure the Community Name

SNMP adopts the community name authentication scheme. SNMP packets that do not match the community name will be discarded. SNMP community is named by a string, known as the community name. Different communities can have read-only or read-write access permission. A community with read-only access can only query system information. However, in addition to query the system information, the community with read-write access permission can perform the system configurations. It defaults to no community name.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Configure the community name	**snmp-agent community** *community-name* { ro | rw } { deny | permit } [view *view-name*]	
Display the community name	**display snmp-agent community**	
Remove the community name	**undo snmp-agent community** *community-name*	

17.2.4 Configure the Views

It is used to configure the views available to access control and the subtrees that they contain. The iso, internet, and sysview exist by default. Delete and modify the internet is not supported.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Configure the views	**snmp-agent view** *view-name oid-tree* { included | excluded }	
Delete the views	**undo snmp-agent view** *view-name* [oid-tree]	

17.2.5 Configure the Group

This configuration task can be used to configure an access control group. By default, there are two snmpv3 groups: (1) The initial group with the security level of auth; (2) The initial group with the security level of noauthpriv(No authentication is required and no encryption is required).

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Configure the group	**snmp-agent group** *groupname* { 1 | 2c | 3 [auth | noauth | priv] [context context-name] } [read *readview*] [wrete *writeview*] [notify *notifyview*]	
Delete the group	**undo snmp-agent group** *groupname* { 1 | 2c | 3 [auth | noauth | priv] [context *context-name*] }	

17.2.6 Configure the User

It is used to configure the user for the local engine or for the remote engine that can be identified. By default, the following users exist: (1)initialmd5, (2) initialsha, (3) initialnone.

The above three users are reserved for the system and cannot be used by the user. When Configure a user, you need to ensure that the engine to which this user belongs is identifiable. When an identifiable engine is deleted, the users it contains are also deleted.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Configure the user	**snmp-agent user** *username groupname* [remote *host* [udp-port *port*]] [auth { md5 | sha } { authpassword { encrypt-auth password *authpassword* | *authpassword* } | authkey { encrypt-authkey *authkey* | *authkey* } } [priv des { privpassword { encrypt-privpassword *privpassword* | *privpassword* } | privkey { encrypt-privkey *privkey* | *privkey* } }]	
Delete the user	**undo snmp-agent user** *username* [remote *host* [udp-port *port*]]	

17.2.7 Display SNMP-Agent Configuration

Operation	Command	Remarks
display snmp community configuration	**display snmp community**	
display snmp contact configuration	**display snmp contact**	
display snmp engineid configuration	**display snmp engineid** { local | remote }	
display snmp group configuration	**display snmp group**	
display snmp host configuration	**display snmp host**	
display snmp location configuration	**display snmp location**	
display snmpmax-packet-length configuration	**display snmp max-packet-length**	
display snmp name configuration	**display snmp name**	
display snmp notify configuration	**display snmp notify**	
display snmp user configuration	**display snmp user**	
display snmp view configuration	**display snmp view**	

17.3 RMON

RMON (Remote Network Monitoring) mainly implements statistics and alarm functions, and is used for remote monitoring and management of managed devices by management devices in the network.

The statistics function means that the managed device can track and count various traffic

information on the network segment connected by its port periodically or continuously, such as the total number of messages received on a network segment in a certain period of time, or the total number of ultra long messages received.

The alarm function refers to that the managed device can monitor the value of the specified MIB variable. When the value reaches the alarm threshold (for example, the port rate reaches the specified value, or the proportion of broadcast messages reaches the specified value), it can automatically record logs, generate alarm information, and send it to the SNMP module, which sends it to the management device. For details about alarm information, see "SNMP" in "Network Management and Monitoring Configuration Guide".

17.3.1 Working mechanism of RMON

RMON allows multiple monitors to collect data in two ways:

• The first method uses a dedicated RMON probe to collect data, and the management device directly obtains management information from the RMON probe and controls network resources. This method can obtain all the information of the RMON MIB;

• The second method is to directly implant the RMON Agent into network devices (routers, switches, HUBs, etc.) to make them become network facilities with RMON probe function. The management device uses the basic operations of SNMP to exchange data information with the RMON Agent and collect network management information. However, this method is limited by the device resources and cannot obtain all the data of the RMON MIB. It only collects the information of four groups: event group, alarm group, history group and statistics group.

17.3.2 RMON group

Multiple RMON groups are defined in the RMON protocol. The device implements the statistics group, history group, event group, alarm group, agent configuration group and user history group supported in the public MIB

17.3.3 Statistics group

The statistics group stipulates that the system will continuously make statistics on various traffic information of ports (currently only supports statistics on Ethernet ports), and store the statistics results in the Ethernet Statistics Table for management devices to view at any time. After the statistics table item is successfully created under the specified interface, the statistics group will count the number of messages of the current interface. The result of its statistics is a continuous cumulative value.

The statistical information includes the number of network conflicts, the number of CRC check error messages, the number of data messages that are too small (or too large), the number of broadcast and multicast messages, the number of received bytes, the number of received messages, etc.

17.3.4 Event Group

The event group is used to define the event index number and the event handling method. The events defined by the event group are used in the alarm group entries and extended alarm group entries. When the monitored object reaches the alarm condition, an event will be triggered. The event can be handled in the following ways:

• Log: Record the event related information (event occurrence time, event content, etc.) in the event log table of the RMON MIB of the device, so that the management device can view it through the SNMP Get operation.

• Trap: indicates that when an event is triggered, an alarm message will be generated and sent to the SNMP module of the device.

• Log Trap: When an event is triggered, it not only records the log on the device, but also generates alarm information and sends it to the SNMP module of the device.

• None: No processing.

17.3.5 Alarm group

RMON alarm management can monitor the specified alarm variables (such as the total number of messages received by the port etherStatsPkts). After the user defines the alarm table item, the system will obtain the value of the monitored alarm variable according to the defined time cycle. When the value of the alarm variable is greater than or equal to the upper limit threshold, an upper limit alarm event will be triggered; When the value of the alarm variable is less than or equal to the lower limit threshold, a lower limit alarm event will be triggered, and the alarm management will handle it according to the definition of the event.

17.3.6 Protocol Specification

Protocol specifications related to RMON include:

• RFC 4502：Remote Network Monitoring Management Information Base Version 2

• RFC 2819：Remote Network Monitoring Management Information Base Status of this Memo

17.3.7 Configure the RMON Ethernet statistics function

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the Ethernet interface view	**interface** *interface-type interface-number*	
Create Statistics Table Item	**rmon statistics** *entry-number* [**owner** *text*]	

17.3.8 Configure RMON historical statistics function

When configuring the RMON historical statistics function, you should pay attention to:

•The entry number of the history control table item must be globally unique. If it has been used under other interfaces, the creation operation will fail.

• Under the same interface, multiple historical control table items can be created, but the values of entry number and sampling interval of different table items must be different, otherwise the creation operation fails.

• The maximum number of control history table entries allowed to be created for the entire device is 100. When the total number of control history table entries is more than 100, the creation operation fails.

• When creating a historical control table item, if the specified bucket number parameter value exceeds the historical table capacity actually supported by the device, the historical control table item will be added, but the value of the bucket number corresponding to the table item is the historical table capacity actually supported by the device.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the Ethernet interface view	**interface** *interface-type interface-number*	
Create History Control Table Entry	**Rmon** **history entry-number buckets number int** **erval interval [owner text]**	

17.3.9 Configure RMON alarm function

If alarm information needs to be sent to the management device (NMS) when an alarm event is triggered, you must ensure that the SNMP Agent has been correctly configured before configuring the RMON alarm function. For the configuration of SNMP Agent, see SNMP in the Network Management and Monitoring Configuration Guide.

Operation	Command	Remarks
Event Table Entry	*Description string, event type (log, trap,* *logtrap or none) and community name* *(security string)*	
Alarm table item	*Alarm variable, sampling interval, sampling* *type (absolute or delta), upper threshold*	

	(threshold value1) and lower threshold (threshold value2)	
Extended alarm table item	*Alarm variable formula (primalarm formula), sampling interval, sampling type (absolute or delta), upper threshold (threshold value1) and lower threshold (threshold value2)*	

Configuration Steps

Operation	Command	Remarks
(Optional) Create an event table entry.	**rmon event entry-number [description str ing] { log | log-trap security-string | none | trap security-string } [owner text]**	
Create alarm table item	**rmon alarm** *entry-number alarm-variable sampling-interval {* **absolute** | **delta** *} [* **startup-alarm** *{* **falling** | **rising** | **rising-falli ng** *}]* **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-val ue2 event-entry2 [* **owner** *text]*	
Create extended alarm table item	**rmon prialarm entry-number prialarm-formula prialarm-des**	

	sampling-interval **{ absolute | delta } [startup-alarm { fallin** **g | rising |** **rising-falling }] rising-threshold threshold** **-value1** **event-entry1 falling-threshold threshold-v** **alue2** **event-entry2 entrytype { forever | cycle cy** **cle-period } [owner text]**	

17.3.10 RMON display and maintenance

After completing the above configuration, execute the display command in any view to display the running status of RMON after configuration. Verify the configuration effect by viewing the display information.

Operation	Command	Remarks
Display RMON statistics	**display rmon statistics** [*interface-type* *interface-number]*	
Display RMON historical control table and historical sampling information	**display rmon history** [*interface-type* *interface-number]*	

Display relevant information of RMON alarm table items	**display rmon alarm** [*entry-number]*	
Display relevant information of RMON extended alarm table items	**display rmon prialarm** [*entry-number]*	
Displays information about RMON event table entries	**display rmon event** [*entry-number]*	
Display information about event log entries	**display rmon eventlog** [*entry-number]*	

17.3.11 Example of typical configuration of RMON

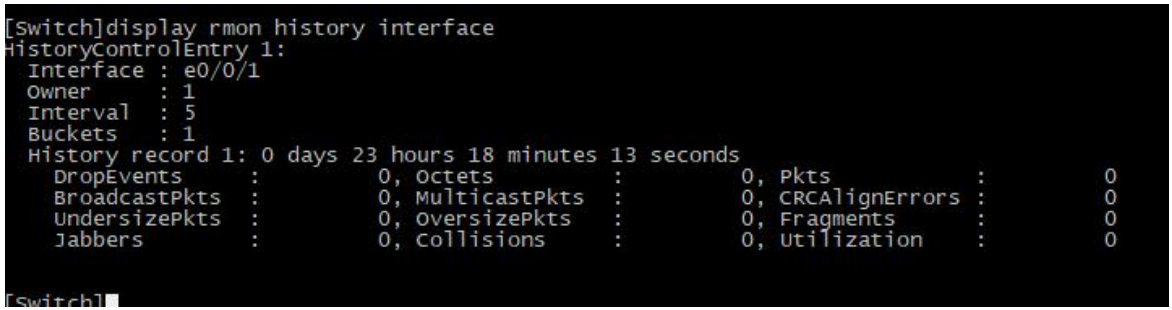
1)Now it is necessary to conduct performance statistics on the messages received by Gigabit Ethernet 0/0/1 through the RMON statistics table. The administrator can check the statistical data at any time to understand the status of the interface receiving messages.

```
<Sw> system-view
[sw] interface gigabitethernet 1/0/1
[sw-Ethernet0/0/1] rmon statistics 1 owner user1
```

```
[Switch]display rmon statistics interface ethernet 0/0/1
EtherStatsEntry 1:
  Interface : e0/0/1
  Owner     : test
  Octets          :         0, Pkts           :         0, BroadcastPkts  :         0
  MulticastPkts   :         0, CRCAlignErrors :         0, UndersizePkts  :         0
  OversizePkts    :         0, Fragments      :         0, Jabbers        :         0
  Collisions      :         0, DropEvents     :         0, Pkts64         :     25450
  Pkts65to127     :     24955, Pkts128to255   :       281, Pkts256to511   :     21744
  Pkts512to1023   :     43488, Pkts1024to1518 :         0
```

2)Example of typical configuration of historical statistics function

```
<SW> system-view
[Sw] gigabitethernet 0/0/1
[Sw-Ethernet1/0/1] rmon history 1 buckets 1 interval 60 owner user1
```



3)Example of typical configuration of alarm function

snmp-agent community public ro permit view iso

snmp-agent community private rw permit view iso

snmp-agent host 10.1.1.200 version 2c public udp-port 162 notify-type bridge g

bn gbnsavecfg interfaces rmon snmp

snmp-agent enable traps

```
[SW] interface gigabitethernet 1/0/1
[SW-GigabitEthernet1/0/1] rmon statistics 1 owner user1
[SW-GigabitEthernet1/0/1] quit
[SW] rmon event 1 trap public owner user1
```

```
[SW] rmon alarm 1 1.3.6.1.4.1.8888.1.2.4.4.20.1.1 2 5 delta rising-threshold 100
1 falling-threshold 50 1 owner user1



<SW> display rmon alarm 1
AlarmEntry 1 owned by user1 is VALID.
  Sample type          : delta
  Sampled variable     : 1.3.6.1.4.1.8888.1.2.4.4.20.1.1 2<etherStatsOctets.1>
  Sampling interval (in seconds)    : 5
  Rising threshold      : 100(associated with event 1)
  Falling threshold     : 50(associated with event 1)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Latest value          : 0



[Switch]display rmon statistics interface ethernet 0/0/1
EtherStatsEntry 1:
  Interface : e0/0/1
  Owner     : test
  Octets       :       0, Pkts         :       0, BroadcastPkts  :       0
  MulticastPkts  :       0, CRCAlignErrors :       0, UndersizePkts  :       0
  OversizePkts   :       0, Fragments     :       0, Jabbers       :       0
  Collisions     :       0, DropEvents    :       0, Pkts64        :   27559
  Pkts65to127    :   26028, Pkts128to255   :     297, Pkts256to511   :   22800
  Pkts512to1023  :   45600, Pkts1024to1518 :       0
```

Chapter 18 Info-center

18.1 Info-center Overview

As the information center of the system, the Info-center processes and outputs information in a unified manner.

Other modules in the system send information to be outputted to the Info-center. The Info-center determines the output format based on user configurations and outputs information to the specified display device based on information output functions and filtering rules in user configurations.

Info-center information producers (modules outputting information) only need to output information to the Info-center, without concerning whether information needs to be outputted to the console, telnet terminal, or log host (Info-center server). Information consumers (the console, telnet terminal, history buffer, log host, and SNMP agent) can select the desired information and discard the unwanted information based on their demands, on condition that proper filtering rules are configured.

18.2 Configure Info-center

18.2.1 Info-center Configuration List

Configuration Task	Description	Detailed Configuration

Enabling/Disabling the Info-center for the equipment	Required	18.2.2
Configure the function of Display the sequence number in Info-center outputs	Optional	18.2.3
Configure the time stamp type in Info-center outputs	Optional	18.2.4
Configure the function of outputting Info-center information to terminals	Optional	18.2.5
Configure the function of outputting Info-center information to the history buffer	Optional	18.2.6
Configure the function of outputting Info-center information to the flash storage	Optional	18.2.7
Configure the function of outputting Info-center information to the log host	Optional	18.2.8
Configure the function of outputting Info-center information to the SNMP agent	Optional	18.2.9
Configure the module debugging function	Optional	18.2.10

18.2.2 Enabling/Disabling the Info-center for the Equipment

In global configuration mode, enable or disable the Info-center function. When the Info-center function is disabled, no information is outputted. By default, the info-center function is enabled

on the equipment.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enable the log output function of the system.	**info-center**	
Disable the log output function of the system.	**undo info-center**	
Display log configurations of the system.	**display info-center**	

18.2.3 Configure the Function of Display the Sequence Number in Info-center Outputs

In global configuration mode, set to or not to display the global sequence number in Info-center outputs.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enable the function of Display log sequence numbers.	**info-center sequence-numbers**	
Disable the function of Display log sequence numbers.	**undo info-center sequence-numbers**	

18.2.4 Configure the Time Stamp Type in Info-center Outputs

In global configuration mode, configure the time stamp type in Info-center outputs. The time stamp type can be set to **notime**, **uptime**, or **datetime**.

The default value is **uptime**.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enable the function of Display the time stamp of logs and configure the time display format.	**info-center timestamps** { **notime** | **uptime** | **datetime** }	
Restore the default setting of Display the time stamp of logs.	**undo info-center timestamps**	

18.2.5 Configure the Function of Outputting Info-center Information to Terminals

In global configuration mode, configure the information output function, information display function, and filtering rules for outputting Info-center information to terminals. By default, Info-center information is outputted only to the buffer and not outputted to the console or terminal.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	

Enable the log output function and output logs to the specified terminal.	**info-center monitor** { **all** | *monitor-num* }	When **monitor-num** is set to **0**, logs are outputted to the console. When **monitor-num** is set to 1–5, logs are outputted to telnet terminals.
Disable the function of outputting logs to a or all terminals.	**undo info-center monitor** { **all |** *monitor-num* }	
Return to the privileged mode.	**quit**	
Enable the function of Display system information.	**terminal monitor**	Enabled by default,The setting affects only the current login of the current terminal and is invalid for other terminals or the next login

		of the current terminal.
Disable the function of Display system information to prevent outputting any logs to the current terminal.	**undo terminal monitor**	The setting affects only the current login of the current terminal and is invalid for other terminals or the next login of the current terminal.
Configure the filtering rules of logs to be outputted to terminals. Specify the level and module whose logs are outputted to the specified terminal.	**info-center monitor** { **all** | *monitor-no* } { *level* | **none** | **level-list** { *level* [**to** *level*] } **&<1-8>** } [**module** { **xxx | …** } *****]	
Delete the filtering rules of logs to be outputted to the terminals in the system and restore the default configuration.	**undo info-center monitor** { **all |** ***monitor-no*** } **filter**	

18.2.6 Configure the Function of Outputting Info-center Information

to the History Buffer

In global configuration mode, configure the information output function and filtering rules for outputting Info-center information to the history buffer. By default, the function is enabled.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enable the function of outputting logs to the buffer.	**info-center buffered**	Enabled by default
Disable the function of outputting logs to the buffer.	**undo info-center buffered**	
Configure the filtering rules of logs to be outputted to the buffer. Specify the level and module whose logs are outputted to the buffer.	**info-center buffered** { *level* | **none** | **level-list** { *level* [**to** *level*] } **&** < **1-8** > } [**module** { xxx | … } *****]	
Delete the filtering rules of logs to be outputted to the buffer in the system and restore the default configuration.	**undo info-center buffered filter**	

18.2.7 Configure the Function of Outputting Info-center Information to the Flash Storage

In global configuration mode, configure the information output function and filtering rules for outputting Info-center information to the flash storage. By default, Info-center information is not saved to the flash storage. In addition, the interval of saving Info-center information to the flash storage cannot be configured and the system saves Info-center information once every 30 minutes by default.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enable the function of outputting logs to the flash storage.	**info-center flash**	
Disable the function of outputting logs to the flash storage.	**undo info-center flash**	Disabled by default)
Configure the filtering rules of logs to be outputted to the flash storage. Specify the level and module whose logs are outputted to the flash storage.	**info-center flash** { *level* | **none** | **level-list** { *level* [**to** *level*] } & < 1-8 > } [**module** { xxx | …} *]	
Delete the filtering rules of logs to be outputted to the flash storage in the system and restore the default configuration.	**undo info-center flash filter**	

18.2.8 Configure the Function of Outputting Info-center Information to the Log Host

In global configuration mode, configure the server address, information output function, filtering rules, info-center tool, and fixed source address for outputting Info-center information to the log host.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Configure the IP address of the log host.	**info-center** *ip-address*	A maximum of 15 server IP addresses can be configured.
Delete the IP address configured for the log host.	**undo info-center** *ip-address*	
Enable the function of outputting logs to the specified host.	**info-center host** { **all** | *ip-address* }	
Disable the function of outputting logs to the specified host.	**undo info-center host** { **all |** *ip-address* }	

Configure the filtering rules of logs to be outputted to the host. Specify the level and module whose logs are outputted to the host.	**info-center host** { **all** | *ip-address* } { *level* | **none** | **level-list** { *level* [**to** *level*] } **&** < **1-8** > } [**module** { xxx | … } *****]	
Delete the filtering rules of logs to be outputted to the host in the system and restore the default configuration.	**undo info-center host** { **all |** *ip-address* } **filter**	
Configure the info-center tool of the system.	**info-center facility** { xxx | … }	
Delete the configured info-center tool name and restore the original setting (**localuse7**).	**undo info-center facility**	
Configure the fixed source address of log output. **ip-address** must be set to an interface address of the equipment.	**info-center source** *ip-address*	
Disable the function of outputting logs from the fixed source address.	**undo info-center source**	After the function is disabled, logs will be externally

		sent through the existing IP interface addresses in the system.

18.2.9 Configure the Function of Outputting Info-center Information to the SNMP Agent

In global configuration mode, configure the information output function and filtering rules for outputting Info-center information to the SNMP agent.

To send Info-center information to the SNMP workstation as Trap packets, you must configure the Trap host address. For details, see SNMP configuration.

By default, the function is disabled.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enable the function of outputting logs to the SNMP agent.	**info-center snmp-agent**	
Disable the function of outputting logs to the SNMP agent.	**undo info-center snmp-agent**	
Configure the filtering rules of logs to be outputted to the SNMP agent.	**info-center snmp-agent** { *level* | **none** | **level-list** { *level* [**to** *level*] } **&** < **1-8** > }	

Specify the level and module whose logs are outputted to the SNMP agent.	[**module** { xxx | … } *]	
Delete the filtering rules of logs to be outputted to the SNMP agent in the system and restore the default configuration.	**undo info-center snmp-agent filter**	

18.2.10 Configure the Module Debugging Function

In global configuration mode, enable/disable the module debugging function. By default, the module debugging function is disabled.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enable the function of outputting the debugging information about the specified module to logs.	**debug** { **all** | { xxx | … } * }	
Disable the function of outputting the debugging information about the specified module.	**undo debug** { **all |** { xxx | …} * }	
Display the current configuration of the function of outputting debugging	**display debug**	

information.		

Chapter 19 L3 Base Function

19.1 L3 Base Function Overview

Switch is a 10-Gigabit intelligent routing Switch Switch based on the application specific integrated circuit (ASIC) technology and supports layer 2 (L2) and layer 3 (L3) forwarding. It performs L2 forwarding when hosts in the same virtual local area network (VLAN) access each other and L3 forwarding when hosts in different VLANs access each other.

19.2 Configure L3 Base Function

19.2.1 L3 Base Function Configuration List

Configuration Task	Description	Detailed Configuration
Planning VLANs and creating L3 interfaces	Required	19.2.2
Configure the forwarding mode	Optional	19.2.3
Creating VLAN interfaces for common VLANs	Optional	19.2.4
Creating superVLAN interfaces and adding VLANs to the superVLAN	Required	19.2.5
Configure IP addresses for VLAN or superVLAN interfaces	Required	19.2.6

Configure an IP address range for VLAN or superVLAN interfaces	Required	19.2.7
Configure the Address Resolution Protocol (ARP) proxy	Optional	19.2.8
Display interface configurations	Optional	19.2.9
Configure unicast reverse path forwarding (URPF)	Optional	19.2.10
Disabling the function of sending Internet Control Message Protocol (ICMP) packets with an unreachable destination host on interfaces	Optional	19.2.11

19.2.2 Planning VLANs and Creating L3 Interfaces

For details about VLAN planning, see VLAN configurations.

L3 interfaces are classified into common VLAN interfaces and superVLAN interfaces. Common VLAN interfaces are created on VLANs and superVLAN interfaces on superVLANs (superVLANs do not exist or contain any port).

19.2.3 Configure the Forwarding Mode

The L3 Switch supports stream forwarding and network topology-based forwarding. In stream forwarding mode, The L3 Switch identifies the failed route or the unreachable destination host route and sends packets to the CPU for further processing. In network topology-based forwarding mode, The L3 Switch directly discards the packets. By default, The L3 Switch works in stream forwarding mode.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Set the packet forwarding mode in the system to stream forwarding.	**ip def cpu**	
Set the packet forwarding mode in the system to network topology-based forwarding.	**undo ip def cpu**	
Display the configured packet forwarding mode.	**display ip def cpu**	

19.2.4 Creating VLAN Interfaces for Common VLANs

A VLAN interface needs to be configured for each VLAN that performs L3 forwarding or the VLAN needs to be added to the superVLAN.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Create a VLAN interface with the VLAN ID being **vid** and enter the VLAN interface configuration mode.	**interface vlan-interface** *vid*	
Return to the global configuration mode.	**quit**	

Delete the VLAN interface with the VLAN ID being **vid**.	**undo interface vlan-interface** *vid*	

19.2.5 Creating SuperVLAN Interfaces and Adding VLANs to the SuperVLAN

SuperVLAN interfaces are used for communication between hosts in different VLANs in the same network segment. SuperVLAN interfaces are implemented through the ARP proxy.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Create a superVLAN interface with the interface ID being **vid** and enter the superVLAN interface configuration mode.	**interface supervlan-interface** *vid*	
Return to the global configuration mode.	**quit**	
Delete the superVLAN interface with the interface ID being **vid**.	**undo interface supervlan-interface** *vid*	
Configure sub VLANs for the superVLAN interface.	**subvlan** *vid*	
Delete the sub VLANs configured for	**undo subvlan** *vid*	

the superVLAN interface.		

19.2.6 Configure IPv4/v6 Addresses for VLAN or SuperVLAN Interfaces

Each VLAN or superVLAN interface can be configured with a maximum of 32 IP addresses and the IP addresses of VLAN or superVLAN interfaces cannot be in the same network segment. The first IP address of an interface will be automatically selected as the primary IP address. When the primary IP address is deleted, the interface automatically selects another IP address as the primary IP address or a configured IP address can be manually specified as the primary IP address.

For example, Create ip interface based on Vlan the management address of ipv4 and ipv6.

ip address 10.1.1.1 255.255.255.0 ,ipv6 address 2000::1/64

if the IP address of VLAN interface 1 is 10.11.0.1/16, the IP addresses of other interfaces must not be in the 10.11.0.0/16 network segment (such as 10.11.1.1/24).

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Configure an IP address and a mask for the interface.	**ip address** *ipaddress ipaddress mask*	
Delete all IP addresses of the	**undo ip address**	

interface.		
Delete the specified IP address of the interface.	**undo ip address** *ipaddress ipaddress mask*	
Configure the primary IP address for the interface.	**ip address primary** *ipaddress*	

19.2.7 Configure an IP Address Range for VLAN or SuperVLAN Interfaces

Each VLAN or superVLAN interface can be configured with a maximum of eight IP address ranges. After an IP address range is configured, only the ARP entries within this range can be learnt so as to restrict user access. When a VLAN or superVLAN interface is deleted, relevant configurations are automatically deleted.

For superVLAN interfaces, sub VLANs can be specified at the same time so that the set address range is applicable only to these sub VLANs.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Configure the IP address range supported by this interface, ranging	**ip address range** *startip endip*	

from **startip** to **endip**.		
Delete all IP address ranges supported by the interface.	**undo ip address range**	
Delete the specified IP address ranges supported by the interface.	**undo ip address range** *startip endip*	
Configure the IP address range for sub VLANs of the superVLAN.	**ip address range** *startip endip* **vlan** *vlanid*	
Delete the IP address ranges of the sub VLANs of the superVLAN.	**undo ip address range** *startip endip* **vlan** *vlanid*	

19.2.8 Configure the ARP Proxy

ARP request packets are broadcast packets and cannot pass through VLANs. If the ARP proxy function is enabled, ARP interaction is supported between hosts in sub VLANs of the same superVLAN. When the ARP proxy is disabled, the hosts of the sub VLANs in the superVLAN interface cannot communicate with each other.

By default, the ARP request packets from all sub VLANs are processed in the preceding manner. In addition, relevant commands can be used to prevent the ARP request packets from a sub VLAN from being broadcast to other sub VLANs when they are processed by the ARP proxy.

Operation	Command	Remarks

Enter the VLAN configuration mode.	**interface vlan-interface** *vlan-id*	
Enable the arp-proxy function for the VLAN.	**local-arp-proxy**	
Disable the arp-proxy function for the VLAN.	**undo local-arp-proxy**	
Enable the arp-proxy broadcast function for the VLAN.	**local-arp-proxy broadcast**	
Disable the arp-proxy broadcast function for the VLAN.	**undo local-arp-proxy broadcast**	
Display the information about the ARP proxy configured in the system.	**display local-arp-proxy**	
Display information about the ARP proxy broadcast function configured in the system.	**display local-arp-proxy broadcast**	

19.2.9 Display VLAN and SuperVLAN Interface Information

The L3 Switch integrates VLAN interface information and superVLAN interface information. They can be viewed by running a unified display command.

Operation	Command	Remarks
Display information about the VLAN	**display ip interface** [[**vlan-interface**	

and superVLAN interfaces currently configured in the system.	*vlanid*] | [**supervlan-interface** *supervlanid*]]	

19.2.10 Configure URPF

URPF aims to prevent network attack behaviors based on source address spoofing. URPF obtains the source address and ingress interface of a packet and uses the source address as the destination address to query the routing table for the matching route. The packet is forwarded if it meets conditions and discarded if it does not meet conditions. Two URPF modes are supported:

Strict mode: In this mode, the source address must exist in the routing table and the egress interface of the source address of the packet is the same as the ingress interface of the packet.

Loose mode: In this mode, the system only checks whether the source address of the packet exists in the unicast routing table. If yes, the packet is forwarded.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Enable URPF for this interface and specify the URPF mode.	**urpf** { **loose** | **strict** }	
Disable URPF for this interface.	**undo urpf**	

Display URPF information in the system.	**display urpf**	

19.2.11 Disabling the Function of Sending ICMP Packets with an Unreachable Destination Host on Interfaces

To avoid attacks from address scanning software similar to ip-scan, users can disable the function of sending ICMP packets with an unreachable host on interfaces.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Enable the function of this interface for sending ICMP packets with an unreachable destination	**ip icmp unreachable**	
Disable the function of this interface for sending ICMP packets with an unreachable destination	**undo ip icmp unreachable**	
Display the configuration of the function of sending ICMP packets with an unreachable destination	**display ip icmp unreachable**	

Chapter 20 ARP

20.1 ARP Overview

Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address.

An IP address is the address of a host at the network layer. To send a network layer packet to a destination host, the device must know the data link layer address (such as the MAC address) of the destination host. To this end, the IP address must be resolved into the corresponding data link layer address.

Unless otherwise stated, the data link layer addresses that appear in this chapter refer to the 48-bit Ethernet MAC addresses.

20.2 Configure ARP

20.2.1 ARP Configuration List

Configuration Task	Description	Detailed Configuration
Add/Delete ARP	Required	20.2.2
Bind dynamic arp to static	Optional	20.2.3
Display ARP entry	Optional	20.2.4

Configure ARP aging-time	Optional	20.2.5

20.2.2 Add/Delete ARP

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Add ARP	**arp** *ip-address* **mac** *mac-address* **vid** *vlan-id* **port** *interface-num*	
Delete ARP	**undo arp** { all | static | dynamic | *ip-address* }	

20.2.3 Bind dynamic Arp to Static

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Bind dynamic arp	**arp bind dynamic** { *ip-address* | all }	

20.2.4 Display ARP Entry

Operation	Command	Remarks
Display arp entry	**display arp** { all | static | dynamic | *ip-address* | interface { vlan-interface *vlan-id* | supervlan-interface *vlan-id* } }	

20.2.5 Configure ARP Aging-time

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Configure ARP aging-time	**arp aging-time** *aging-time*	
Configure default ARP aging-time	**undo arp aging-time**	20minutes by default
Display arp aging-time	**display arp aging-time**	

Chapter 21 ARP Spoofing and Flood

21.1 ARP Spoofing and Flood Attack Overview

ARP provides no security mechanism and thus is prone to network attacks. An attacker can construct and send ARP packets, thus threatening network security.

A forged ARP packet has the following characteristics:

- The sender MAC address or target MAC address in the ARP message is inconsistent with the source MAC or destination MAC address in the Ethernet frame.
- The mapping between the sender IP address and the sender MAC address in the forged ARP message is not the true IP-to-MAC address binding of a valid client.

ARP attacks bring many malicious effects. Network communications become unstable, users cannot access the Internet, and serious industrial accidents may even occur. ARP attacks may also intercept accounts and passwords of services such as games, network banks, and file services.

ARP spoofing attacks to protection, the key is to identify and prohibit forwarding spoofed ARP packets. From the principle of ARP spoofing, we can see, to prevent ARP spoofing attack requires two ways, first to prevent the virus disguised as the gateway host, it will cause the entire segment of the user can not access; followed by preventing the virus from the host masquerade as another host, eavesdropping data or cause the same network segment can’t

communicate between the individual host.

Switches provide active defense ARP spoofing function, in practical applications, the network hosts the first communication, the Switch will record the ARP table entries, entries in the message of the sender IP, MAC, VID and port correspondence.

To prevent the above mentioned ARP attacks, the Switches launches a comprehensive ARP attack protection solution.

An access Switch is a critical point to prevent ARP attacks, as ARP attacks generally arise from the host side. To prevent ARP attacks, the access Switches must be able to

- Establish correct ARP entries, detect and filter out forged ARP packets, and ensure the validity of ARP packets it forwards
- Suppress the burst impact of ARP packets.

After Configure the access Switches properly, you do not need to deploy ARP attack protection configuration on the gateway. This relieves the burden from the gateway.

If the access Switches do not support ARP attack protection, or the hosts are connected to a gateway directly, the gateway must be configured to

- Create correct ARP entries and prevent them from being modified.
- Suppress the burst impact of ARP packets or the IP packets that will trigger sending of ARP requests.

The merits of Configure ARP attack protection on the gateway are that this gateway configuration hardly affects the Switches and can properly support the existing network, thus effectively protecting user investment.

21.1.1 ARP against ARP Flood

Flood attacks are based on the principle of the general flow of a large number of attack packets in the network equipment such as routers, Switches, and servers, leading to depletion of network equipment, leaving the CPU down the network.

Flood attacks are based on the principle of the general flow of a large number of attack packets in the network equipment such as routers, Switches and servers, leading to depletion of network equipment, leaving the CPU down the network.

ARP flood attack is aimed mainly at the impact of network device's CPU, the core CPU resources leading to depletion. To defend this type of attack, the Switch must determine in advance and to prohibit flood packet forwarding.

Switches 's ARP anti-flood function to identify each ARP traffic, according to the ARP rate setting security thresholds to determine whether the ARP flood attack, when a host's ARP traffic exceeds a set threshold, the Switch will be considered a flood attack , immediately pulled into the black host of the virus, banned from the host and all packet forwarding.

In order to facilitate the management of the network administrator to maintain, the Switches, while the automatic protection will be saved in the system log related to alarms. For disabled users, administrators can set automatic or manual recovery.

Switches on the entire process is as follows:

- Enable ARP anti-flood function will be broadcast ARP packets received on the CPU, according to an ARP packet source MAC address to identify the different streams.

- Set security ARP rate, if the rate exceeds the threshold, the Switch that is ARP attack.
- If you select the above command deny-all, when an ARP traffic exceeds the threshold set, the Switch will determine the source MAC address, the MAC address to the black hole list of addresses to ban this address to forward all subsequent messages.
- If you select the above command deny-arp, ARP traffic when more than a set threshold, the Switch will be judged based on the source MAC address, the address against all subsequent handling of ARP packets.

For recovery to be disabled in the user's forwarding, administrators can set up automatic or manual recovery recovery time in two ways.

21.2 Configure ARP Anti-Spoofing

21.2.1 ARP Anti-Spoofing Configuration List

Configuration Task	Description	Detailed Configuration
Configure Anti-Spoofing	Required	21.2.2
Configure ARP Packet Source MAC Address Consistency Check	Required	21.2.3
Configure Anti-Gateway-Spoofing	Required	21.2.4

21.2.2 Configure Anti-Spoofing

Operation	Command	Remarks

Enter global configuration mode	**system-view**	
Enable ARP anti-spoofing	**arp anti-spoofing**	
Configure the method of unknown static ARP packet	**arp anti-spoofing unknown** { *discard* | *flood* }	

21.2.3 Configure ARP Packet Source MAC Address Consistency Check

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure ARP Packet Source MAC Address Consistency Check	**arp anti-spoofing valid-check**	
validation operation	**display arp anti-spoofing**	

21.2.4 Configure Anti-Gateway-Spoofing

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable arp anti-spoofing	**arp anti-spoofing**	
Enable anti-gateway-spoofing	**arp anti-spoofing deny-disguiser**	
Disable anti-gateway-spoofing	**undo arp anti-spoofing deny-disguiser**	

21.3 Configure against ARP Flood

21.3.1 ARP against ARP Flood Configuration List

Configuration Task	Description	Detailed Configuration
Configure against ARP Flood	Required	21.3.2
Display and Maintain against ARP Flood	Required	21.3.3

21.3.2 Configure against ARP Flood

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable ARP flooding	**arp anti-flood**	
Configure safety trigger threshold	**arp anti-flood threshold** *threshold*	
Configure approach for the attacker	**arp anti-flood action** { **deny-arp** | **deny-all** } **threshold** *threshold*	
Configure automatically banned user recovery time	**arp anti-flood recover-time** *time*	
Banned user manual resume forwarding..	**arp anti-flood recover** { *H:H:H:H:H:H* | *all* }	

21.3.3 Display and Maintain Against ARP Flood

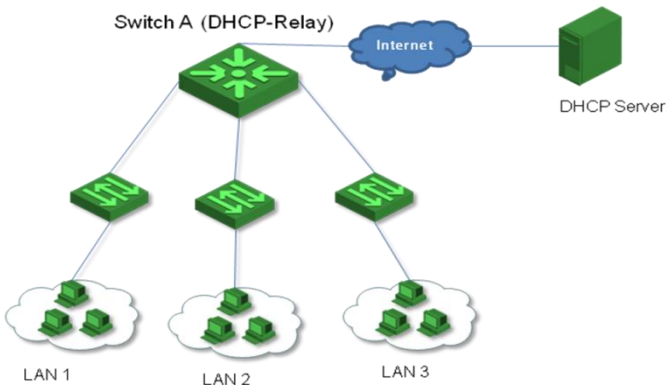
Operation	Command	Remarks
Display ARP anti-flood configuration and attackers list	**display arp anti-flood**	

Chapter 22 DHCP-Relay

22.1 DHCP-Relay Overview

Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

DHCP Relay is designed to address this problem. It enables DHCP clients in a subnet to communicate with the DHCP server in another subnet so that the DHCP clients can obtain IP addresses. In this case, the DHCP clients in multiple networks can use the same DHCP server, which can decrease your cost and provide a centralized administration.



- Typical DHCP relay application

DHCP relays can transparently transmit broadcast packets on DHCP clients or servers to the

DHCP servers or clients in other network segments.

In the process of dynamic IP address assignment through the DHCP relay, the DHCP client and DHCP server interoperate with each other in a similar way as they do without the DHCP relay. The following sections only describe the forwarding process of the DHCP relay.

The DHCP client broadcasts the DHCP-DISCOVER packet.

After receiving the packets, the network device providing the DHCP relay function unicasts the packet to the designated DHCP server based on the configuration.

The DHCP server assigns IP addresses, and then broadcasts the configuration information to the client through the DHCP relay. The sending mode is determined by the flag in the DHCP-DISCOVER packets from the client.

22.2 Configure DHCP-Relay

22.2.1 DHCP-Relay Configuration List

Configuration Task	Description	Detailed Configuration
Configure DHCP Server Group	Required	22.2.2
Configure DHCP Relay to Support Option60	Optional	22.2.3
Enable the DHCP Relay Function	Required	22.2.4
Configure DHCP Option82	Optional	22.2.5

22.2.2 Configure DHCP Server Group

To improve reliability, you can set up multiple DHCP servers in a network. Each DHCP server corresponds to a DHCP server group. After a VLAN or super-VLAN interface references a DHCP server group, it forwards the DHCP packets from the client to all the servers in the server group.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure the DHCP server group	**dhcp-server** *group-id* **ip** *server-ip*	
Enter VLAN interface configuration mode	**dhcp-server** *group-id* **ip** *server-ip*	
Configure the DHCP server group referenced by the interface	**interface vlan-interface** *vid* or **interface supervlan-interface** *super-vid*	
Configure the DHCP server group	**dhcp-server** *group-id*	

22.2.3 Configure DHCP Relay to Support Option60

DHCP relay supports the processing of DHCP packets with option 60 option fields.On the VLAN interfaces or super VLAN configuration option 60 options, when the interface receives a

DHCP packet from the client, if the option60 option field is included in the packet, it will be matched with the value configured on this interface.

If a match is found, the gateway uses the gateway address in the match to relay the packet and forwards the DHCP packet to the server address in the match.

If no match is found, relay processing is performed according to the requested IP address or the client's IP address.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter VLAN interface configuration mode	**interface vlan-interface** *vid* or **interface supervlan-interface** *super-vid*	
Configure option 60 of the interface	**dhcp option60** { **equals** | **starts-with** } { **ascii** *string* | **hexadecimal** *hexdata* } **gateway** *A.B.C.D* [**dhcp-server** *group-id*] [**server-reply** { **ascii** *string* | **hexadecimal** *hexdata* }]	

22.2.4 Enable the DHCP Relay Function

If the DHCP server and the DHCP client are not on the same subnet or the device is configured as a DHCP server, you need to enable the DHCP relay function.

Sometimes, for network security considerations, network administrators do not want the DHCP client to know the address of the DHCP server. In order to meet such requirements, a device that enables a DHCP relay can be configured to hide the address of a real DHCP server. In

this way, the DHCP client regards the device which enables the DHCP relay as a DHCP server to hide the real DHCP server. Of course, if the device that enables the DHCP relay is also a DHCP server, this function is no longer applicable.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable global DHCP relay	**dhcp-relay**	
Hide the IP of the real DHCP Server	**dhcp-relay hide server-ip**	
Configure the maximum number of hops for DHCP messages	**dhcp max-hops** *hops*	

22.2.5 Configure DHCP Option82

The DHCP Option 82 function must be used together with DHCP relay or DHCP snooping.

After the DHCP message received by the Switch already has the Option 82 field, the following three policies are supported:

drop: Drop all DHCP packets that carry the Option 82 field.

keep: Keep Option 82 and forward it.

replace: Replace the existing Option 82 in the packet with the new option82 and forward it according to the actual situation in the local area.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable DHCP Option82	**dhcp option82**	
Configure the DHCP option82 format	**dhcp option82 format** { **normal | verbose | henan** }	
Configure the node-identifier when the DHCP option82 format is verbose	**dhcp option82 format verbose node-identifier** { **mac** | **hostname** | **user-defined** *node-id* }	
Enter port configuration mode	**interface ethernet** *port-id*	
Configure the Switch to process DHCP packets that carry the Option 82 field	**dhcp option82 strategy** { **drop** | **keep** | **replace** | **append** { **hostname** | **hostname-ip** } }	
Configure the circuit-id of DHCP option82	**dhcp option82 circuit-id string** *id*	

Configure Remote Option for DHCP Option82	**dhcp option82 remote-id string** { *string* | **hostname** }	
Display DHCP option82 configuration	**display dhcp option82**	

Chapter 23 DHCP Snooping

23.1 DHCP Snooping Overview

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients. Switches can track DHCP client IP addresses through the DHCP snooping function, which monitors DHCP broadcast packets.

DHCP snooping monitors the following two types of packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

DHCP-ACK packet

DHCP-REQUEST packet

When an unauthorized DHCP server exists in the network, a DHCP client may obtains an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, you can specify a port to be a trust port or an untrusted port by the DHCP snooping function:

Trusted ports can be used to connect DHCP servers or ports of other Switches. Untrusted ports can be used to connect DHCP clients or networks.

Untrusted ports drop the DHCP-ACK and DHCP-OFFER packets received from DHCP servers. Trusted ports forward any received DHCP packets to ensure that DHCP clients can obtain IP addresses from valid DHCP servers.

Trusted vlan: untrusted port will not drop the DHCP-ACK and DHCP-Offer.

23.2 Configure DHCP Snooping

23.2.1 DHCP Snooping Configuration List

Configuration Task	Description	Detailed Configuration
Enable DHCP Snooping	Required	23.2.2
Configure DHCP Snooping Trust port	Required	23.2.3
Configure Max Clients Number	Optional	23.2.4
Configure Link-Down Operation	Optional	23.2.5
Configure IP-Source-Guard	Optional	23.2.6
DHCP Snooping Display and Maintenance	Optional	23.2.7

23.2.2 Enable DHCP Snooping

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable DHCP Snooping	**dhcp-snooping**	

Disable DHCP Snooping	**undo dhcp-snooping**	Disabled by default

23.2.3 Configure DHCP Snooping Trust port

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable interface mode	**interface ethernet** *interface-num*	
Configer trust port	**dhcp-snooping trust**	
Delete trust port	**undo dhcp-snooping trust**	

23.2.4 Configure Max Clients Number

If the attacker exists, it will disguise as multiple users to ask DHCP Server for address to use up the Server allocable address. As a consequence, Server has no address to allocate to the user who needs the IP address. For this problem, network administrator can take the following measures:

Restrict the DHCP-Client number connected to Switch port. In this case, only the clients connected to the same port with the attacker will suffer the attack.

Restrict the DHCP-Client number in specified VLAN. In this case, only the clients in the same VLAN with the attacker will suffer the attack.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Enable interface mode	**interface ethernet** *interface-num*	
Configure max DHCP-Client number connected to Switch port	**dhcp-snooping max-clients** *num*	
Enter vlan configuration mode	**vlan** *vlan-id*	
Configure max DHCP-Client number in specified VLAN	**dhcp-snooping max-clients** *num*	

23.2.5 Configure Link-Down Operation

When the link is down, you can perform the following actions on the dynamic entries which Dhcp-snooping has learned:

enable fast-remove to delete Dhcp-snooping dynamic entries immediately when the port is down.

disable fast-remove to normally age the dynamic entries according to the tenancy term instead of deleting the Dhcp-snooping dynamic entries immediately when the port is down.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure link-down operation of the	**dhcp-snooping port-down-action**	

port	**fast-remove**	
Delete link-down operation of the port	**undo dhcp-snooping port-down-action fast-remove**	

23.2.6 Configure IP-Source-Guard

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports. When using IP-Source-Guard, pay attention:

DHCP-Snooping has been enabled

Use this function in Trust port

After enabling IP-Source-Guard, all traffic with that IP source address is permitted from that trusted client. Traffic from other hosts is denied. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address. The filtering info can be source MAC, source IP and source port number.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	-
Configure IP-source-guard bind table	**ip-source-guardbind** { **ip** *ip-address* | **mac** *mac-address* | **interface ethernet** *interface-num* }	-
Enter interface configuration mode	**interface ethernet** *interface-num*	-
Enable IP-Source-Guard on Trust port	**ip-source-guard**	By default, ip-source-guard

		on port is disabled.

23.2.7 DHCP Snooping Display and Maintenance

Operation	Command	Remarks
Display DHCP-Snooping clients	**display dhcp-snooping clients**	
Display DHCP-Snooping status in interface	**display dhcp-snooping interface** [ethernet *interface-num*]	
Display DHCP-Snooping status in VLAN	**display dhcp-snooping vlan**	
Display IP-Source-Guard status in interface	**display ip-source-guard**	
Display source IP binding table of IP-Source-Guard	**display ip-source-guard bind** [ip *ip-address*]	

Chapter 24 DHCP-Server

24.1 DHCP-Server Overview

In the following cases, the DHCP server is usually used to complete the IP address allocation:

Due to the large scale of the network, manual configuration requires a lot of work and it is difficult to centrally manage the entire network.

Since the number of hosts in the network is larger than the number of IP addresses supported by the network, it is impossible to allocate a fixed IP address to each host. Moreover, there are also restrictions on the number of users accessing the network(for example, service providers of Internet access). Therefore, a large number of users must obtain their own IP address through the DHCP.

Only a few hosts on the network need fixed IP addresses. Most hosts do not have a fixed IP address.

24.2 Configure DHCP-Server

24.2.1 DHCP-Server Configuration List

Configuration Task	Description	Detailed Configuration
Configure IP pool	Required	24.2.2

Configure IP Pool Gateway	Required	24.2.3
Configure IP Pool Range	Optional	24.2.4
Enable/Disable IP Address	Optional	24.2.5
Configure IP Pool Lease	Optional	24.2.6
Configure the DHCP Server to Allocate the DNS Server Address	Optional	24.2.7
Configure the DHCP Server to Assign WINS server Addresses	Optional	24.2.8
Display IP Pool configuration	Optional	24.2.9
Configure dhcp-client bind	Optional	24.2.10

24.2.2 Configure IP Pool

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter IP pool configuration mode	**ip pool** *ippoolname*	
Delete IP Pool	**undo ip pool** *ippoolname*	

24.2.3 Configure IP Pool Gateway

Operation	Command	Remarks

Enter global configuration mode	**system-view**	
Enter ip pool configuration mode	**ip pool** *ippoolname*	
Configure gateway	**gateway** *ip-address mask*	

24.2.4 Configure IP Pool Range

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter IP pool configuration mode	**ip pool** *ippoolname*	
Configure IP pool range	**section** *section-id from-ip to-ip*	
Delete IP pool range	**undo section** *section-id*	

24.2.5 Enable/Disable IP Address

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
enter IP pool configuration mode	**ip pool** *ippoolname*	
Enable/disable IP address	**ip** { **disable** | **enable** } *ip-address*	

24.2.6 Configure IP Pool Lease

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter IP pool configuration mode	**ip pool** *ippoolname*	
Configure IP Pool Lease	**lease** *day:hour:min*	

24.2.7 Configure the DNS Server Address of DHCP Server

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter IP pool configuration mode	**ip pool** *ippoolname*	
Configure the DNS server address	**dns** { **primary-ip** | **second-ip** | **third-ip** | **fourth-ip** } *ip-address*	
Delete the DNS server address assigned for the DHCP client	**undo dns** { **primary-ip** | **second-ip** | **third-ip** | **fourth-ip** }	
Configure the domain name	**dns suffix** *suffix-name*	
Delete the domain name	**undo dns suffix**	

24.2.8 Configure the DHCP Server to Assign WINS Server Addresses

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter IP pool configuration mode	**ip pool** *ippoolname*	
Configure the WINS server address	**wins** { **primary-ip** | **second-ip** } *ip-address*	
Delete the WINS server address	**undo wins** { **primary-ip** | **second-ip** }	

24.2.9 Display IP Pool Configuration

Operation	Command	Remarks
Display IP Pool configuration	**display ip pool** [*ippool-name* [*section-num*]]	

24.2.10 Configure Dhcp-client Bind

Some clients (FTP servers, Web servers, etc.) need fixed IP addresses, which can be implemented by binding the MAC address of the client to the IP address. When a client with this MAC address requests an IP address, the DHCP server searches for the corresponding IP address based on the MAC address of the client and assigns that IP address to the client.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable dhcp-client bind	**dhcp-client bind**	
Disable dhcp-client bind	**undo dhcp-client bind**	
Display dhcp-client bind	**display dhcp-client bind**	
Add dhcp-client	**dhcp-client** *mac-address ip-address vlan-id username*	
Delete dhcp-client	**undo dhcp-client** { *mac-address vlan-id* | all }	
Display dhcp-client	**display dhcp-client** [ip	

	ip-address] | [mac *mac-address*]	

Chapter 25 IGMP Snooping

25.1 IGMP Snooping Overview

IGMP (Internet Group Management Protocol) is a part of IP protocol which is used to support and manage the IP multicast between host and multicast router. IP multicast allows transferring IP data to a host collection formed by multicast group. The relationship of multicast group member is dynamic and host can dynamically add or exit this group to reduce network load to the minimum to realize the effective data transmission in network.

IGMP Snooping is used to monitor IGMP packet between host and routers. It can dynamically create, maintain, and delete multicast address table according to the adding and leaving of the group members. At that time, multicast frame can transfer packet according to his own multicast address table.

25.2 IGMP Snooping Configuration

25.2.1 IGMP Snooping Configuration List

Configuration Task	Description	Detailed Configuration
Enable IGMP Snooping	Required	25.2.2
Configure IGMP Snooping Timer	Optional	25.2.3
Configure Port Fast-leave	Optional	25.2.4

Configure Number of Multicast Group Allowed Learning	Optional	25.2.5
Configure IGMP Snooping Querier	Optional	25.2.6
Configure IGMP Snooping Multicast Learning Strategy	Optional	25.2.7
Configure IGMP Snooping Router-Port	Optional	25.2.8
Configure IGMP Snooping Port Multicast VLAN	Optional	25.2.9
Configure Host Port Record MAC Functions	Optional	25.2.10
Configure Port of Dropped Query Packets or Not	Optional	25.2.11
Configure Port of Discarded Packets Report or Not	Optional	25.2.12
Configure multicast preview	Optional	25.2.13
Configure Profile of Black and White List	Optional	25.2.14
Display and Maintenance of IGMP Snooping	Optional	25.2.15

25.2.2 Enable IGMP Snooping

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Enable IGMP Snooping	**igmp-snooping**	igmp-snooping is disabled by default.
Disable IGMP Snooping	**undo igmp-snooping**	

25.2.3 Configure IGMP Snooping Timer

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure IGMP Snooping host aging time	**igmp-snooping host-aging-time** *seconds*	300s by default
Configure maximum leave time	**igmp-snooping max-response-time** *seconds*	10s by default

25.2.4 Configure IGMP-snooping Fast-leave

Under normal circumstances, IGMP-Snooping on IGMP leave message is received directly will not remove the port from the multicast group, but to wait some time before the port from the multicast group.

Enabling quickly delete function, IGMP-Snooping IGMP leave packet received, directly to the port from the multicast group. When the port is only one user, can be quickly removed to save bandwidth.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Enter port configuration mode	**interface** { { ethernet *interface-num* } | interface-name }	
Configure IGMP-snooping fast-leave	**igmp-snooping fast-leave**	Disable by default

25.2.5 Configure Number of Multicast Group Allowed Learning

Use igmp-snooping group-limit command to configure the number of the multicast group allowed learning.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface** { { ethernet *interface-num* } | interface-name }	
Configure the number of the multicast group allowed learning	**igmp-snooping group-limit** *number*	

25.2.6 Configure IGMP Snooping Querier

In an IP multicast network running IGMP, a multicast router or Layer 3 multicast Switch is responsible for sending IGMP general queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer .This router or Layer 3 Switch is called IGMP querier.

However, a Layer 2 multicast Switch does not support IGMP, and therefore cannot send general queries by default. By enabling IGMP Snooping on a Layer 2 Switch in a VLAN where multicast traffic needs to be Layer-2 Switched only and no multicast routers are present, the

Layer 2 Switch will act as the IGMP Snooping querier to send IGMP queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configuration is not black and white list in the multicast group to learn the rules of the default	**igmp-snooping** { **permit** | **deny** } { **group all** | **vlan** *vlan-id* }	By default, not black and white list in the multicast group to learn the rules for the learning of all multicast group
Enter port configuration	**interface ethernet** *interface-num*	
Configure the port multicast black list	**igmp-snooping** { **permit** | **deny** } **group-range** multicast-*mac-address* **multi-count** *num* **vlan** *vlan-id*	Configure the port to learn (not learn) VID of the start of continuous num mac multicast groups
Configure the port multicast black list	**igmp-snooping** { **permit** | **deny** } **group** multicast-*mac-address* **vlan** *vlan-id*	By default, any multicast group

		are not black and white list are added

25.2.7 Configure IGMP Snooping Multicast Learning Strategy

Configured multicast learning strategies, the administrator can control the router only to learn the specific multicast group. If a multicast group is added to the blacklist, then the router will not learn the multicast group; the contrary, in the white list in the router can learn multicast group.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Open the IGMP-Snooping querier	**igmp-snooping querier**	
Configure VLAN general query messages	**igmp-snooping querier-vlan** *vlan-id*	
Configured to send general query message interval	**igmp-snooping query-interval** *interval*	
Configuration is generally the maximum query response time of message	**igmp-snooping query-max-respond** *time*	
Configured to send general inquiries packet source IP address	**igmp-snooping general-query source-ip** *ip-address*	

25.2.8 Configure IGMP Snooping Router-Port

You can configure the router port will be automatically added to the dynamic IGMP Snooping Multicast learn to make routing port also has a multicast packet forwarding capability.

When the Switch receives a host membership report sent packets, the port will be forwarded to the route.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure hybrid routing port	**igmp-snooping route-port forward**	
Configure dynamic routing port aging time	**igmp-snooping router-port-age** { **on** | **off** | *age-time* }	
Configure static routing port	**igmp-snooping route-port vlan** *vlan-id* **interface** { all | ethernet *interface-num* }	

25.2.9 Configure IGMP Snooping Port Multicast VLAN

Multicast VLAN on the port function, regardless of the port receiving the IGMP messages belong to which VLAN, the Switch will be modified as a multicast VLAN.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**Interface ethernet** *interface-num*	
Configure IGMP Snooping port multicast VLAN	**igmp-snooping multicast vlan** *vlan-id*	

25.2.10 Configure Host Port Record MAC Functions

When this feature is enabled on the port, the Switch will record the source packet IGMP report MAC address.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**Interface ethernet** *interface-num*	
Configure the host port record MAC	**igmp-snooping record-host**	

25.2.11 Configure Port of Dropped Query Packets

When this feature is enabled on a port, the Switch drops the IGMP query message. Default port to receive all IGMP packets.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Discard the query message to the configuration port	**igmp-snooping drop query**	
Configure the port to receive the query message	**undo igmp-snooping drop query**	

25.2.12 Configure Port of Discarded Report Packets

When this feature is enabled on a port, the Switch drops the IGMP report message. Default port to receive all IGMP packets.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Enter port configuration mode	**interface ethernet** *interface-num*	
Configure the port discarded packets report	**igmp-snooping drop report**	
Configure the port to receive a report with	**undo igmp-snooping drop report**	

25.2.13 Configure Multicast Preview

Multicast IGMP Snooping provides preview feature, users can configure the multicast channel preview, you can configure a single multicast length preview, preview interval, duration, and reset to allow preview times.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure Multicast preview	**igmp-snooping preview**	
Configure multicast channel preview	**igmp-snooping preview group-ip** *ip-address* **vlan** *vlan-id* **interface ethernet** *interface-num*	
Configuration when the long single preview, preview interval, duration and allows preview preview reset the number of	**igmp-snooping preview** { time-once *time-once* | time-interval *time-interval* | time-reset *time-reset* | permit-times *preview-times* }	

25.2.14 Configure Profile of Black and White List

IGMP Snooping provides the way black and white list feature profile, first in global configuration mode to create a number of profile, then the port configuration mode to configure the port reference profile list. Users can configure the IGMP Snooping profile of the type and scope, which refers to the type of permit / deny, you can use the multicast IP address range or MAC address to configure. IGMP Snooping profile only the port referenced to take effect, the configuration port reference profile, the more the type of profile must be the same between that port can only refer to the same type (permit or deny) the profile. When the port is referenced permit the profile, the profile can only learn the definition of the corresponding multicast group; when the port reference deny the profile, the profile can be defined in addition to learning outside of all multicast group; when the port does not refer to any profile, in accordance with Normally learning multicast group.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Create a profile, and enter profile configuration mode	**igmp-snooping profile** *profile-id*	
Configuration profile types	**profile limit** { **permit** | **deny** }	
Configuration profile ip range	**ip range** *start-ip end-ip* [vlan *vlan-id*]	
Range of configuration profile mac	**mac range** *start-mac end-mac* [vlan *vlan-id*]	
Enter port configuration mode	**interface ethernet** *interface-num*	
Reference configuration profile	**igmp-snooping profile refer** *profile-list*	

25.2.15 Display and Maintenance of IGMP Snooping

After completing the above configuration, can use the following command to view configuration.

Operation	Command	Remarks
See the related configuration IGMP Snooping	**display igmp-snooping**	
See dynamic routing port	**display igmp-snooping router-dynamic**	
Display static router port configuration	**display igmp-snooping router-static**	
Display Record in host MAC	**display *igmp-snooping* record-host** [interface ethernet *interface-num*]	
Display information about multicast preview	**display igmp-snooping preview**	
Display the current state of multicast channel preview	**display igmp-snooping preview status**	
Display profile configuration information	**display igmp-snooping profile** [interface ethernet *interface-num*] [*profile-list*]	
Display multicast group	**display multicast** [interface ethernet *interface-num*]	

Chapter 26 MLD Snooping

26.1 MLD Snooping Overview

MLD (Multicast Listener Discovery) Internet Group Management Protocol is part of the IPv6 protocol, to support and manage hosts and multicast routers IP multicast. IP Multicast allows the transmission of IP packets to a multicast group constitutes a set of host, multicast group membership relationship is dynamic, host can dynamically join or leave the group, so to minimize the network load, effective online data transfer.

MLD Snooping is used to monitor hosts and routers between the MLD messages, according to group members join, leave, and dynamically create, maintain and delete the multicast address table, this time, multicast frames based on their respective multicast address table be forwarded.

26.2 MLD Snooping

26.2.1 MLD Snooping Configuration List

Configuration Task	Description	Detailed Configuration
Start MLD Snooping	Required	26.2.2
Configure MLD Snooping Timer	Optional	26.2.3
Configure Fast-leave Port	Optional	26.2.4

Maximum number of learning multicast configuration port	Optional	26.2.5
Configure MLD-Snooping Multicast Learning Strategies	Optional	26.2.6
Configure MLD-Snooping querier	Optional	26.2.7
Configure Routing port	Optional	26.2.8
Multicast VLAN port configuration	Optional	26.2.9
Display and maintenance of MLD Snooping	Optional	26.2.10

26.2.2 Start MLD Snooping

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Start MLD Snooping	**mld-snooping**	

26.2.3 Configure MLD Snooping Timer

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure dynamic multicast member port aging time	**mld-snooping host-aging-time** *time*	300s by default
Configure the maximum response time to leave	**mld-snooping max-response-time** *time*	10s by default

26.2.4 Configure Fast-leave Port

Under normal circumstances, MLD-Snooping in MLD leave message is received directly will not remove the port from the multicast group, but to wait some time before the port from the multicast group.

Start quickly delete function, MLD-Snooping received MLD leave message, the direct port from the multicast group. When the port is only one user, it can be quickly removed to save bandwidth.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Fast-leave configuration port	**mld-snooping fast-leave**	

26.2.5 Maximum Number of Learning Multicast Configuration Port

You can use the following command to set up each port can learn the number of multicast.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configured port number of the largest study of multicast	**mld-snooping group-limit** *number*	By default, the maximum learning of multicast port number NUM_MULTICA

		ST_GROUPS

Caution:

NUM_MULTICAST_GROUPS refers to the machine can learn the maximum number of multicast, each product NUM_MULTICAST_GROUPS may be different. Although theoretically a maximum of learning multicast port number NUM_MULTICAST_GROUPS, but also that other ports can learn the number of multicast will be occupied. In other words, all the ports will share this NUM_MULTICAST_GROUPS multicast group resources.

26.2.6 Configure MLD Snooping Multicast Learning Strategies

Configured multicast learning strategies, the administrator can control the router only to learn the specific multicast group. If a multicast group is added to the blacklist, then the router will not learn the multicast group; the contrary, in the white list in the multicast group of routers can be learned.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configuration is not black and white list in the multicast group to learn the rules of the default	**mld-snooping** { permit | deny } { group all | vlan *vlan-id* }	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configure the port multicast black list	**mld-snooping** { permit | deny } **group-range** *multicast-address* **multi-count** *num* **vlan**	

	vlan-id	
Configure the port multicast black list	**mld-snooping** { permit | deny } **group** *multicast-address* **vlan** *vlan-id*	

26.2.7 Configure MLD-Snooping querier

After running the MLD protocol multicast network, there will be a full-time query multicast router or Layer 3 multicast router is responsible for sending MLD query.

However, MLD does not support Layer 2 Switch function, so no way to query device capabilities, universal group can't send query message. Users can configure MLD-Snooping querier, the Switch to the second floor take the initiative in the data link layer to send general queries, messages, in order to establish and maintain multicast forwarding entry.

Users can also configure the MLD Snooping querier sends general query messages with the source address, the maximum response time and query cycle.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
On MLD-Snooping querier	**mld-snooping querier**	
Configured to send general query message interval	**mld-snooping query-interval** *interval*	
Configuration is generally the maximum query response time of message	**mld-snooping query-max-respond** *time*	

26.2.8 Configure Routing Port

You can configure the router port will be automatically added to the dynamic MLD Snooping Multicast learn to make routing port also has a multicast packet forwarding capability.

When the Switch receives a host membership report sent packets, the port will be forwarded to the route.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Hybrid routing port configuration function	**mld-snooping route-port forward**	
Configure dynamic routing port aging time	**mld-snooping router-port-age** { on | off | *age-time* }	
Configure static routing port	**mld-snooping route-port vlan** *vlan-id* **interface** { all | ethernet *interface-num* }	

26.2.9 Multicast VLAN Port Configuration

Multicast VLAN on the port function, regardless of the port received MLD messages belong to which VLAN, the Switch will be modified as a multicast VLAN.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Multicast VLAN port configuration	**mld-snooping multicast vlan** *vlan-id*	

26.2.10 Display and Maintenance of MLD Snooping

After completing the above configuration, can use the following command to view configuration.

Operation	Command	Remarks
See related MLD Snooping Configuration	**display mld-snooping**	
See dynamic routing port	**display mld-snooping router-dynamic**	
View static router port configuration	**display mld-snooping router-static**	
View multicast group	**display mld-snooping group**	

Chapter 27 Static Multicast Table

27.1 Static Multicast Table Overview

In addition to dynamic learning, multicast tables support manually configuration, and a manually configured multicast table is a static multicast table. The static multicast MAC table will not be aged and it cannot be lost after being saved.

At present, only the corresponding multicast entries of ipv4 can be static configured, and ipv6 multicast entries cannot be static configured.

27.2 Configure Static Multicast Table

27.2.1 Static Multicast GroupConfiguration List

Configuration Task	Description	Detailed Configuration
Create a Static Multicast Group	Required	27.2.2
Add a Port to the Multicast Group	Required	27.2.3
Create a Static Multicast Group based on Group IP	Optional	27.2.4
Display and Maintenance of Static MulticastTable	Optional	27.2.5

27.2.2 Create a Static Multicast Group

Operation	Command	Remarks

Enter global configuration mode	**system-view**	
Create a static multicast group	**multicast mac-address** *mac-address* **vlan** *vlan-id*	
Delete a static multicast group	**undo multicast** [mac-address *mac-address* vlan *vlan-id*]	

The parameter mac refers to the mac address of the multicast group. It is required to use the multicast address format, for example: 01: 00: 5e: **: **: **, ip refers to multicast ip, for example, 224.0.1.1; vlan-id refers to VLAN ID, with the range of 1 to 4094. It must be an existed VLAN. If the added static multicast group belongs to a VLAN that does not exist,, the multicast group fails to be added.

27.2.3 Add a Port to the Multicast Group

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Add a port to a static multicast group	**multicastmac-address** *mac-address* **vlan** *vlan-id* **interface** { all | ethernet *interface-list* }	
Delte a por from static multicast group	**undo multicast mac-address** *mac-address* **vlan** *vlan-id* **interface** { all | ethernet *interface-list* }	

27.2.4 Create a Static Multicast Group based on Group IP

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Create a static multicast group based on group IP	**multicast ip-address** *ip-address* **vlan** *vlan-id*	
Delete a static multicast group based group IP	**undo multicast ip-address** *ip-address* **vlan** *vlan-id*	
Add a port to a static multicast group base on group IP	**multicast ip-address** *ip-address* **vlan** *vlan-id* **interface** { all | ethernet *interface-list* }	
Delte a por from static multicast group base on group IP	**undo multicast ip-address** *ip-address* **vlan** *vlan-id* **interface** { all | ethernet *interface-list* }	

27.2.5 Display and Maintenance of Static Multicast Table

Operation	Command	Remarks
DisplayStatic MulticastTable by MAC	**display multicast mac-address** *mac-address*	
DisplayStatic MulticastTable by IP	**display multicast ip-address** *ip-address*	

Chapter 28 IGMP

28.1 IGMP Overview

IGMP (Internet Group Management Protocol) is used to manage IP multicast group member as well as to establish and maintain the relationship between the IP host and multicast router.

Currently, there are three versions of IGMP: IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) and IGMPv3 (RFC 3376). The IGMPv2 version is widely used.

IGMPv1 defines two types of message: General Query and Group Membership Report. It manages the multicast group members based on query mechanism and response mechanism.

IGMPv2 defines three types of message: Membership Query (including General Query and Group-Specific Query), Group Membership Report and Group Membership-Leave. Compared with IGMPV1, IGMPV12 added querier election mechanism and leave group mechanism.

IGMPv3 added source filter mechanism on the basis of v2, enhancing the function of query and report. Moreover, it presents the clear requirements to accept or reject the multicast message from some certain multicast source when the host adds certain multicast group.

All versions support ASM mode. Only IGMPv3 supports SSM mode. IGMPv1 and IGMPv2 can be able to apply to SSM mode under the help of IGMP SSM Mapping technology.

28.2 Configure IGMP

28.2.1 IGMP Configuration List

Configuration Task	Description	Detailed Configuration
Enable Multicast Routing Protocol	Required	28.2.2
Enable IGMP Protocol	Required	28.2.3
Configure IGMP Version	Optional	28.2.4
Configure IGMP General Query Interval	Optional	28.2.5
Configure Last-Member-Query-Interval	Optional	28.2.6
Configure Robustness Variable of IGMP Querier	Optional	28.2.7
Configure the Maximum Number of the Multicast Group Added to the Interface	Optional	28.2.8
Configure IGMP Maximum Query Response Time	Optional	28.2.9
Configure Multicast Group Filter Function	Optional	28.2.10
Establish Static IP Multicast Table	Optional	28.2.11
Configure Static Multicast Group	Optional	28.2.12
Configure IGMP Proxy	Optional	28.2.13
Configure IGMP SSM Mapping	Optional	28.2.14
Configure SSM-Mapping static group address mapping rule	Optional	28.2.15
IGMP Display and Maintenance	Optional	28.2.16

28.2.2 Enable Multicast Routing Protocol

You should enable multicast routing before Configure IGMP protocol. Only if you enable the multicast protocol can relative configurations take effect.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enable enable multicast routing	**ip multicast-routing**	
Disable multicast routing	**undo ip multicast-routing**	

28.2.3 Enable IGMP Protocol

Enable the IGMP protocol on interface to make Switch forward multicast message. Please perform the configurations under interface configuration mode (including VLAN interface and SuperVlan interface).

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Enable IGMP protocol	**ip igmp**	
Disable IGMP protocol	**undo ip igmp**	

28.2.4 Configure IGMP Version

Due to different versions of the IGMP protocol have different message structures and message types, so you need to configure the same IGMP version for all the routers in the same network segment. Otherwise, IGMP cannot be able to run normally. Please perform the configurations

under interface configuration mode (including VLAN interface and SuperVlan interface).

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configure the interface to run IGMP version	**ip igmp version** { 1 | 2 | 3 }	IGMPv2 by default
Configure defaultIGMPversion	**undo ip igmp version**	

28.2.5 Configure IGMP General Query Interval

The Ethernet Switch periodically sends the Membership Query Message to discover which multicast groups exist on the network connected to the Ethernet Switch. This time interval is set by the Query Interval timer. You can configure the Query Interval timer to modify the interval at which IGMP hosts send query messages.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configure IGMP general query interval	**ip igmp query-interval** *seconds*	125 seconds by default.
Configure default IGMP general query interval	**undo ip igmp query-interval**	

28.2.6 Configure Last-Member-Query-Interval

After receiving leave-message, Switch will forward specified group query message to know whether there are other group members in multicast group. User can be able to modify the interval value of specified group query message.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configure last-member-query-interval	**ip igmp last-member-query-interval** *seconds*	1 second by default.
Configure default last-member-query-interval	**undo ip igmp last-member-query-interval**	

28.2.7 Configure Robustness Variable of IGMP Querier

The robustness variable is a very important parameter that reflects the performance of the IGMP protocol running on the Switch. It is mainly used to control message forwarding frequency so as to enhance the robustness of network protocol operation. In addition, the robustness variable coefficient is also an important parameter for calculating other variables, such as the existence time of other inquires, group membership time, etc.

Operation	Command	Remarks
Enter global configuration	**system-view**	

Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configure robustness variable of IGMP querier	**ip igmp robustness-variable** *value*	2 by default.
Configure default robustness variable of IGMP querier	**undo ip igmp robustness-variable**	

28.2.8 Configure the Maximum Number of the Multicast Group Added to the Interface

Through this function, users can easily control the number of multicast groups that an interface can join. If the maximum number is exceeded, the Switch will not process the newly added IGMP messages.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configure the maximum number of the multicast group added to the interface	**ip igmp limit-group** *limit-num*	By default, the maximum number of IGMP groups added to an interface is the maximum

		number of multicast groups
Configurethe default maximum number of the multicast group added to the interface	**undo ip igmp limit-group**	

28.2.9 Configure IGMP Maximum Query Response Time

When the host receives the query from the Switch, it will start the Delay Timers for each multicast group it joins. It uses a random number between 0 and Max Response Time as the initial value. The Max Response Time is the maximum response time specified by the query message (the maximum query response time for IGMP Version 1 is 10 seconds). The host should inform Switch the member of the multicast group before the timer expired. If the Switch does not receive any group member reports after the maximum query response time has expired, it considers that there is no local group member and it will not send the multicast packets it receives to the network to which it is connected.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configure the maximum query response time of IGMP	**ip igmp query-max-response-time** *seconds*	10 seconds by default
Configure the default maximum	**undo ip igmp query-max-response-time**	

query response time of IGMP		

28.2.10 Configure Multicast Group Filter Function

The Switch determines which multicast group includes the local group members that are directly connected to the Switch by sending an IGMP query message. If you do not want to add certain multicast groups to a host on the network segment where the interface is located, you can configure the ACL rule on the interface. The interface filters the received IGMP report according to the rule. The multicast group maintains the group membership.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configure filter function of multicast group	**ip igmp access-group** *acl-number* [all | ethernet*interface-list*]	By default, hosts on this interface can join any valid multicast group.
Delete filter function of multicast group	**undo ip igmp access-group** *acl-number* [all | ethernet*interface-list*]	

28.2.11 Establish Static IP Multicast Table

Create a static IP multicast entry to realize the forwarding of multicast message. You can create (S, G) and (*, G) entries. If a static multicast member exists (which is created through

the command of ip igmp static-group), It will automatically add the static member's port to the egress port of the corresponding static entry.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Create static IP multicast table	**ip igmp create-group** *groups-address-list* **source** { * | *source-address* }	There is no static multicast table by default.
Delete static IP multicast table	**undo ip igmp create-group** *groups-address-list* **source** { * | *source-address* }	

28.2.12 Configure Static Multicast Group

Configure the Switch port to become a static multicast group so that the Switch can forward the multicast packets to this port and specify the source address list at the same time. Please perform the configurations under interface configuration mode (including VLAN interface and SuperVlan interface). When Configure this function under the SuperVlan interface mode, you should specify the sub-VLAN.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface |	

	supervlan-interface } *vlan-id*	
Add a port into static multicast group	**ip igmp static-group** { ***** **|** *groups-address* } { all | ethernet *interface-list* } **sourcelist** { * | *sourcelist* }	
Delete a port from static multicast group	**undo ip igmp static-group** { all | *groups-address* { all | ethernet *interface-list* } sourcelist { * | *sourcelist* } }	

28.2.13 Configure IGMP Proxy

After enabling IGMP proxy, Switch acts as a host forwards the multicast group information via report message. When the multicast router receives the message, it transmits the multicast traffic to Switch and then Switch will transmit the multicast traffic to the downlink user. If a certain multicast has no host, Switch will forward leave message to multicast routing, and then multicast routing will stop forwarding multicast data to Switch. This function is mainly applied to network peripheral Switches, which effectively saves Switch resources since Switches can complete the multicast forwarding without enabling the multicast routing protocols.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Enable IGMP-Proxy	**igmp-proxy**	
Disable IGMP-Proxy	**undo igmp-proxy**	

28.2.14 Configure IGMP SSM Mapping

In the SSM network, some recipient hosts only run IGMPv1 or IGMPv2 due to the variety of possible restrictions. You can configure the IGMP SSM Mapping function in router so as to offer SSM service to those recipient hosts of IGMPv1 or IGMPv2.

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter VLAN-interface mode	**Interface** { vlan-interface | supervlan-interface } *vlan-id*	
Enable ssm-mapping	**ip igmp ssm-mapping**	
Disable ssm-mapping	**undo ip igmp ssm-mapping**	

28.2.15 Configure SSM-Mapping static group address mapping rule

Operation	Command	Remarks
Enter global configuration	**system-view**	
Enter IGMP global configuration mode	**mroute igmp**	
Configure the SSM-Mapping static group address mapping rule	**ssm-mapping** *ipaddress mask multicast-source-ipaddress*	By default, no static group address mapping rule is configured

Delete the SSM-Mapping static group address mapping rule	**undo ssm-mapping** { *ipaddress mask* | all }	

28.2.16 IGMP Display and Maintenance

Operation	Command	Remarks
Display IGMP interface information	**display ip igmp interface** [{ vlan-interface *vlan-id* } | { supervlan-interface *vlan-id* }]	
Display static configurations and the IGMP multicast group information	**display ip igmp groups** [*multicast-ip*]	
Display IGMP proxy	**display igmp-proxy**	
Display SSM-Mapping mapping rule	**display ip igmp ssm-mapping** [*multicast-ip*]	

Chapter 29 PIM

29.1 PIM Overview

Protocol Independent Multicast-Dense Mode (PIM-DM) is a dense-mode multicast routing protocol, which is applicable to small-sized networks. In a PIM-DM network, members of a multicast group are densely distributed.

29.1.1 Principles of PIM-DM

The operation of PIM-DM can be understood as neighbor discovery, flooding-prune, and graft.

1) Neighbor discovery

   Upon save, a PIM-DM router needs to discover neighbors by sending Hello packets. The relationships between PIM-DM capable network nodes are maintained through exchange of Hello packets. In PIM-DM, Hello packets are sent periodically.

2) Flooding&Prune

   PIM-DM assumes that all the hosts on a network are ready to receive multicast data. A packet is transmitted from multicast source S to multicast group G. After receiving this multicast packet, the router performs an RPF check based on the unicast routing table and creates an (S,G) entry if the RPF check is successful. Then the router floods the packet to all the downstream PIM-DM nodes in the network. The router discards the packet if the RPF check fails (the multicast packet is from an incorrect interface). In the

flooding process, an (S,G) entry will be created in the PIM-DM multicast domain.

If no downstream node is a multicast group member, the router sends a Prune message to notify the upstream node that data should not be sent to downstream nodes any more. After receiving the Prune message, the upstream node removes the interface that sends the multicast packet from the outbound interface list matching the (S,G) entry. Eventually, a Shortest Path Tree (SPT) with S as the root is created. The prune process is initiated by a leaf router.

The whole process is called the flooding&prune process. A timeout mechanism is made available on a pruned router so that the router may initiate a flooding&prune process again if the prune process times out. The flooding&prune mechanism of PIM-DM operates periodically over and over again.

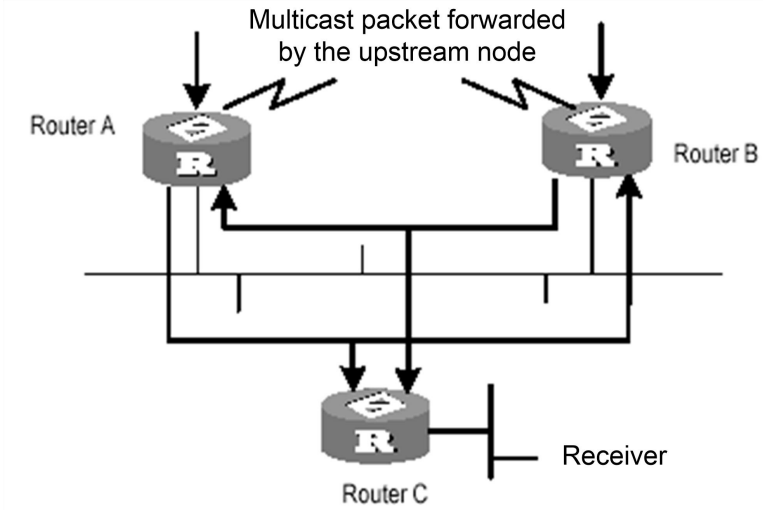
In the flooding&prune process, PIM-DM performs RPF check and builds a multicast forwarding tree with the data source as the root based on the current unicast routing tables. When a multicast packet arrives, the router first judges whether the path of the multicast packet is correct. If the interface where the packet arrives is what specified in the unicast route, the path is considered correct. Otherwise, the multicast packet is discarded as a redundant packet and will not be forwarded in multicast mode. The unicast route may be discovered by any unicast routing protocol such as RIP and OSPF instead of a specific routing protocol.

3) Assert

As shown in the following figure, multicast routers A and B are on the same LAN segment and they have their respective paths to multicast source S. After receiving a multicast

packet from S, both of them will forward the packet on the LAN. As a result, the downstream multicast router C will receive two identical multicast packets.

An upstream router uses the Assert mechanism to select the only forwarder. The upstream router sends Assert messages to select the best route. If two or more paths have the same priority and metric value, the router with the largest IP address is selected as the upstream neighbor of the (S,G) entry and is responsible for forwarding the (S,G) multicast packet.



Assert mechanism

4) Graft

When the pruned downstream node needs to enter the forwarding state again, it sends a Graft message to the upstream node. Before Configure the features of IGMP, you must enable the multicast routing function.

5) SRM

To avoid repeated flooding&prune actions, the SRM is added to new protocol standards. The router in direct connection with the multicast source sends state update packets periodically. After receiving a state update packet, the PIM-capable router refreshes the prune state.

29.1.2 Principles of PIM-SM

The operation of Protocol Independent Multicast-Sparse Mode (PIM-SM) can be understood as neighbor discovery, rendezvous point tree (RPT) generation, multicast source registration, and SPT Switch. The neighbor discovery of PIM-SM is the same as that of PIM-DM.

1) RPT generation

When a host joins a multicast group (G), the leaf router which is directly connected with the host if detecting receivers of G by sending IGMP packets, calculates an RP for G and sends a Join message to an upper-level node of the RP for participating in the multicast group. Every router between the leaf router and the RP will generate a (*,G) entry in its forwarding table and therefore they will forward any packets destined for G regardless of where the packets come from. When the RP receives a packet bound for G, the packet will later be sent to the leaf router along the established path and then reach the host. Finally an RPT with the RP as the root is created.

2) Multicast source registration

When multicast source S is sending a multicast packet to multicast group G, the PIM-SM router which is directly connected with S encapsulates the multicast packet into a registration packet and then sends it to an RP in unicast mode. If multiple PIM-SM routers exist on a network

segment, the designated router (DR) sends the multicast packet.

29.1.3 Principles of PIM-SSM

PIM-Source Specific Multicast (PIM-SSM) is dependent on PIM-SM and they may coexist on a router. Whether PIM-SSM or PIM-SM is used is subject to the multicast address in a data or protocol packet. IANA assigns SSM an address segment (232.0.0.0 to 232.255.255.255). The multicast groups on this address segment will not join an RPT but is processed by SSM. In PIM-SSM, Hello packets are also transmitted periodically between routers for neighbor discovery and DR election.

Usually IGMPv3 is deployed on the host to establish and maintain multicast group memberships. Compared with IGMPv2, IGMPv3 is designed with the source-based filtering function. This function allows a host to receive only the data from a specific group and even from a specific source in this group. Based on a received IS_IN packet of IGMPv3, the SSM-enabled router learns that a host on the network connected with the interface receiving the IS_IN packet wants to receive (S,G) packets. This router unicasts a PIM (S,G) Join message to the next-hop router of the multicast source hop by hop and thereby an SPT can be established between the multicast source and the last-hop router. When the multicast source is sending multicast data, the data reaches the receiver along the SPT.

If a host supports only IGMPv1/IGMPv2, you can configure SSM mapping on the router connected with the host to convert the (*,G) Join messages of IGMPv1/IGMPv2 into (S,G) Join messages.

29.2 Configure PIM

29.2.1 PIM Configuration List

The operations listed in the tablemust be performed sequentially during PIM configuration. It is recommended that PIM-DM be enabled on all the interfaces of a non-border router running in PIM-DM domains. In contrast, PIM-SM does not need to be enabled on every interface.

Configuration Task	Description	Detailed Configuration
Basic PIM Configuration	Required	29.2.2
Advanced PIM Configuration	Required	29.2.3

29.2.2 Basic PIM Configuration

Operation	Command	Remarks
Enables PIM-DM on an interface.	**ip pim dense-mode**	
Disables PIM-DM on an interface.	**undo ip pim dense-mode**	
Enables PIM-SM on an interface.	**ip pim sparse-mode**	
Disables PIM-SM on an interface.	**undo ip pim sparse-mode**	

Note:

Enable a multicast protocol before PIM-SM on an interface.

29.2.3 Advanced PIM Configuration

Operation	Command	Remarks

Configures the transmission interval of Hello packets.	**ip pim query-interval** *seconds*	
Restores the default transmission interval.	**undo ip pim query-interval**	
Configures an interface as the border of a BSR.	**ip pim bsr-border**	
Deletes the BSR border configuration of an interface.	**undo ip pim bsr-border**	
Enters the PIM mode.	**pim**	
Quits the PIM mode.	**quit**	
Filters the received multicast packets based on the source.	**source-policy** *acl-number*	
Cancels source-based filtering.	**undo source-policy**	
Filters PIM neighbors.	**ip pim neighbor-policy** *acl-number*	
Cancels PIM neighbor filtering.	**undo ip pim neighbor-policy**	
Configures the maximum of PIM neighbors for an interface.	**ip pim neighbor-limit** *limit*	
Restores the default value.	**undo ip pim neighbor-limit**	
Configures a static RP.	**static-rp** *address*	
Deletes a static RP.	**undo static-rp**	
Configures a C-BSR.	**bsr-candidate** *interface-type*	

	interface-number hash-mask-length priority	
Deletes a C-BSR.	**undo bsr-candidate**	
Configures a C-RP.	**rp-candidate** *interface-type interface-number* **group-list** *acl-number priority*	
Deletes a C-RP.	**rp-candidate** *interface-type interface-number* **group-list** *acl-number*	
Configures a Switching threshold.	**spt-threshold** { *immediately* | *infinity* }	
Restores the default Switching threshold.	**undo spt-threshold**	
Displays the information of PIM interfaces.	**display ip pim interface** [**vlan-interface** ***vid***]	
Displays the information of PIM neighbors.	**display ip pim neighbor**	
Displays the multicast routing tables learned by PIM, including static and dynamic routing entries.	**display ip mroute** *group-address* [*static* | *dynamic*]	
Displays dynamic and static RPs of PIM.	**display ip pim rp-info** *group-address*	
Displays the information of BSRs, including the elected BSR and local	**display ip pim bs**	

C-BSRs.		
Displays the range of SSM group addresses.	**display ip pim ssm range**	
Configures the range of an SSM multicast group.	**ssm** { **default** | **range** *acl* }	
Deletes the configuration of the range of an SSM multicast group.	**undo ssm** { **default** | **range** *acl* }	

Note: Be sure to enable PIM on an interface before Configure the PIM attributes of the interface. This point must be noted when you use the commands for Configure interface attributes and will not be given again.

Ensure that all the devices in the domain are configured with the same range of SSM multicast group addresses. Otherwise, multicast information cannot be transmitted using the SSM model.

If members of an SSM multicast group send Join messages over IGMPv1 or IGMPv2, (*,G) Join messages will not be triggered.

Chapter 30 SNTP

30.1 SNTP Overview

The Simple Network Time Protocol Version 4 (SNTPv4), which is a subset of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. In common, there is at least one server in the network, it provides reference time for clienets, finally, all clients in the network synchronized local clocks.

30.1.1 SNTP Operation Mechanism

SNTPv4 can be worked in four modes: unicast, multicast, broadcast and anycast. In unicast mode, client actively sends a request to server, and server sends reply packet to client according to the local time structure after receiving requirement.

In broadcast and multicast modes, server sends broadcast and multicast packets to client periodically, and client receives packet from server passively.

In anycast mode, client actively sends request to local broadcast or multicast address, and all servers in the network will reply to the client. Client will choose the server whose reply packet is first received to be the server, and drops packets from others. After choosing the server, working mode is the same as that of the unicast.

In all modes, after receiving the reply packet, client resolves this packet to obtain current

standard time, and calculates network transmit delay and local time complementary, and then adjusts current time according them.

30.2 Configure SNTP Client

30.2.1 SNTP Client Configuration List

Configuration Task	Description	Detailed Configuration
Enable SNTP client	Required	30.2.2
Modify SNTP client mode	Optional	30.2.3
Configure SNTP sever IP address	Optional	30.2.4
Modify broadcast transfer delay	Optional	30.2.5
Configure multicast TTL	Optional	30.2.6
Configure interval polling	Optional	30.2.7
Configure overtime retransmit	Optional	30.2.8
Configure valid sever list	Optional	30.2.9
Configure MD5 authentication	Optional	30.2.10
Display and maintain SNTP client	Optional	30.2.11

30.2.2 Enable SNTP Client

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable SNTP client	**sntp client**	

Disable SNTP client	**undo sntp client**	

30.2.3 Modifying SNTP Client Operating Mode

Administrators can modify SNTP operating mode according to the network------ unicast, multicast, broadcast or anycast.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
modifying SNTP client Operation mode	**sntp client mode** { **broadcast** | **unicast** | **multicast** | **anycast** [**key** *key*] }	Broadcast modeby default

30.2.4 Configure SNTP Sever Address

SNTP client must configure appointed SNTP sever in the unicast way. You can also use below Commands to configure key when connecting to SNTP server by authentication.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
configure SNTP sever address	**sntp server** *IP* [**key** *key*]	

30.2.5 Modifying Broadcast Transfer Delay

When SNTP client works in the broadcast or multicast way, it needs to use broadcast transfer delay. In the broadcast way, the local time of SNTP client equals the time receiving from sever adds transferring time. Administrators modify the transferring time according to the actual bandwidth in the network.

Operation	Command	Remarks

Enter globally configuration mode	**system-view**	
configure broadcast transfer delay	**sntp client broadcastdelay** *time*	3ms by default

30.2.6 Configure Multicast TTL

To restrict the pass range of multicast message, SNTP client needs configure the sending multicast TTL when working both in the any cast and in the request way of forwarding the multicast address.

Operation	Command	Remarks
Enter globally configuration	**system-view**	
Configure multicast TTL	**sntp client multicast ttl** *ttl*	255 by default

30.2.7 Configure Interval Polling

Configure interval polling is necessary when SNTP client works in the uticast or any cast way.SNTP client adjusts the local system time by each interval polling requesting to sever.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *device/slot/port*	
Configure interval polling	**sntp client poll-interval** *time*	1000s by default

30.2.8 Configure Overtime Retransmist

This Command is effective in unicast and any cast operating mode. SNTP request packet is UDP packet, overtime retransmission system is adopted because the requirement packet cannot be guaranteed to send to the destination. Use above Commands to configure retransmit times

and the interval.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
configure overtime retransmit	**Sntp client retransmit-interval** *time*	5s by default,
configure overtime retransmit times	**sntp client retransmit** *times*	By default 0, means do not retransmit

30.2.9 Configure Valid Servers

In broadcast and multicast mode, SNTP client receives protocol packets from all servers without distinction. When there is malice attacking server (it will not provide correct time), local time cannot be the standard time. To solve this problem, a series of valid servers can be listed to filtrate source address of the packet.

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
configure valid servers	**sntp client valid-server** *IP mask*	

30.2.10 Configure MD5 Authentication

To enhance the safety, MD5 authentication can be setup between SNTP sever and SNTP client which only receives the authenticated message. MD5 authentication configures as below:

Operation	Command	Remarks
Enter globally configuration mode	**system-view**	
Startup MD5 authentication	**sntp client authenticate**	

Configure authentication keys	**sntp client authentication-key** *key-number* **md5** *value*	

30.2.11 Display and Maintain SNTP Client

After finishing above configuration, you can use below Commands to display SNTP client configuration.

Operation	Command	Remarks
Display and maintain SNTP client	**display sntp client**	

Chapter 31 802.1X

31.1 802.1X Overview

IEEE 802.1X is the accessing management protocol standard based on interface accessing control passed in June, 2001. Traditional LAN does not provide accessing authentication. Users access the devices and resources in LAN when connecting to the LAN, which is a security hidden trouble. For application of motional office and CPN, device provider hopes to control and configure user's connecting. There is also the need for accounting.

IEEE 802.1X is a network accessing control technology based on interface which is the accessing devices authentication and control by physical accessing level of LAN devices. Physical accessing level here means the interface of LAN Switch devices. When getting authentication, Switch is the in-between (agency) of client and authentication server. It obtains user's identity from client of accessing Switch and verifies the information through authentication server. If the authentication passes, this user is allowed to access LAN resources or it will be refused.

31.1.1 Architecture of 802.1X

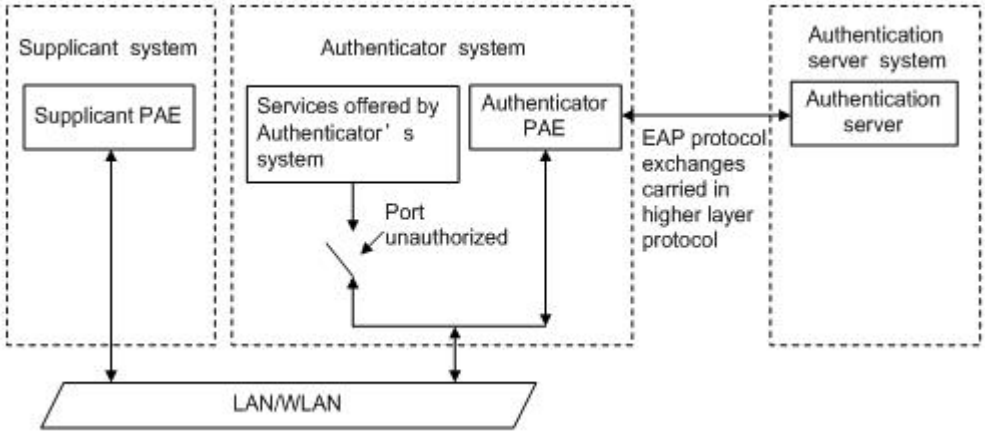
802.1X operates in the typical client/server model and defines three entities: supplicant system, authenticator system, and authentication server system.

Supplicant system: A system at one end of the LAN segment, which is authenticated by the

authenticator system at the other end. A supplicant system is usually a user-end device and initiates 802.1x authentication through 802.1x client software supporting the EAP over LANs (EAPOL) protocol.

Authenticator system: A system at the other end of the LAN segment, which authenticates the connected supplicant system. An authenticator system is usually an 802.1x-enabled network device and provides ports (physical or logical) for supplicants to access the LAN.

Authentication server system: The system providing authentication, authorization, and accounting services for the authenticator system. The authentication server, usually a Remote Authentication Dial-in User Service (RADIUS) server, maintains user information like username, password, VLAN that the user belongs to, committed access rate (CAR) parameters, priority, and ACLs.



The above systems involve three basic concepts: PAE, controlled port, control direction.

1) PAE

Port access entity (PAE) refers to the entity that performs the 802.1x algorithm and protocol

operations.

The authenticator PAE uses the authentication server to authenticate a supplicant trying to access the LAN and controls the status of the controlled port according to the authentication result, putting the controlled port in the authorized or unauthorized state. In authorized state, the port allows user data to pass, enabling the supplicant(s) to access the network resources; while in unauthorized state, the port denies all data of the supplicant(s).

The supplicant PAE responds to the authentication request of the authenticator PAE and provides authentication information. The supplicant PAE can also send authentication requests and logoff requests to the authenticator.

2) Controlled port and uncontrolled port

An authenticator provides ports for supplicants to access the LAN. Each of the ports can be regarded as two logical ports: a controlled port and an uncontrolled port.

The uncontrolled port is always open in both the inbound and outbound directions to allow EAPOL protocol frames to pass, guaranteeing that the supplicant can always send and receive authentication frames.

The controlled port is open to allow normal traffic to pass only when it is in the authorized state.

The controlled port and uncontrolled port are two parts of the same port. Any frames arriving at the port are visible to both of them.

3) Control direction

In the unauthorized state, the controlled port can be set to deny traffic to and from the supplicant or just the traffic from the supplicant.

31.1.2 Rule of 802.1x

The 802.1x authentication system employs the Extensible Authentication Protocol (EAP) to exchange authentication information between the supplicant PAE, authenticator PAE, and authentication server.

At present, the EAP relay mode supports four authentication methods: EAP-MD5, EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security), and PEAP (Protected Extensible Authentication Protocol).

1) When a user launches the 802.1x client software and enters the registered username and password, the 802.1x client software generates an EAPOL-Start frame and sends it to the authenticator to initiate an authentication process.

2) Upon receiving the EAPOL-Start frame, the authenticator responds with an EAP-Request/Identity packet for the username of the supplicant.

3) When the supplicant receives the EAP-Request/Identity packet, it encapsulates the username in an EAP-Response/Identity packet and sends the packet to the authenticator.

4) Upon receiving the EAP-Response/Identity packet, the authenticator relays the packet in a RADIUS Access-Request packet to the authentication server.

5) When receiving the RADIUS Access-Request packet, the RADIUS server compares the identify information against its user information table to obtain the corresponding password information. Then, it encrypts the password information using a randomly generated challenge, and sends the challenge information through a RADIUS Access-Challenge packet to the authenticator.

6) After receiving the RADIUS Access-Challenge packet, the authenticator relays the contained EAP-Request/MD5 Challenge packet to the supplicant.

7) When receiving the EAP-Request/MD5 Challenge packet, the supplicant uses the offered challenge to encrypt the password part (this process is not reversible), creates an EAP-Response/MD5 Challenge packet, and then sends the packet to the authenticator.

8) After receiving the EAP-Response/MD5 Challenge packet, the authenticator relays the packet in a RADIUS Access-Request packet to the authentication server.

9) When receiving the RADIUS Access-Request packet, the RADIUS server compares the password information encapsulated in the packet with that generated by itself. If the two are identical, the authentication server considers the user valid and sends to the authenticator a RADIUS Access-Accept packet.

10) Upon receiving the RADIUS Access-Accept packet, the authenticator opens the port to grant the access request of the supplicant. After the supplicant gets online, the authenticator periodically sends handshake requests to the supplicant to check whether the supplicant is still online. By default, if two consecutive handshake attempts end up with failure, the authenticator concludes that the supplicant has gone offline and performs the necessary operations, guaranteeing that the authenticator always knows when a supplicant goes offline.

11) The supplicant can also send an EAPOL-Logoff frame to the authenticator to go offline unsolicitedly. In this case, the authenticator changes the status of the port from authorized to unauthorized and sends an EAP-Failure frame to the supplicant.

31.2 Configure AAA

Finish necessary configuration of domain and RDIUS project of 802.1X authentication.

31.2.1 Configure RADIUS Server

RADIUS server saves valid user's identity. When authentication, system transfers user's identity to RADIUS server and transfer the validation to user .User accessing to system can access LAN resources after authentication of RADIUS server.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter AAA mode	**aaa**	
Enter RAIDUS configuration	**radius host** *radius-name*	
Configure primary auth RADIUS	**primary-auth-ip** *ip-address port*	
Configure primary acct RADIUS	**primary-acct-ip** *ip-address port*	
Configure second auth RADIUS	**second-auth-ip** *ip-address port*	
Configure second acct RADIUS	**second-acct-ip** *ip-address port*	
Configure key string of RADIUS	**auth-secret-key** *keystring*	
Configure key string of RADIUS	**acct -secret-key** *keystring*	
Configure NAS-RAIDUS address	**nas-ipaddress** *ip-address*	
Setup the username format	**username-format** { with-domain | without-domain }	
Configure accounting	**realtime-account**	
Configure the times of accouting	**realtime-account interval** *account-times*	

31.2.2 Configure Local User

Client need configure local user name and password.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter AAA mode	**aaa**	
Configure local user	**local-user username** *name* **password** *pwd* [**vlan** *vlan-id*]	

31.2.3 Configure Domain

Client need provide username and password when authentication. Username contains user's ISP information, domain and ISP corresponded. The main information of domain is the RADIUS server authentication and accounting the user should be.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter AAA mode	**aaa**	
Configure default Domain	**default domain-name** { disable | enable }	
setup Domain	**domain** *domain-name*	
Configure default Domain scheme	**scheme** { local | radius [local] }	
choice RADIUS name	**radius host binding** *radius-name*	
configure access limit users	**access-limit** { enable *number* | disable }	
active the state	**state** { active | block }	

31.2.4 Configure RADIUS Features

Configure RADIUS some compatible or special features as below:

Operation	Command	Remarks

Enter global configuration mode	**system-view**	
Enter AAA mode	**aaa**	
Enable user re-authentication, when it executives	**accounting-on** { enable *account-num* | disable }	
H3C Cams compatible under this feature can uprate-value / dnrate-value to configure the upstream bandwidth / downstream bandwidth of the Vendor Specific attribute name of the attribute number.	**h3c-cams** { enable | disable }	
Accounting function	**radius accounting**	
Accounting packets without response need cut off users	**radius server-disconnect drop 1x**	
Enable port priority	**radius 8021p enable**	This feature is turned on, if the user authentication passes, it will be modified by the user where the priority of the port.
Enable port PVID	**radius vlan enable**	This feature is turned on, if the user authentication

		passes , it will be modified by the user where port PVID is
Enable limit port of MAC address numbers	**radius mac-address-number enable**	This feature is turned on, if the user authentication passes, the user will modify the port about the limiting number of MAC address learning.
Enable limit port bandwidth	**radius bandwidth-limit enable**	By default unit is kbps, can be modified through radius config-attribute access-bandwidth unit.

31.3 Configure 802.1X

31.3.1 Configure EAP

The 802.1X authentication can be initiated by either a supplicant or the authenticator system. A supplicant can initiate authentication by launching the 802.1x client software to send an EAPOL-Start frame to the authenticator system, while an authenticator system can initiate authentication by unsolicitedly sending an EAP-Request/Identity packet to an unauthenticated

supplicant.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
set the protocol type between system and RADIUS	**dot1x** { eap-finish | eap-transfer }	

31.3.2 Enable 802.1x

802.1x provides a user identity authentication scheme. However, 802.1x cannot implement the authentication scheme solely by itself. RADIUS or local authentication must be configured to work with 802.1x

Enabling 802.1S authentication, users connected to the system can access to LAN per passing the authentication.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable 802.1x	**dot1x method** { macbased | portbased }	

31.3.3 Configure 802.1x Parameters for a Port

The 802.1x proxy detection function depends on the online user handshake function. Be sure to enable handshake before enabling proxy detection and to disable proxy detection before disabling handshake.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure 802.1x parameters for a	**dot1x port-control** { auto | forceauthorized |	

port	forceunauthorized } [interface ethernet *interface-list*]	

31.3.4 Configure Re-Authentication

In EAP-FINISH way, the port supports re-authentication. After the user is authenticated, the port can be configured to immediately re-certification, or periodic re-certification.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Immediately re-certification	**dot1x re-authenticate** [interface ethernet *interface-list*]	
Periodic re-authentication enabled on a port	**dot1x *re-authentication*** [interface ethernet *interface-list*]	
Periodic re-authentication time configuration port	**dot1x timeout re-authperiod** *time* [interface ethernet *interface-list*]	

31.3.5 Configure Watch Feature

Opening function, the port without the user's circumstances, will watch regularly sends a 1x packet, triggering the following 802.1x user authentication.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Open the watch function	**dot1x daemon** [interface ethernet *interface-list*]	
Configuration time between sending	**dot1x daemontime** [interface ethernet	

packets Watch	*interface-list*]	

31.3.6 Configure User Features

The operations mainly conclude of the number of users for port configuration, user and delete users, and heartbeat detection operations.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configuration allows the maximum number of users through the authentication	**dot1x max-user** *user-num* [interface ethernet *interface-list*]	
Deletes the specified users online	**dot1x user cut** { **username** *name* | **mac-address** *mac-address* }	
Open heartbeat detection	**dot1x detect** [interface ethernet *interface-list*]	
Heartbeat detection time configuration	**dot1x detect interval** *time*	

Chapter 32 LLDP

32.1 LLDP Overview

LLDP (Link Layer Discovery Protocol), a L2 protocol, defined by IEEE802.1AB-2005 standard has nothing to do with the manufacturer. It announces its information to other neighbor devices in the network, receives the neighbor's information and saves to standard MIB of LLDP for users to check the downlink devices and connected ports for easy network maintenance and management. Network administrator can know L2 connections by accessing.

32.1.1 LLDP Fundamentals

LLDP devices announce their own information through multicast address 01-80-c2-00-00-0e. LLDP devices will send 2 LLDP notice and the sending interval is set by hello-time. After receiving neighbor's advertisement, LLDP device will read the advertisement content and save in LLDP neighbor table. LLDP neighbor table can be aged with TTL value being aging time. If neighbor's LLDP advertisement cannot be received within aging time, the neighbor entry will be removed.

32.1.2 LLDP Timer

Hello-time: The time interval for sending LLDP packet.

Hold-time: LLDP aging time granularity for neighbor entry.

TTL: TTL equals to hello-time ties hold-time which means aging time of neighbor entry.

32.2 Configure LLDP

32.2.1 LLDP Configuration List

Configuration Task	Description	Detailed Configuration
Enable LLDP	Required	32.2.2
Configure LLDP Hello-time	Optional	32.2.3
Configure LLDP Hold-time	Optional	32.2.4
Configure LLDP packet sending & receiving mode	Optional	32.2.5
Configure LLDP managementaddress	Optional	32.2.6
LLDP display and debugging	Optional	32.2.7

32.2.2 Enable LLDP

Only after enabling global LLDP, all related configurations can be effective. Global and port LLDP can be configured and saved no matter the LLDP is enabled. When global LLDP is enabled, the configuration is effective.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable LLDP	**lldp**	
Disable LLDP	**undo lldp**	Disabled by default
Enter port configuration mode	**interface ethernet** *interface-num*	
Disable interface LLDP	**undo lldp**	Enabled by default

32.2.3 ConfigureLLDP Hello-Time

By default, LLDP Hello-time is 30S.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	-
Configure LLDP Hello-time	**lldp hello-time** *time*	hello-time: <5-32768>(seconds)
Configure default LLDP Hello-time	**undo lldp hello-time**	

32.2.4 ConfigureLLDP Hold-Time

By default, LLDP Hold-time is 4S.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure LLDP Hello-time	**lldp hold-time** *time*	hold-time: <2-10>(seconds)
Configure default LLDP Hello-time	**undo lldp hold-time**	

32.2.5 ConfigureLLDP Packet Transferring and Receiving Mode on Port

There are three types of mode:

Rx: receiving only.

Tx: transferring only.

Rxtx: transferring and receiving.

By default, the mode for all ports is rxtx, that is, transferring and receiving all LLDP packets.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	

Configure LLDP packet transferring and receiving mode on port	**lldp** { **rx** | **rxtx** | **tx** }	

32.2.6 Configure LLDP Management Address

Management address is the IP address of the device.LLDP devices use the vlan-interface IP address to encapsulate the LLDP packet and send the packet to the neighbor.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode	**interface ethernet** *interface-num*	
Configuremanagementaddress	**lldp management-address** { vlan-interface | supervlan-interface } *vlan-id*	
Delete managementaddress	**undo lldp management-address**	

32.2.7 LLDP Display and Debugging

After the above configurations, you can execute the display commands in any configuration mode to display information, so as to verify your configurations.

Operation	Command	Remarks
Display LLDP status	**display lldp** [interface ethernet *interface-num*]	

Chapter 33 PPPoE Plus

33.1 PPPoE Plus Overview

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and in plain Metro Ethernet networks. It was developed by UUNET, Redback Networks and RouterWare and is available as an informational RFC 2516.

33.2 ConfigurePPPoE Plus

33.2.1 PPPoE PlusConfiguration List

Configuration Task	Description	Detailed Configuration
Enable PPPoE Plus	Required	33.2.2
Configure Option Content	Optional	33.2.3
PPPoE Plus Monitor and Maintenance	Optional	33.2.4

33.2.2 Enable PPPoE Plus

PPPoE packet will be forwarded to trust port. Trust port should be configured after enable this function. Generally, PPPoE plus will add option content to PPPoE packet. If the received PPPoE packet has contained option content, the handling strategy will be defined.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable PPPoE Plus	**pppoeplus**	
Disable PPPoE Plus	**undo pppoeplus**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Configure PPPoE trust port	**pppoeplus trust**	
Delete PPPoE trust port	**undo pppoeplus trust**	
Configure option strategy	**pppoeplus strategy** { drop | keep | replace | transmit }	
Configure PPPoE drop PADO/PADI	**pppoeplus drop** { padi | pado }	
Delete PPPoE drop PADO/PADI	**undo pppoeplus drop** { padi | pado }	

33.2.3 ConfigureOption Content

The option content need to be added before PPPoE packet forwarding out, the contents of this option can be determined by a variety of ways. Option content can be specified in interface configuration mode. If the content is not specified, it will be constructed according to configured rules. If pppoe plus type is self-defined, the format should also be specified.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure PPPoE Plus type	**pppoeplus type** { **huawei** | **standard** | **self-defined** { **ciruit-id** { *string* | vlan | port | Switch-mac | hostname | client-mac } * | **remote-id** { *string* | Switch-mac | hostname | client-mac } * }	
Configure default PPPoE Plus type	**undo pppoeplus type**	By default, type

		is standard
Configure format	**pppoeplus format** { binary | ascii }	Optional
Configure default format	**undo pppoeplus format**	By default, it is binary
Configure delimiter	**pppoeplus delimiter** { colon | dot | slash | space }	
Configure default delimiter	**undo pppoeplus delimiter**	By default, it is space
Enter interface configuration mode	**interface ethernet** *interface-num*	
Specify circuit ID	**pppoeplus circuit-id** *string*	
Delete PPPoE cid	**undo pppoeplus circuit-id**	

33.2.4 PPPoE Plus Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Operation	Command	Remarks
Display PPPoE Plus configuration	**display pppoeplus interface** [ethernet *interface-list*]	

Chapter 34 CFM

34.1 CFM Overview

CFM (Connectivity Fault Management, the connectivity fault management protocol), defined by the IEEE 802.1ag standard is a Layer 2 link on the VLAN-based end to end OAM mechanism used to Carrier Ethernet fault management.

34.1.1 CFM Concepts

Concept	Remark
MD	Maintenancefieldindicates that even the fault detectionis covered through a network of its boundary is configured onaportrangedefined by the MEPs. Maintenance ofthe domain of "Maintain the domain name"to identify, according to network planning can be divided into eight levels. Between different domains can bemaintained adjacent toor nested, but can't cross,and the nesteddomain can only bemaintainedby the high-level domain to the lowlevel maintenancenested, that is, low-levelmaintenance ofthe domain mustbeincluded in the domainof high-level maintenance department.
Maintenance set	Within the maintenancedomain can be configured as neededto maintain multiple sets, eachset ismaintained withinsomemaintenance to maintainthe set point. Maintenanceset to "maintainthedomain name +maintenanceset name"to identify.

	Maintainset service on aVLAN, to maintainfocus on themaintenancepoint of sending packets of thebandarethe VLAN tag, at thesametime Maintainfocus onthe maintenancepoint can receive byMaintainfocus on its maintenancepointsentthe message.
Maintenance point	Maintenance points configured on a port, part of a maintenance set, can be divided into MEPs and MIPs two. (1)MEP IDin orderto maintainendpoint identity, whichdefinesthe scope andmaintenance ofthe domain boundary.MEP has a directional, sub-UPMEP and DOWN MEP for the two.MEP direction that themaintenance ofdomain relative to the location oftheport. DOWN MEP isthe port whereto send its message, UP MEPport whereit is not sent to themessage, butit isthe port to the device send its message. (2)Maintenance in themaintenance ofthe domainbetweenpointswithin thedepartment, not the mainaction issued CFMprotocol packets, but can handle andrespond to CFM protocol packets.

34.1.2 CFM Main Function

Connectivity fault detection based on a reasonable and effective application deployment and configuration over the network, its function is maintained in the configuration between points, as long as the following functions:

Function	Remark
Continuity detection	It is a proactive OAM functionality is used to detect the state to maintain connectivity between endpoints. Connectivity failure may be caused by equipment failure or

	configuration error.
Loopback	It is akind ofon-demandOAM functions for thelocaldevice and remote authenticationbetween enddevices connected state.
Link tracking	It is akind ofon-demandOAM functions for thelocal device todeterminethe path between the remote devices, in order to achieve the positioning of link failure.

34.2 Configure CFM

CFM function in the configuration before the network should carry the following plan:

- For the maintenance of the entire network to carry out sub-domain level, determine the level of maintenance of the domain boundary.
- Determine the maintenance of the domain name, the same domain on a different device to maintain the same name.
- Required monitoring of VLAN, determine the set of maintenance within the maintenance domain.
- Determine the maintenance set name, the same maintenance domain within the same set on different devices to maintain the same name.
- That the same maintenance domain within the same set of maintenance to maintain a list of endpoints in the different devices should remain the same.
- In the maintenance field and set the boundaries of the maintenance port on the endpoint should be planned maintenance, non-border or port equipment maintenance can be planned on a mid-point.
- After the completion of network planning, come line the following configuration.

34.2.1 CFM Configuration List

Configuration Task	Description	Detailed Configuration
Maintain Field Configuration	Required	34.2.2
Configuration and maintenance level domain name	Required	34.2.3
Configure to maintain set	Required	34.2.4
Configure name and the associated VLAN to maintain set	Required	34.2.5
Configure MEPs	Required	34.2.6
Configure Remote Maintenance endpoint	Required	34.2.7
Configure MIPs	Optional	34.2.8
Configure continuity detection	Required	34.2.9
Configure loopback	Optional	34.2.10
Configure link tracking	Optional	34.2.11
Display and maintenance of the CFM	Optional	34.2.12

34.2.2 Maintain Field Configuration

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Create a maintenance domain, and domain configuration into maintenance mode	**cfm md** *md-index*	

34.2.3 Configuration and Maintenance Level Domain Name

In order to distinguish between the various maintenance domain, you can specify a different domain for each maintenance of domain names, the name by the name of the format and content of two parts, the whole network a unique domain name is best; to display nested relationship between the maintenance domain, must also designated to maintain the domain level, only the level of maintenance of large domain nested level can only be a small maintenance domain.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Domain configuration into maintenance mode	**cfm md** *md-index*	
Configuration without the maintenance of domain names, only the specified field level maintenance	**cfm md format** none **level** *md-level*	
Equipped with the maintenance of the domain name, and specify the domain name and level of maintenance	**cfm md format** { **dns-name** | mac-uint | string } name*md-name* **level** *md-level*	

34.2.4 Configure Maintain Set

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
To maintainthe domainconfiguration	**cfm md** *md-index*	

mode to enter		
Created to maintain set, and enter the configuration mode set to maintain	**cfm ma ma-index**	

34.2.5 Configure Name and Associated VLAN to Maintain Set

In order to maintain the distinction between the various domains to maintain set, you can specify a different set for each to maintain the instance name, instance name, the name by the name of the format and content of two parts, the maintenance of set where the maintenance of the domain name plus the instance name must ensure that all network only.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
To maintainthe domainconfiguration mode to enter	**cfm md** *md-index*	
Enter the configuration mode set to maintain	**cfm ma ma-index**	
The name of the configuration set and maintain the VLAN associated with the main	**cfm ma format** { primary-vid | string | uint16 | vpn-id } **name** *ma-name* **primary-vlan** *vlan-id*	

34.2.6 Configure MEPs

CFM is mainly reflected in the maintenance of a variety of endpoints operating on, the user can program the network port on the network configuration to maintain the boundary endpoints.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
To maintainthe domainconfiguration mode to enter	**cfm md** *md-index*	
Enter the configuration mode set to maintain	**cfm ma ma-index**	
Create a maintenance endpoint, and specify its associated port	**cfm mep** *mep-id* **direction** { up | down } [***primary-vlan vlan-id***] **interface ethernet** *port-id*	
Enable the state to maintain endpoint management	**cfm mep** *mep-id* **state** { enable | disable }	Required Default is off
CCMand configure the endpoint to send maintenance to use the priorityLTM	**cfm mep** *mep-id* **priority** *priority-id*	Optional Default priority is 0

34.2.7 Configure Remote Maintenance Endpoint

Remote maintenance end point is equivalent to the local maintenance of the end points, and in the maintenance of concentration, in addition to the maintenance of the local endpoint, all other maintenance endpoints should be configured in the local endpoint for the remote maintenance.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

To maintainthe domainconfiguration mode to enter	**cfm md** *md-index*	
Enter the configuration mode set to maintain	**cfm ma ma-index**	
Creating remote maintenance end point, and specify the end of its peer MEPs	**cfm rmep** *rmep-id* **mep** *mep-id*	

34.2.8 Configure MIPs

MIPs used to test the response of CFM message, the user can program the network device or in non-border ports configured to maintain the mid-point.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
To maintainthe domainconfiguration mode to enter	**cfm md** *md-index*	
Enter the configuration mode set to maintain	**cfm ma ma-index**	
Create a maintenance intermediate point, and specify its associated port	**cfm mip** *mip-id* **interface ethernet** *port-id*	

34.2.9 Configure Continuity Detection

Continuity detection through configuration, can be made to maintain interoperability between endpoint CCM packets to check the connectivity between these endpoints maintain

state in order to achieve the link connectivity management.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
To maintainthe domainconfiguration mode to enter	**cfm md** *md-index*	
Enter the configuration mode set to maintain	**cfm ma ma-index**	
Configuration maintenance interval endpoint to send theCCM	**cfm cc interval** {1 | 10 | 60 | 600 }	1s by default
Enable sending MEPccm	**cfm mep** *mep-id* **cc** { enable | disable }	Default is off

Caution:

Different devices at the same maintenance domain and maintain a centralized maintenance endpoint, the sending time interval of CCM must be the same.

34.2.10 Configure Loopback

By Configure the loopback function, you can check the source to the target MEPs MEPs or MIPs link between the situations in order to achieve the link connectivity verification.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
To maintainthe domainconfiguration mode to enter	**cfm md** *md-index*	
Enter the configuration mode set to	**cfm ma ma-index**	

maintain		
Start loopback	**cfm loopback mep*mep-id*** { ***dst-mac mac-address*** | ***dst-mep rmep-id*** } [**priority** *pri-id* | **count** *pkt-num* | **length** *data-len* | *datapkt-data*]	

34.2.11 ConfigureLink Tracking

By Configure the link tracking, you can find the source to the target MEPs MEPs or maintenance intermediate point between the path in order to achieve the positioning of link failure.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
To maintainthe domainconfiguration mode to enter	**cfm md** *md-index*	
Enter the configuration mode set to maintain	**cfm ma ma-index**	
Start Tracking link	**cfm linktrace mep*mep-id*** { *dst-mac mac-address* | *dst-mep rmep-id }* [**timeout** *pkt-time* | **ttl** *pkt-ttl* | **flag** { *use-mpdb* | *unuse-mpdb* }]	

34.2.12 Display and Maintenance of CFM

After completing the above configuration, you can use the following command to display the

CFM configuration.

Operation	Command	Remarks
The Maintenance domain information	**display cfm md** [*md-index*]	
The Maintenance Set Information	**display cfm ma**	
Display the end point of maintenance information	**display cfm mp local**	
Remote maintenance point information display	**display cfm mp remote**	
Display CCM statistics	**display cfm cc**	
Clear CCM statistics	**clear cfm cc**	
CCM database information display	**display cfm cc database**	
Clear CCM database information	**clear cfm cc database**	
CFM alarm information display	**display cfm errors**	

Chapter 35 EFM

35.1 EFM Overview

EFM (Ethernet of First Mile) as the first mile Ethernet, defined by the IEEE 802.3ah standard, used for the two devices point to point Ethernet link between the management and maintenance.

35.1.1 EFM Main Function

EFM Ethernet can effectively improve the management and maintenance capabilities to ensure the stable operation of the network, its main features include:

Function	Remarks
EFM auto-discovery	EFM functionality built on the basis of connections, EFM connection establishment process is achieved by the auto-discovery of EFM. EFM work in two modes: active mode and passive mode, EFM connected only by the active mode of EFM entity initiated the passive mode EFM physical entity can only wait for the end of the connection requests are in a passive mode of the two an EFM can’t be established between the entities connected.
Remote failure indication	When the device detects a link event of an emergency, the fault will end EFM entity's Flag by Information OAMPDU fault information field (the type of emergency event link) EFM notification to the peer entity. In this way, administrators can log information by observing the dynamic understanding of the link state, the

	corresponding error in a timely manner for processing. Event types, including emergency Link Fault, Dying Gasp and Critical Event of three.
Link monitoring capabilities	Link monitoring function is used in a variety of environments and found that the link layer fault detection, EFM through interactive Event Notification OAMPDU to monitor the link: When the end of the EFM to detect the general physical link event, the Event Notification sent to its peer OAMPDU for notification, the administrator can log information by observing the network to dynamically control the situation. Event types include general link-errored-symbol-period, errored-frame, errored-frame-period, errored-frame-seconds four.
Remote loopback	Remote loopback is active mode EFM entity sends to the remote except OAMPDU than all other messages, the remote receives the packet forwarding address is not its purpose, but the road back to its original The end. Remote loopback is controlled by remote Loopback Control OAMPDU remote loopback or remote loopback operation to cancel the function can be used to detect the link quality and positioning of link failure.
Remote access to MIB variable function	EFM entities can interact with Variable Request / Response OAMPDU far end of the entity to obtain the MIB variable value.Include Ethernet MIB variable chain on the road all the performance parameters and error statistics. It provides a local EFM physical entity on the far side of the general performance and error detection mechanisms.

Description:

We said so to the EFM port functions as "EFM Entities".

35.1.2 EFM Protocol Packets

EFM working in the data link layer, the protocol packet is called OAMPDU (OAM Protocol Data Units, OAM protocol data unit).EFM is through regular interaction between the device OAMPDU to report link status, enabling network administrators to effectively manage the network.

Message type	Effect
Information OAMPDU	EFM entity status for the information (including local information, the remote information and custom information) sent to the remote entity EFM, EFM connections to maintain.
Event Notification OAMPDU	Generally used for link monitoring on local and remote connected EFM physical link failures in the warning.
Loopback Control OAMPDU	Mainly use for remote loopback control in order to control the EFM loopback state of remote device. The packet has the information of enabling or disabling loopback .Enabling or disabling remote loopback based on this information.
Variable Request / Response OAMPDU	Mainly used for remoteMIBvariable values, in order to achieve the end of the remote state prosecution.

35.2 Configure EFM

35.2.1 EFM Configuration List

Configuration Task	Description	Detailed Configuration
EFM Basic Configuration	Required	35.2.2
Configure EFM Timer Parameter	Optional	35.2.3
Configure Remote Failure Indication	Optional	35.2.4
Configure Link Monitoring Capabilities	Optional	35.2.5
Enabling Remote Loopback	Optional	35.2.6
Rejecting Remote Loopback Requests Initiated by Remote	Optional	35.2.7
Initiating a Remote Loopback Request	Optional	35.2.8
Starting Remote Access Function MIB Variable	Optional	35.2.9
MIB Variable Access Requests Initiated by Remote	Optional	35.2.10
Display and Maintenance of EFM	Optional	35.2.11

35.2.2 EFM Basic Configuration

EFM mode of operation is divided into proactive mode and passive mode, when the EFM function enabled, the Ethernet port started to use the default mode of operation and the establishment of its peer port connected EFM.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode.	**interface ethernet** *interface-num*	-
StartEFM	**efm**	By default, EFM is off

EFMmode configuration	**efm mode** { passive | active }	By default, EFM mode to active mode

35.2.3 Configure EFM Timer Parameter

EFM connection is established, both ends of the EFM entity will be a certain time interval to send Information OAMPDU cycle to detect whether the connection is normal, the interval is called the interval to send handshake packets. If one end of the connection timeout EFM entity within an entity does not receive remote EFM sent Information OAMPDU, EFM is considered disconnected.

EFM handshake by adjusting packet transmission interval and the connection timeout, the connection can change the EFM detection accuracy. With Configure OAMPDU remote request message to the response timeout, then discard the message which receiving the later response message to the OAMPDU if the time is out.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode.	**interface ethernet** *interface-num*	
Configurethe interval to send handshake packetsEFM	**efm pdu-timeout** *time*	1s by default
Configure the connection timeoutEFM	**efm link-timeout** *time*	5s by default

Response timeout configuration	**efm remote-response-timeout** *time*	2s by default

Caution:

Because EFM connection times out, the local entity will EFM EFM aging and physical connection to the end of the relationship, the EFM connection is broken, so the connection must be greater than the timeout interval to send handshake packets (Recommended for 3 times or more) , otherwise it will lead to EFM connection instability.

35.2.4 Configure Remote Failure Indication

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode.	**interface ethernet** *interface-num*	
Startremote failure indication	**efm remote-failure** { link-fault | dying-gasp | critical-event }	By default,remote failure indication is enabled

Description:

Remote failure indication function device supports a single-pass function required to detect the local emergency link to the remote event notification, in the single-pass functions are not supported on the device, the local emergency is detected only in the event link end of reporting alarms and can’t notify the remote.

35.2.5 Configure Link Monitoring Capabilities

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode.	**interface ethernet** *interface-num*	
Startlink monitoring capabilities	**efm link-monitor** { errored-symbol-period | errored-frame | errored-frame-period | errored-frame-seconds }	By default, the link monitoring is enabled
Configureerrored-symbol-periodevent detection cycle	**efm link-monitor errored-symbol-period window high** *win-value1* **low** *win-value2*	
Configureerrored-symbol-periodevent detection threshold	**efm link-monitor errored-symbol-period threshold high** *th-value1* **low** *th-value2*	
Configureerrored-frameevent detection cycle	**efm link-monitor errored-frame window** *win-value*	
Configureerrored-frameevent detection threshold	**efm link-monitor errored-frame threshold** *th-value*	
Configureerrored-frame-periodevent detection cycle	**efm link-monitor errored-frame-period window** *win-value*	
Configureerrored-frame-periodevent detection threshold	**efm link-monitor errored-frame-period threshold** *th-value*	
Configureerrored-frame-secondsevent detection cycle	**efm link-monitor errored-frame-seconds window** *win-value*	
Configureerrored-frame-secondsevent detection threshold	**efm link-monitor errored-frame-seconds threshold** *th-value*	

Description:

- errored-symbol-period threshold event detection cycle and a 64-bit integer value, **high** and **low** parameter values, respectively, after the value of the high and low 32-bit, that is, the integer value = **(high * (2 ^ 32))** + **low.**

35.2.6 Enabling Remote Loopback

By default, loopback at the far end is in the off state. It can only support the far end loopback device starts far end loopback.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode.	**interface ethernet** *interface-num*	
Start remote loopback	**efm remote-loopback**	

35.2.7 Rejecting Remote Loopback Requests Initiated by Remote

As the remote loopback function will be affected normal business in order to avoid this situation, users can configure the local port of the peer sent from the Loopback Control OAMPDU control, which refused to end the remote initiated EFM loopback request.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode.	**interface ethernet** *interface-num*	
Reject remote loopback requests initiated by remote	**efm remote-loopback** { ignore | process }	By default, the remote refused

		to initiate a remote loopback request

35.2.8 Initiating a Remote Loopback Request

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode.	**interface ethernet** *interface-num*	
Initiate a remote loopback request	**efm remote-loopback** { start | stop }	

Description:

- Only when the port EFM connection has been created, and the mode of EFM proactive mode, in order to launch on the far side of the port loopback request.
- Only the port side and far side far side loopback support feature, and in full-duplex chain on the road to achieve the far end loopback.
- In the open far end loopback, it will cause all data traffic in off; when the exit far end loopback, the local and remote port will be back to normal. Lead to far-side exit port loopback reasons: use undo EFM command to close the EFM function, use the EFM remote-loopback stop command or exit the far end loopback connected EFM over time and so on.

35.2.9 Starting Remote Access Function MIB Variable

Operation	Command	Remarks

Enter global configuration mode	**system-view**	
Enter port configuration mode.	**interface ethernet** *interface-num*	
Startthe remote access functionMIBvariable	**efm variable-retrieval**	By default, remote access to MIB variable is enabled

35.2.10 MIB Variable Access Requests Initiated by Remote

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter port configuration mode.	**interface ethernet** *interface-num*	
Port for the remote deviceMIBvariable value	**display efm port** *port-id-list* **remote-mib** { phyadminstate | autonegadminstate }	
Access to remote devices globalMIBvariable values	**display efm remote-mib** { fecability | fecmode }	

Description:

- Only when the port EFM connection has been created, EFM working model is for the proactive mode, the far side far side port supports MIB variable access function to the port on the far end of the MIB variable for initiating the request.
- Currently only supports remote query capability of FEC, FEC mode, port status and port to enable auto-negotiation enabled, the other MIB variables can later be added on demand to achieve.

35.2.11 Display and Maintenance of EFM

After completing the above configuration, you can use the following command to display the EFM configuration.

Operation	Command	Remarks
Display EFMprotocol running	**display efm status interface** [ethernet *interface-num*]	
Display summary informationEFM	**display efm summary**	
Display EFMfind information	**display efm discovery interface** [ethernet *interface-num*]	
Display EFMprotocol packet statistics	**display efm statistics interface** [ethernet *interface-num*]	
ClearEFMprotocol packet statistics	**clear efm statistics interface** [ethernet *interface-num*]	

Chapter 36 ERRP

36.1 ERRP Overview

Ethernet Redundant Ring Protocol is a link layer protocol specifically designed for Ethernet ring. It prevents broadcast storms caused by data loops when the Ethernet ring is complete; when a link on the Ethernet ring is disconnected, the communication path between the nodes on the ring network can be quickly restored. Compared with STP, ERRP has the characteristics of fast topological convergence speed and convergence time independent of the number of nodes on the ring network.

In order to avoid conflict between ERRP and STP in calculating port congestion / release status, ERRP and STP are mutually exclusive on the enabled port. That is, the STP protocol cannot be enabled by the two ports connected to the ERRP ring, and STP can be enabled by the other ports.

36.1.1 Concept Introduction

ERRP region

The ERRP region is identified by an integer ID. A set of Switch groups configured with the same domain ID, control VLAN and connected to each other form an ERRP domain. An ERRP domain has the following constituent elements:

- ERRP loop
- VLAN controlled by ERRP
- Master node
- Transport node
- Edge node and assistant edge node

ERRP loop

The ERRP ring is also identified by an integer ID, and an ERRP ring physically corresponds to a ring-connected Ethernet topology. An ERRP domain consists of an ERRP ring or multiple ERRP rings that are connected to each other. One of them is the master ring and the other ring is a sub-ring. The master ring and the sub-ring are distinguished by the specified level at the time of configuration. The level of the primary ring is 0 and the level of the sub-ring is 1.

The ERRP ring has two states:

Health state: All links of the ring are normal and the physical link of the ring is connected.

Fault state: The link on the ERRP ring is faulty. One or many physical links of the ring network are down.

Node role

The node on the ERRP ring is divided into the master node and the transit node. The node role is specified by the user. The master node is the decision-making and control node for ring

protection. Each ERRP ring must specify only one master node. All nodes except the master node are called transit nodes.

If more than one ERRP ring intersects, one of the intersecting nodes is designated as an edge node and the other intersecting node is designated as an assistant edge node. The role of the two nodes on the master ring is the transit node. The two nodes role of the sub-ring is the edge node and the assistant edge node. The specific role of the sub-ring can be specified by the user. There is no special requirement, mainly to distinguish the two nodes.

Port role

Each node of an ERRP ring has two ports connected to a ring. User can specify one of the ports as the primary port and the other port as the secondary port. The master port of the master node is used to send health detection message (hello message), received from the secondary port of the main node. The master port and secondary port of the transit node are functionally indistinguishable. To prevent the loop from causing broadcast storms, if the ERRP ring is normal, the secondary port of the master node is blocked and all the other ports are in the forwarding state.

If multiple ERRP rings intersect, the ports in the intersecting nodes that access both the primary ring and the sub-ring (that is, the port of the primary ring and the sub-ring common link) are called common ports at the same time. Only the ports that access the sub-rings are called edge ports. Conceptually, a public port is not considered to be a port of a sub-ring, it is regarded as part of the main ring, that is, the public link is the link of the primary ring, not the

link of the sub-ring. The state change of the public link is only reported to the master node of the primary ring. The master node of the sub-ring does not need to know.

Control VLAN

Control VLAN is relative to the data VLAN, the data VLAN is used to transmit data messages, control VLAN is used to transmit ERRP protocol messages.

Each ERRP region has two control VLANs, called the primary control VLAN and the sub-control VLAN. The protocol message of the primary ring is propagated in the master control VLAN, and the protocol message of the sub-ring is propagated in the sub-control VLAN. User need to specify the primary control VLAN. The VLAN that is one greater than the master control VLAN ID, is used as the sub-control VLAN.

Only port (ERRP port) connecting the Ethernet of each Switch belongs to the control VLAN, and the other ports cannot join the control VLAN. The ERRP port of the primary ring belongs to both the primary control VLAN and the sub-control VLAN. The ERRP port of the sub-ring belongs to the sub-control VLAN. The data VLAN can contain ERRP ports or non-ERRP ports. The primary ring is regarded as a logical node of the sub-ring. The protocol messages of the sub-ring are transmitted through the primary ring and processed in the primary ring as data messages. The protocol messages of the primary ring are transmitted only within the primary ring. Don’t enter sub-rings.

Query Solicit function

ERRP is used in conjunction with IGMP Snooping, if the topology of the ERRP changes, the forwarding state of the port will be changed. If the multicast state is not updated through the IGMP Snooping module after the port state changes, the multicast forwarding may become abnormal. To introduce the query solicit function. When a topology change occurs in the ERRP, the device sends a query solicit message or a general IGMP query message to all the ports so that the member port re-initiates an IGMP report to update the multicast entry.

36.1.2 Protocol Message

HELLO message

The hello message is initiated by the master node, and detects loop integrity of the network. The master node periodically sends HELLO message from its primary port, and the transit node forwards the message to the next node, which is then received by the secondary port of the master node. Periodically send, and the sending period is Hello timer.

LINK_UP message

The LINK_UP message is initiated by the transit node, edge node, or assistant edge node that recovers the link. It informs the master node that there is link recovery on the loop. Trigger to send.

LINK_DOWN message

The LINK_DOWN message is initiated by the transit node, edge node, or assistant edge node that fails the link. It informs the master node that there is link failure on the loop, and the physical loop disappears. Trigger to send.

COMMON_FLUSH_FDB message

It is initiated by the master node, and informs the transit node, the edge node and the assistant edge node to update their respective MAC address forwarding tables. Trigger on link failure or link recovery.

COMPLETE_FLUSH_FDB message

It is initiated by the master node, and informs the transit node, the edge node and the assistant edge node to update their respective MAC address forwarding tables, and informs the transit node to release the blocked state of the port temporarily blocking the data VLAN. It is sent when the link recovery (That is, the secondary port of the master node receives Hello packets) is complete.

EDGE_HELLO message

The EDGE_HELLO message is initiated by the edge node of the sub-ring to check the loop integrity of the major ring in the domain.

Edge nodes send EDGE_HELLO messages periodically from the two ports connected to the primary ring. The nodes in the primary ring process the message as data message and receive

them from the assistant edge nodes on the same sub-ring. Periodically send, sending cycle is the Edge Hello timer.

MAJOR_FAULT message

The MAJOR_FAULT message is originated by the assistant edge node and reports to the edge node that the primary ring of the domain is faulty. When the assistant edge node of the sun-ring cannot receive the EDGE_HELLO message from the edge node in the specified time, the assistant edge node sends a MAJOR_FAULT message from its edge port. After the sub-ring node receives the message, it forwards the message directly to the next node, and finally the edge node of same sub-ring receives. Periodically send after triggering, the sending period is Edge Hello timer.

36.1.3 Operate Principle

Health status

The master node periodically sends the hello message from its primary port, which in turn travels through the transit nodes of the ring. If the secondary port of the master node receives a hello message before it times out, it considers that the ERRP ring is health status. The status of the master node reflects the health of the ring. When the ring network is in a healthy state, the master node blocks its secondary port in order to prevent the data message from forming a broadcast loop.

Link failure

Two mechanisms are provided for detecting link failures:

(1) LINK_DOWN escalation and processing:

When an ERRP port of the transit node detects a port Link Down, the node sends a LINK_DOWN message to the master node from the ERRP PORT in the up state that is paired with the faulty port.

After the master node receives the LINK_DOWN message, the node state is immediately changed for failed state. Disable the blocking state of the secondary port. The FDB table is refreshed and a COMMON_FLUSH_FDB message is sent from the primary and secondary ports to notify all transit nodes to refresh their respective FDB tables.

After receiving the COMMON_FLUSH_FDB message, the transit node immediately refreshes the FDB table and starts learning the new topology.

(2) Polling mechanism:

The fault reporting mechanism is initiated by the transit node. In order to prevent the LINK_DOWN message from losing during transmission, the master node implements the Polling mechanism. The Polling mechanism is the mechanism that the master node of the ERRP ring actively detects the health status of the ring network. The master node periodically sends HELLO message from its master port, and then transmits it through the transmission nodes.

If the master node can receive the HELLO message from the secondary port in time, it indicates that the ring network is complete and the master node will keep the secondary port blocked. If the secondary port of the master node cannot receive HELLO message in the specified time, it is considered that a link fault has occurred on the ring network. The fault handling process is the same as the LINK_DOWN process mechanism.

Link recovery

There are two situations to deal with:

(1) LINK_UP escalation and processing

After the ports of the transit node that belong to the ERRP region are re-up, the master node may find loop recovery after a certain period of time. In the time, the network may form a temporary loop, which makes data VLAN produce a broadcast storm.

In order to prevent the generation of the temporary loop, the transit node moves to the Preforwarding state and immediately blocks the port that has just been recovered, after it finds the port accessing the ring network re-up. At the same time, the transmitting node that has recovered the link sends a LINK_UP message to the master node from ERRP port that is paired with the recovery port in the UP state. After receiving the LINK_UP message from the transmitting node, the master node sends a COMMON_FLUSH_FDB message from the primary port and the secondary port to notify all transit nodes to refresh the FDB table. The

port recovered by the transit node only releases the blocked state after receiving the COMPLETE_FLUSH_FDB packet sent by the master node or the Preforward timer expires.

The response of the master node to the LINK_UP message does not represent the response processing to the ring network recovery. If multiple links on the ring network fail and then one of the links is restored, the LINK_UP reporting mechanism and the response mechanism of the master node are introduced to quickly refresh the FDB tables of the nodes on the ring.

(2) Ring network recovery processing:

Ring network recovery processing is initiated by the main node. The master node sends the Hello messages periodically from the master port. After the faulty link on the ring network is restored, the master node will receive its own test messages from the secondary port. After receiving the HELLO message from the host, the master node first moves the state back to the complete state, blocks the secondary port, and then sends the COMPLETE_FLUSH_FDB message from the primary port. After receiving the COMPLETE_FLUSH_FDB message, the transit node moves back to the Link_Up state, releases the temporarily blocked port, and refreshes the FDB table.

If the COMPLETE_FLUSH_FDB message is lost during transmission, a backup mechanism is adopted to recover the temporarily blocked port of the transit node. The transmission node is in the Pre-forwarding state, if the COMPLETE_FLUSH_FDB message from the master node is not received in the specified time, Self-release temporary blocking port, restore data

communication.

36.1.4 Multi-loop Intersection Processing

Multi-ring and single-ring is almost the same, The difference between a multi-ring and a single ring is that multiple rings are introduced the sub-ring protocol message channel state detection mechanism in the main ring, after the channel is interrupted, the edge port of the edge node is blocked before the secondary port of the master node of the sub-ring is released to prevent the data loop from forming between the sub-ring. For details, see Sub-channel Protocol Channel Status Check Mechanism on the Main Ring.

In addition, when a node on the master ring receives a COMMON-FLUSH-FDB or COMPLETE-FLUSH-FDB message from the sub-ring, it will refresh the FDB table. The COMPLETE-FLUSH-FDB of the sub-ring does not cause the sub ring transit node to release the temporarily blocked port. The COMPLETE-FLUSH-FDB message of the primary ring does not do so.

36.2 Configure ERRP

36.2.1 ERRP Configuration List

Configuration Task	Description	Detailed Configuration
ERRP Configuration List	Required	36.2.2

Configure Time Parameter	Optional	36.2.3
Configure Domain	Required	36.2.4
Configure Work Mode	Optional	36.2.5
Configure Control VLAN	Required	36.2.6
Configure the Ring	Required	36.2.7
Enable/Disable ERRP Ring	Required	36.2.8
Configure the Query Solicit Function	Optional	36.2.9
Configure the Topology Discovery Function	Optional	36.2.10
Display and Maintenance of ERRP	Optional	36.2.11

36.2.2 Enable/Disable ERRP

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enable ERRP	**errp**	
Disable ERRP	**undo errp**	

36.2.3 Configure Time Parameter

User can modify the ERRP timer parameters as requirement, but make sure that the timer parameters are the same on all nodes. Ensure that the value of the Failed timer is not less than 3 times the Hello timer value.

Operation	Command	Remarks

Enter the global configuration mode	**system-view**	
Enter the global configuration mode	**errp hello-timer** *value*	
Configure the health message timer	**errp fail-timer** *value*	
Configure the information timeout timer	**errp preup-timer** *value*	
Configure the recovery delay timer	**errp hello-timer** *value*	

36.2.4 Configure Domain

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Create and enter the domain configuration mode	**errp domain** *domain-id*	
Delete domain	**undo errp domain** [*domain-id*]	

36.2.5 Configure Work Mode

In order to connect with other vendors device, user can modify the work mode in the ERRP domain, and configure multiple ERRP domains on the same device. Each domain can be configured with different work modes. All the nodes in the same ERRP domain must work in the same mode.

By default, it works in standard mode. Support compatible with EIPS and RRPP.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	

Create and enter the domain configuration mode	**errp domain** *domain-id*	
Configure work mode	**workmode** { standard | huawei | eips-subring }	

36.2.6 Configure Control VLAN

Control VLAN is relative to the data VLAN, the data VLAN is used to transmit data message, control VLAN is used to transmit ERRP protocol message.

Each ERRP domain has two control VLANs, called the primary control VLAN and the sub-control VLAN. The protocol messages of the primary ring are propagated in the master control VLAN, and the protocol messages of the sub-ring are propagated in the sub-control VLANs. User needs to specify only the primary control VLAN and a VLAN with the maximum control VLAN ID of 1 as the sub-control VLAN.

When an ERRP port sends protocol messages, it always takes control VLAN tags, regardless of whether the ERRP port is in trunk mode.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Create and enter the domain configuration mode	**errp domain** *domain-id*	
Configure control VLAN	**control-vlan** *vlan-id*	
Delete control VLAN	**undo control-vlan**	

36.2.7 Configure the Ring

To avoid conflict between ERRP and STP in calculating port blocking / releasing status, ERRP and STP are mutually exclusive on the port. Before specifying an ERRP port, user must disable STP on the port.

If a device is on multiple ERRP rings of the same ERRP domain, only one master ring can exist. The node role of the device on other sub-rings can be only the edge node or assistant edge node.

The ERRP field takes effect only when both the ERRP protocol and the ERRP ring enable. To enable the ring, user must first configure the control VLAN.

ERRP ring is divided into the main ring and sub-ring. Respectively use 0,1.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Create and enter the domain configuration mode	**errp domain** *domain-id*	
Configure ring and ring levels	**ring** ring-id **role master primary-port** *pri-port* **secondary-port** *sec-port* **level** *level*	
Configure transit node	**ring** *ring-id* **roletransit primary-port** *pri-port* **secondary-port** *sec-port* **level** *level*	
Configure **edge** node	**ring** *ring-id* **roleedge common-port** *common-port* **edge-port** *edge-port*	

Configure **assistant-edge**node	**ring** *ring-id* **role assistant-edge** **common-port** *common-port* **edge-port** *edge-port*	
Delete ring	**undo ring** [*ring-id*]	

36.2.8 Enable/Disable ERRP Ring

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Create and enter the domain configuration mode	**errp domain** *domain-id*	
Enable/Disable ERRP Ring	**ring** *ring-id* { **enable** | **disable** }	

36.2.9 Configure the Query Solicit Function

This function is used to cooperate with IGMP SNOOPING. When the topology of the ERRP ring network changes, it immediately notifies the IGMP querier to resend the IGMP general query to update the IGMP SNOOPING multicast database in time. Currently, there is not related standard. The query solicit message is private and the IGMP type is 0xff.

Specific implementation is as follows:

1. The default Query solicitation function is enabled on the master node, the transit node closes Query solicitation function.

2. The master node topology change is determined by: The master node status is from Health

to Fault or from Fault to Health.

3. Other nodes topology changes are determined by: The primary and secondary port status is from forwarding to non-forwarding (block/disable) or from non-forwarding to forwarding (block/disable).

4. When the node detects a topology change: If the node itself is the IGMP querier, it immediately sends a General Query message to all the ports. Otherwise, immediately send a Query Solicit message to all ports;

5. After the IGMP querier receives the Query Solicit message: Respond immediately to the receiving port a General Query message.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Create and enter the domain configuration mode	**errp domain** *domain-id*	
Enable query-solicit	**ring** *ring-id* **query-solicit**	
Disable query-solicit	**undo ring** *ring-id* **query-solicit**	

36.2.10 Configure the Topology Discovery Function

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Create and enter the domain configuration mode	**errp domain** *domain-id*	

Enable topo-collect	**topo-collect**	
Disable topo-collect	**undo topo-collect**	

36.2.11 Display and Maintenance of ERRP

Operation	Command	Remarks
Display ERRP Domain	**display errp** [domain *domain-id* [ring *ring-id*]]	
Display ERRP control-vlan	**display errp control-vlan** [*vlan-id*]	
Display ERRP topology discovery	**display errp topology** [domain *domain-id* [ring *ring-id*] | summary [domain *domain-id* [ring *ring-id*]]	

Chapter 37 ERPS

37.1 ERPS Overview

ERPS (Ethernet Ring Protection Switching) is released by ITU-T with the convergence rate of telecommunication level. If all devices inside the ring support this agreement, it can achieve intercommunication.

37.1.1 ERPS Basic Conception

ERPS mainly includes ERPS ring, node, port role and port status.

1. ERPS Example

EPRS instance is formed by the same instance ID, control VLAN and interconnected Switches.

2. Control VLAN

Control VLAN is the transmission VLAN of ERPS protocol, and the protocol packet will carry corresponding VLAN tag.

3. RPL

RPL (Ring Protection Link), Link designated by mechanism that is blocked during Idle state to

prevent loop on Bridged ring

4. ERPS ring

ERPS ring is EPRS basic unit. It composed by a set of the same control VLAN and the interlinked L2 Switch equipment.

5. Node

The L2 Switch equipment added in ERPS ring are called nodes. Each node cannot be added to more than two ports in the same ERPS ring. The nodes are divided into RPL Owner, Neighbor, Next Neighbor, and Common.

6. Port Role

In ERPS, port roles include: RPL Owner, Neighbor, Next Neighbor, and Common:

RPL Owner: An ERPS ring has only one RPL Owner port configured by the user and it prevents loops in the ERPS ring via blocking the RPL Owner port. The node that owns the RPL Owner port becomes the RPL Owner node.

RPL Neighbour: An ERPS ring has only one RPL Neighbor port configured by the user and it must be a port connected to the RPL Owner port. If the network is normal, it will block together with the RPL Owner port to prevent loops in the ERPS ring. The node with the RPL Neighbor port becomes the RPL Neighbor node.

RPL Next Neighbour: An ERPS ring can have up to two RPL Next Neighbor ports configured by the user. It must be the port connecting the RPL Owner node or the RPL Neighbor node. To become the RPL Next Neighbor node, the RPL Next Neighbor port should own the node of RPL Next Neighbor port.

Note:RPL Next Neighbour nodes are not much different from ordinary nodes. They can be replaced by Common nodes.

Common: The common port. The ports except RPL owner, Neighbor and Neighbor port are common ports. If the node has only the Common port, this node will become the Common node.

7．Port Status

In the ERPS ring, the port status of the ERPS protocol is divided into three types.

Forwarding: In Forwarding status, the port forwards user traffic and receives / forwards R-APS packets. Moreover, it forwards R-APS packets from other nodes.

Discarding: In the Discarding status, the port can only receive / forward R-APS packets and cannot forward R-APS packets from other nodes.

Disable: port in Linkdown status.

8．Wrok Mode: ERPS operating mode

Work mode includes: revertive and non-revertive.

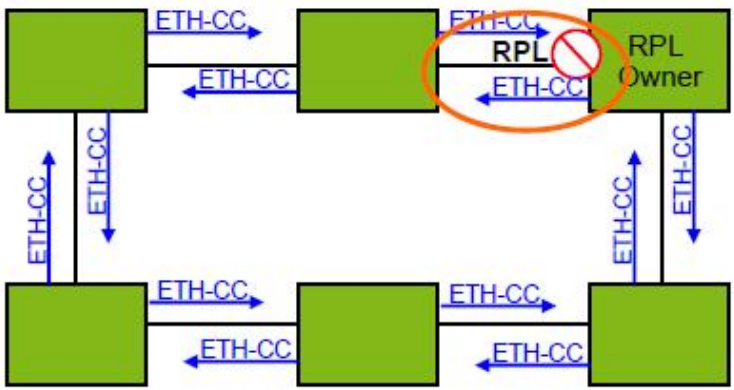
Revertive: When the link fails, the RPL link is in the release protection state and the RPL link is re-protected after the faulty link is restored to prevent loops.

Non-revertive: After the fault is rectified, the faulty node remains faulty (without entering Forwarding) and the RPL link remains in the release protection state.

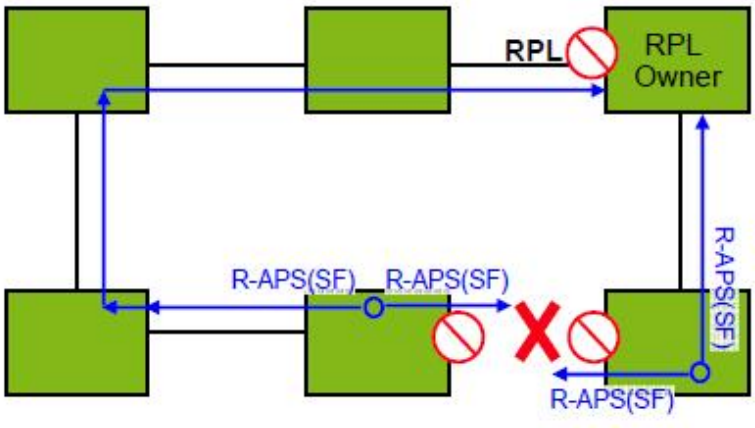
37.1.2 ERPS Ring Protection Mechanism

ERPS uses ETH CFM for link monitoring. When the network is normal, a blocking link is set on the ring network to prevent the ring network from ringing. If a fault occurs in the network, a blocked backup link is opened to ensure uninterrupted link between each node. The general process is as follows:

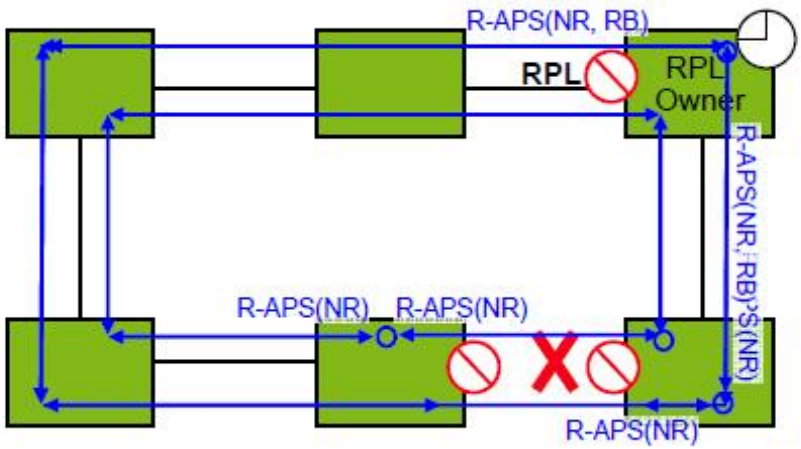
As shown , when six devices are connected in a ring and the link is in the IDLE state, the loop is removed via setting the RPL link and locking the port (RPL Owner port).



When a node on the link detects a fault, it immediately blocks the faulty node and reports the fault message (R-APS (SF)) to all the other devices in the ring. After receiving the message, all other nodes refresh the FDB. The RPL owner port receives the fault message, and the recovery port is in the forwarding state. The ERPS ring enters the protection state. As shown in the Figure:



when the link of the faulty device recovers, it sends RAPS (NR) packets to other devices in the ring to inform them that there is no local request. When the RPL owner receives the packet, it will block the port and send the R-APS (NR, RB) message again after some time. After receiving the packet, the other nodes will refresh the FDB entry. Later, the port of the faulty node will be restored to the forwarding state, and the ring will revert to the IDLE state.



37.2 Configure ERPS

37.2.1 ERPS Configuration List

Configuration Task	Description	Detailed Configuration
Enable/Disable ERPS	Required	37.2.2
Configure ERPS Instance	Required	37.2.3
Configure Connectivity Detection of ERRP Link	Optional	37.2.4
Configure ERPS Related Timers	Optional	37.2.5
ERPS Display and Maintenance	Optional	37.2.6

37.2.2 Enable/Disable ERPS

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	

Enable ERPS	**erps**	
Disable ERPS	**undo erps**	

37.2.3 Configure ERPS Instance

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Configure erps instance	**erps instance** *instance-id*	
Configure control-vlan	**control-vlan** *vlan id*	
Configure work-mode	**work-mode** { *revertive* | *non revertive* }	
Configure ring id	**ring** *ring id*	
Configure ring level	**ring** *level*	
Configure ring port role	{ **port0** | **port1** } **ethernet** *interface-num* [neighbor | next-neighbour | owner]	
Configure protected-instance	**protected-instance** *inst-list*	
Enable/Disable ring	**ring** [enable | disable]	

Note:

About Ring ID: ERPS ring ID, the last byte of the DMAC in the R-APS message is Ring Id. From G.8032 can be learned that the ERPS ring ID can be the same, and the control VLAN needs to be different. The reverse is also true. The ring ID of each instance can be 1 to 239, and the control VLAN does not allow duplication.

To configure ERPS port, you must disable the spanning tree.

37.2.4 Configure Connectivity Detection of ERRP Link

In ERPS, there is no HELLO packet to monitor link connectivity in real time. Instead, it uses the CC function in ETH CFM to detect the link connectivity by sending ETH-CC messages between the two ports. Therefore, you need to configure the CFM CC for the ports in the ERPS. In the ERRP instance, you need to configure the MEL (MEG level, which must be consistent with the CFM configuration).

For more information about CFM, please refer to the CFM User Manual.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Configure erps instance	**erps instance** *instance-id*	
Configure MEL	**mel** *level*	

37.2.5 Configure ERPS Related Timers

ERPS has two timers: WTR timer and Guard timer.

WTR timer: When the RPL owner port is restored to the Forwarding state due to another device or link failure, if the fault is restored and some ports may not have been changed from the Down state to the Up state, it starts the WTR timer when the RPL owner port receives the fault-free RAPS packet from a port to prevent the shock of blocking point; If the fault is received before the timer expires, the WTR timer is disabled. If a faulty RAPS packet from another port is received before the timer times out, the WTR timer will be disabled. If the WTR timer does not receive any faulty RAPS packets from other ports, it will block the RPL Owner

port and send RPL blocking RAPS packets after timed out. After receiving the packet, the other ports set the forwarding state of its own port as Forwarding state.

Guard timer: After the failure recovery, the equipment involved in link failure or node failure will send R-APS packet to the other devices and it will start the Guard Timer at the same time. The device does not process RAPS packets until the timer times out with the purpose to prevent the receipt of outdated faulty R-APS packets. If the device receives the faulty RAPS packet from another port after the timer times out, the port forwarding state will turn to Forwarding.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Configure erps instance	**erps instance** *instance-id*	
Configure wtr-timer	**wtr-timer** *timer value*	
Configure guard-timer	**guard-timer** *timer value*	

37.2.6 ERPS Display and Maintenance

Operation	Command	Remarks
Display ERPS information	**display erps** [*instance instance id*]	
Display control-vlan	**display erps control-vlan** [*vid*]	
Display the sending and receiving packets	**display erps** [*instance instance id*] **statistics**	
Display the sending and receiving packets	**clear erps** [*instance instance id*] **statistics**	

Chapter 38 FlexLink

38.1 FlexLink Overview

Flex links is layer 2 links backup protocol which provides for STP option scheme. Choose Flex links to realize link backup when the STP is not wanted in customer network. If STP enables, flex links is disabled. Flex links consists of a pair of interfaces (can be ports or convergent interface). One interface is transmitting data, the other is standby. The backup interface starts transmitting data when there is default in master link. The failure interface will be standby when it turns well and it will be transmitting data in 60 seconds when preempt mechanism is set. Flex links interface should disable STP and Flex links interface can configure bandwidth and delay being preempt mechanism and the superior one will be the master interface. There must be trap alarm when master or backup link default.

Flex Link is dedicated to dual-uplink networks. It delivers the following benefits:

-Keeping one uplink connected and the other blocked when both uplinks in a dual uplink network are healthy, thus preventing broadcast storms caused by network loops.

-Switching the traffic to the backup link within a few sub-seconds when the primary link fails, thus ensuring the normal forwarding of traffic in the network.

-Easy to configure.

38.1.1 Basic Concept of Flex Links

1. Flex Links group

A Flex link group consists of only two member ports: the master and the slave. At a time, only one port is active for forwarding, and the other port is blocked, that is, in the standby state. When link failure occurs on the active port due to port shutdown or presence of unidirectional link for example, the standby port becomes active to take over while the original active port transits to the blocked state.

2. Master port

The master port of a Flex link group is a port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface.

3. Slave port

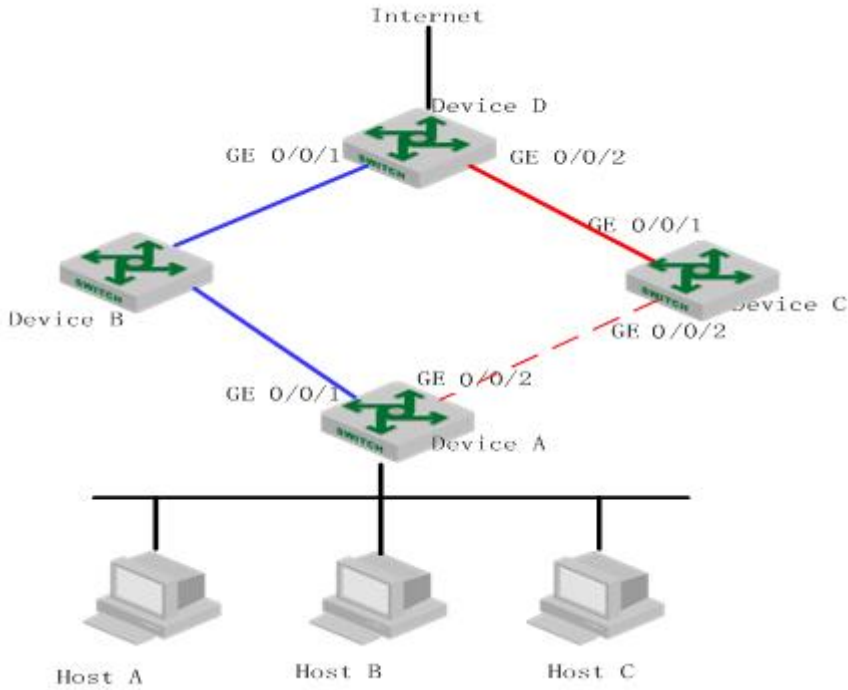
The slave port of a Flex link group is another port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface. The link on which the slave port resides is called the backup link.

4. MMU (MAC address-table Move Update)message

When link Switch over occurs in a Flex link group, the old forwarding entries are no longer useful for the new topology. Therefore, all devices in the network need to refresh their MAC address forwarding entries. Flex Link notifies devices to refresh their MAC address forwarding entries by sending MMU messages to them.

38.1.2 Operating Mechanism of Flex Link

This section uses the network shown in the below figure to describe the Flex link mechanism as the link status transiting from normal, to faulty, and then to recovery.



Link-Normal Operating

GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 of Switch A form a Flex link group, with the former as the master port and the latter as the slave port. When both uplinks are healthy, the master port is in the forwarding state, while the slave port is in the standby state, and the links on which the two ports are seated respectively are called the primary link and the backup link. In this case, data is transmitted along the link indicated by the blue line. There is no loop in the network, hence no broadcast storms either.

Link-Faulty Handling

When the primary link on Switch A fails, the master port GigabitEthernet 0/0/1 transits to the

standby state, while the slave port GigabitEthernet 0/0/2 transits to the forwarding state. A link Switchover occurs. After the link Switch over, the MAC address forwarding entries kept on the devices in the network may become incorrect, and need to be refreshed, so that traffic can be rapidly Switched to another link, thus avoiding traffic loss. Currently, one mechanism is available for refreshing MAC address forwarding entries: MMU message-notified refreshing.

This mechanism is applicable when the upstream devices (such as Switch B, Switch C, and Switch D in the Figure) support Flex Link and are able to recognize MMU messages.

To enable rapid link Switch over, you need to enable Switch A to send MMU messages, and all upstream devices' ports that are on the dual uplink network to receive and process MMU messages.

After link Switchover occurs on Switch A, MMU messages are sent along the new primary link, that is, through GigabitEthernet 0/0/2. When an upstream device receives and handles a MMU message, transmit MAC address carried in the MMU message to the receiving port.

After that, when Switch D receives a data packet destined for Host A, Host B, Host C, Switch D will broadcasts the packet at Layer 2; Switch C will search MAC address table after receiving it, and forward it to Switch A from GE0/0/2; Switch A forward it to Host A, Host B, Host C. In this way, data traffic can be forwarded correctly.

This mechanism will update MAC address without waiting for entry aged. Generally, the whole link will be shifted in milliseconds without traffic lost.

Link-Recovery Working Modes

Flex Link supports three working modes: role preemption, non-role preemption and bandwidth

preemption. Under different modes, the port state changes are different:

- If role preemption is configured, when the primary link recovers, the master port enters the forwarding state and takes over the traffic, while the slave port enters the standby state. The slave port transits from standby to forwarding only when the primary link fails.
- If non-role preemption is configured, when the primary link recovers, the slave port remains in the forwarding state, while the master port remains in the standby state, so as to keep the traffic stable.
- If bandwidth preemption is configured, when the primary link recovers, the slave port remains in the forwarding state if it occupies more bandwidth, while the master port remains in the standby state; the slave port transits from forwarding to standby only when master port occupies more bandwidth.

As shown in the Figure, if role preemption is configured on the Flex link group on Switch A, when the link of GigabitEthernet 0/0/1 on Switch A recovers, GigabitEthernet 0/0/2 is immediately blocked and transits to the standby state, while GigabitEthernet 0/0/1 transits to the forwarding state. If non-role preemption is configured, when the link of GigabitEthernet 0/0/1 on Switch A recovers, GigabitEthernet 0/0/1 remains in the standby state, and no link Switchover occurs, thus keeping the traffic stable.

38.2 Configure FlexLinks

38.2.1 FlexLinks Configuration List

Configuration Task	Description	Detailed Configuration
Configure Flex Links group	Required	38.2.2
Configure Flex Links preemption mode	Optional	38.2.3

Configure Flex links preemption delay	Optional	38.2.4
Configure Flex links MMU	Optional	38.2.5
Flex Links monitor and maintenance	Optional	38.2.6

38.2.2 Configure FlexLinks group

Configure Flex Links group needs specify master and slave port. If master port is Ethernet port, the configuration should be in interface configuration mode; if master port is channel-group port member, the configuration should be in global configuration mode.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure Flex Links group	**channel-group** *channel-group-number_1* **backup** { **interface** *device/slot/port_2* | **channel-group** *channel-group-number_2* }	*channel-group-number_1* is master port,*port_2/channel-group-number_2* is slave port
Delete Flex Links group	**undo channel-group** *channel-group-number_1* **backup**	
Enter interface configuration mode	**interface ethernet** *device/slot/port_1*	
Configure Flex Links group	**port backup** { **interface** *device/slot/port_2* | **channel-group** *channel-group-number_2* }	*port_1* is master port, *port_2/channel-group-number_2* is slave port
Delete Flex Links group	**undo port backup**	

Note:

The STP of master port and slave port should be disabled, and cannot be ERRP port.

38.2.3 Configure FlexLinks Preemption Mode

At a time, only one port is active for forwarding, and the other port is blocked, that is, in the

standby state. When link failure occurs on the active port due to port shutdown or presence of unidirectional link for example, the standby port becomes active to take over while the original active port transits to the blocked state.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	-
Configure Flex Links preemption mode	**channel-group** *channel-group-number_1* **backup** { **interface** *device/slot/port_2* | **channel-group** *channel-group-number_2* } **preemption mode** { **forced** | **bandwidth** | **off** }	*channel-group-number_1* is master port,*port_2/channel-group-number_2* is slave port
Enter interface configuration mode	**interface ethernet** *device/slot/port_1*	
Configure Flex Links preemption mode	**port backup** { **interface** *device/slot/port_2* | **channel-group** *channel-group-number_2* } **preemption mode** { **forced** | **bandwidth** | **off** }	*port_1* is master port, *port_2/channel-group-number_2* is slave port

38.2.4 Configure FlexLinks Preemption Delay

After Configure Flex Links preemption mode, the port will not be active status immediately. There has to be a time delay. The default delay is 45s.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	-
Configure Flex links preemption delay	**channel-group** *channel-group-number_1* **backup** { **interface** *device/slot/port_2* | **channel-group** *channel-group-number_2* } **preemption delay** <1-60>	*channel-group-number_1* is master port,*port_2/channel-group-number_2* is slave port
Enter interface configuration mode	**interface ethernet** *device/slot/port_1*	-
Configure Flex links preemption	**port backup** { **interface** *device/slot/port_2* |	*port_1* is master

delay	**channel-group** *channel-group-number_2* } **preemption mode** <1-60>	port, *port_2/channel-group-number_2* is slave port

38.2.5 Configure FlexLinks MMU

MMU messages are used by a Flex link group to notify other Switches to refresh their MAC address forwarding entries and ARP/ND entries when link Switchover occurs in the Flex link group. MMU messages are common unicast data packets, and will be dropped by a blocked receiving port. This function is disabled by default.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	-
Configure Flex links MMU	**mac-address-table move update** { **transmit** | **receive** }	*port_1* is master port, *port_2/channel-group-number_2* is slave port

38.2.6 FLexLinks Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Operation	Command	Remarks
Display configured Flex Links group	**display interface Switch backup**	
Display Flex Links MMU status	**display mac-address-table move update**	

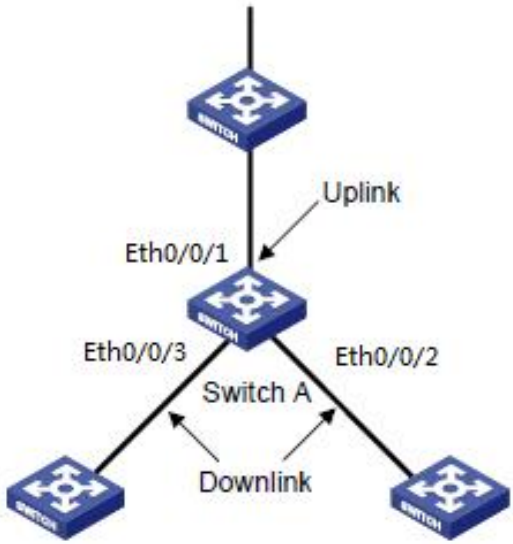
Chapter 39 Monitorlink

39.1 Monitorlink Overview

Monitor Link is developed to complement the Flex Link feature. By monitoring the uplink, and synchronizing the downlink with the uplink, Monitor Link triggers the Switchover between the primary and backup links in a Flex link group, thus perfecting the link redundancy mechanism of Flex Link.

39.1.1 Monitor Link Group

A monitor link group is a set of uplink and downlink ports. Downlink ports adapt to the state changes of uplink ports.



As shown in the figure, ports GigabitEthernet 0/0/1, GigabitEthernet 0/0/2, and GigabitEthernet 0/0/3 of Switch A form a monitor link group.

1. Uplink Port

An uplink port is a monitored port in a monitor link group. It is a port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface.

As shown in the figure, GigabitEthernet 0/0/1 of Switch A is the only uplink port of the monitor link group configured on the device.

For a monitor link group that has multiple uplink ports, as long as at least one of its uplink ports is in the forwarding state, the monitor link group is up. However, when all uplink ports of the monitor link group fail, the monitor link group goes down, shutting down all the downlink ports.

If no uplink port is specified in a monitor link group, the system considers the monitor link group's uplink ports to be faulty, and thus shuts down all the downlink ports in the monitor link group.

2. Downlink Port

A downlink port is a monitoring port in a monitor link group. It is another port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface.

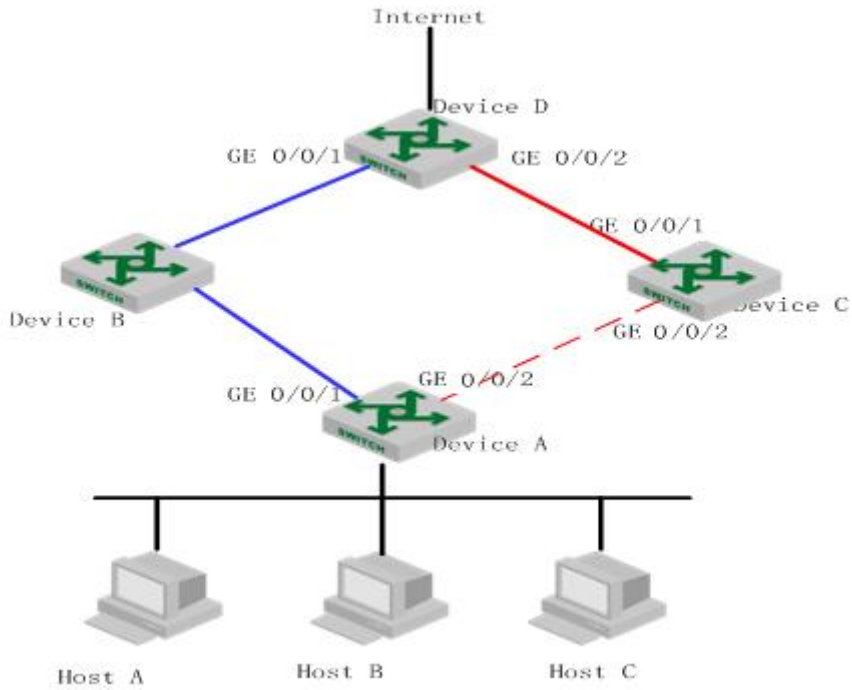
As shown in the figure, GigabitEthernet 0/0/2 and GigabitEthernet 0/0/3 of Switch A are two downlink ports of the monitor link group configured on the device.

Note:

When a monitor link group's uplink ports recover, only downlink ports that were blocked due to uplink port failure will be brought up. Downlink ports manually shut down will not be brought up automatically. The failure of a downlink port does not affect the uplink ports or other downlink ports.

39.1.2 Monitor Link Mechanism

As shown in the below figure, to provide reliable access to the Internet for the hosts, a Flex link group is configured on Switch A. GigabitEthernet 0/0/1 is the master port of the Flex link group, and is in the forwarding state. GigabitEthernet 0/0/2 is the slave port.



To avoid traffic interruption due to the failure of the link on which GigabitEthernet 0/0/1 of Switch B resides, configure a monitor link group on Switch B, and specify GigabitEthernet 0/0/1 as the uplink port, and GigabitEthernet 0/0/2 as the downlink port.

When the link on which GigabitEthernet 0/0/1 of Switch B resides fails, the monitor link group shuts down its downlink port GigabitEthernet 0/0/2, triggering a link Switchover in the Flex link group configured on Switch A.

When the link on which GigabitEthernet 0/0/1 of Switch B resides recovers, the downlink port GigabitEthernet 0/0/2 is also brought up, triggering another link Switchover in the Flex link group if role preemption is configured in the Flex link group on Switch A.

Collaboratively, Monitor Link and Flex Link deliver reliable link redundancy and fast convergence for dual-uplink networks.

39.2 Configure Monitor Link

39.2.1 MonitorLink Configuration List

Configuration Task	Description	Detailed Configuration
Configure MonitorLink Group	Required	39.2.2
Monitor Link monitor and maintenance	Optional	39.2.3

39.2.2 Configure MonitorLink Group

If the port is Ethernet port, configuration should be in interface configuration mode; if port is channel-group member, configuration should be in global configuration mode.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Monitor Link for channel-group	**channel-group** *channel-group-number* **monitor-link-group** *group-ID* { **uplink** | **downlink** }	
Delete channel-group from Monitor Link group	**undo channel-group** *channel-group-number* **monitor-link-group** *group-ID* { **uplink** | **downlink** }	
Enter interface configuration mode	**interface ethernet** *device/slot/port*	
Monitor Link for port	**port monitor-link-group** *group-ID* { **uplink** | **downlink** }	
Delete port from Monitor Link group	**undo port monitor-link-group** *group-ID* { **uplink** | **downlink** }	

39.2.3 MonitorLink Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Operation	Command	Remarks
Display Monitor Link group	**display monitor-link-group**	

Chapter 40 L3 Base Function Configuration

40.1 L3 Base Function Overview

The L3 Switch is a 10-Gigabit intelligent routing Switch based on the application specific integrated circuit (ASIC) technology and supports layer 2 (L2) and layer 3 (L3) forwarding. It performs L2 forwarding when hosts in the same virtual local area network (VLAN) access each other and L3 forwarding when hosts in different VLANs access each other.

40.2 ConfigureL3 Base Function

40.2.1 L3 Base Function Configuration List

Configuration Task	Description	Detailed Configuration
Planning VLANs and creating L3 interfaces	Required	40.2.2
Configure the forwarding mode	Required	40.2.3
Creating VLAN interfaces for common VLANs	Required	40.2.4
Creating superVLAN interfaces and adding VLANs to the superVLAN	Required	40.2.5
Configure IP addresses for VLAN or superVLAN interfaces	Required	40.2.6

Configure an IP address range for VLAN or superVLAN interfaces	Required	40.2.7
Configure the Address Resolution Protocol (ARP) proxy	Required	40.2.8
Display interface configurations	Required	40.2.9
Configure unicast reverse path forwarding (URPF)	Required	40.2.10
Disabling the function of sending Internet Control Message Protocol (ICMP) packets with an unreachable destination host on interfaces	Required	40.2.11

40.2.2 Planning VLANs and Creating L3 Interfaces

For details about VLAN planning, see VLAN configurations.

L3 interfaces are classified into common VLAN interfaces and superVLAN interfaces. Common VLAN interfaces are created on VLANs and superVLAN interfaces on superVLANs (superVLANs do not exist or contain any port).

40.2.3 Configure the Forwarding Mode

The L3 Switch supports stream forwarding and network topology-based forwarding. In stream forwarding mode, The L3 Switch identifies the failed route or the unreachable destination host route and sends packets to the CPU for further processing. In network topology-based forwarding mode, The L3 Switch directly discards the packets. By default, The L3 Switch works in stream forwarding mode.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Set the packet forwarding mode in the system to stream forwarding.	**ip def cpu**	
Set the packet forwarding mode in the system to network topology-based forwarding.	**undo ip def cpu**	
Display the configured packet forwarding mode.	**display ip def cpu**	

40.2.4 Creating VLAN Interfaces for Common VLANs

A VLAN interface needs to be configured for each VLAN that performs L3 forwarding or the VLAN needs to be added to the superVLAN.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Create a VLAN interface with the VLAN ID being **vid** and enter the VLAN interface configuration mode.	**interface vlan-interface** *vid*	
Return to the global configuration mode.	**quit**	

Delete the VLAN interface with the VLAN ID being **vid**.	**undo interface vlan-interface** *vid*	

40.2.5 Creating SuperVLAN Interfaces and Adding VLANs to the SuperVLAN

SuperVLAN interfaces are used for communication between hosts in different VLANs in the same network segment. SuperVLAN interfaces are implemented through the ARP proxy.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Create a superVLAN interface with the interface ID being **vid** and enter the superVLAN interface configuration mode.	**interface supervlan-interface** *vid*	
Return to the global configuration mode.	**quit**	
Delete the superVLAN interface with the interface ID being **vid**.	**undo interface supervlan-interface** *vid*	
Configure sub VLANs for the superVLAN interface.	**subvlan** *vid*	
Delete the sub VLANs configured	**undo subvlan** *vid*	

for the superVLAN interface.		

40.2.6 Configure IP Addresses for VLAN or SuperVLAN Interfaces

Each VLAN or superVLAN interface can be configured with a maximum of 32 IP addresses and the IP addresses of VLAN or superVLAN interfaces cannot be in the same network segment. The first IP address of an interface will be automatically selected as the primary IP address. When the primary IP address is deleted, the interface automatically selects another IP address as the primary IP address or a configured IP address can be manually specified as the primary IP address. For example, if the IP address of VLAN interface 1 is 10.10.0.1/16, the IP addresses of other interfaces must not be in the 10.10.0.0/16 network segment (such as 10.10.1.1/24).

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Configure an IP address and a mask for the interface.	**ip address** *ipaddress ipaddress mask*	
Delete all IP addresses of the interface.	**undo ip address**	
Delete the specified IP address of	**undo ip address** *ipaddress ipaddress mask*	

the interface.		
Configure the primary IP address for the interface.	**ip address primary** *ipaddress*	

40.2.7 Configure an IP Address Range for VLAN or SuperVLAN Interfaces

Each VLAN or superVLAN interface can be configured with a maximum of eight IP address ranges. After an IP address range is configured, only the ARP entries within this range can be learnt so as to restrict user access. When a VLAN or superVLAN interface is deleted, relevant configurations are automatically deleted.

For superVLAN interfaces, sub VLANs can be specified at the same time so that the set address range is applicable only to these sub VLANs.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface<*vid*>** **interface supervlan-interface** <*vid*>	
Configure the IP address range supported by this interface, ranging from **startip** to **endip**.	**ip address range** *startip endip*	
Delete all IP address ranges	**undo ip address range**	

supported by the interface.		
Delete the specified IP address ranges supported by the interface.	**undo ip address range** *startip endip*	
Configure the IP address range for sub VLANs of the superVLAN.	**ip address range** *startip endip* **vlan** *vlanid>*	
Delete the IP address ranges of the sub VLANs of the superVLAN.	**undo ip address range** *startip endip* **vlan** *vlanid*	

40.2.8 Configure the ARP Proxy

ARP request packets are broadcast packets and cannot pass through VLANs. If the ARP proxy function is enabled, ARP interaction is supported between hosts in sub VLANs of the same superVLAN. When the ARP proxy is disabled, the hosts of the sub VLANs in the superVLAN interface cannot communicate with each other.

By default, the ARP request packets from all sub VLANs are processed in the preceding manner. In addition, relevant commands can be used to prevent the ARP request packets from a sub VLAN from being broadcast to other sub VLANs when they are processed by the ARP proxy.

Operation	Command	Remarks
Enter the VLAN configuration mode.	**Vlan** *vlanid*	
Enable the arp-proxy function for the	**arp-proxy**	

VLAN.		
Disable the arp-proxy function for the VLAN.	**undo arp-proxy**	
Enable the arp-proxy broadcast function for the VLAN.	**arp-proxy broadcast**	
Disable the arp-proxy broadcast function for the VLAN.	**undo arp-proxy broadcast**	
Display the information about the ARP proxy configured in the system.	**display arp-proxy**	
Display information about the ARP proxy broadcast function configured in the system.	**display arp-proxy broadcast**	

40.2.9 Display VLAN and SuperVLAN Interface Information

The L3 Switch integrates VLAN interface information and superVLAN interface information. They can be viewed by running a unified display command.

Operation	Command	Remarks
Display information about the VLAN and superVLAN interfaces currently configured in the system.	**display ip interface** [[**vlan-interface** *vlanid*] | [**supervlan-interface** *supervlanid*]]	

40.2.10 Configure URPF

URPF aims to prevent network attack behaviors based on source address spoofing. URPF obtains the source address and ingress interface of a packet and uses the source address as the destination address to query the routing table for the matching route. The packet is forwarded if it meets conditions and discarded if it does not meet conditions. Two URPF modes are supported:

Strict mode: In this mode, the source address must exist in the routing table and the egress interface of the source address of the packet is the same as the ingress interface of the packet.

Loose mode: In this mode, the system only checks whether the source address of the packet exists in the unicast routing table. If yes, the packet is forwarded.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Enable URPF for this interface and specify the URPF mode.	**urpf** { **loose** | **strict** }	
Disable URPF for this interface.	**undo urpf**	
Display URPF information in the system.	**display urpf**	

40.2.11 Disabling the Function of Sending ICMP Packets with an Unreachable Destination Host on Interfaces

To avoid attacks from address scanning software similar to ip-scan, users can disable the function of sending ICMP packets with an unreachable host on interfaces.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Enable the function of this interface for sending ICMP packets with an unreachable destination	**ip icmp unreachable**	
Disable the function of this interface for sending ICMP packets with an unreachable destination	**undo ip icmp unreachable**	
Display the configuration of the function of sending ICMP packets with an unreachable destination	**display ip icmp unreachable**	

Chapter 41 Static Route Configuration

41.1 Static Route Overview

The Switch is an ASIC-based Gigabit intelligent Switch, in which a layer-3 forwarding and routing table is maintained to specify the next hops of routes and relevant information. These routes may be learned dynamically through routing protocols or added manually. A static route is a route to an address or a network segment which is configured manually.

41.2 Configure Static Route

41.2.1 Static Route Configuration List

Configuration Task	Description	Detailed Configuration
Adds a static routing entry	Required	41.2.2
Deletes a static routing entry	Required	41.2.2
Displays a specified routing entry	Optional	41.2.3
Displays an ECMP routing entry	Optional	41.2.3

41.2.2 Adding/Deleting a Static Route

Operation	Command	Remarks

Enters the global configuration mode.	**ip route** dst-ip mask gate-ip	
Enters the global configuration mode.	**undo ip route dst-ip** mask [gate-ip] **undo ip route static all**	

Notes:

gate-ip: next-hop IP address of a static route, in dotted decimal notation;

dst-ip: destination address of a static route to be added, in dotted decimal notation;

mask: mask of the destination address, in dotted decimal notation.

41.2.3 Display Routing Entries

This command displays the information relevant to the specified routing entry, such as the next-hop address and route type. You can choose to view the routes to a specific destination address, all static routes, and all routes. By default, all routes will be displayed.

Operation	Command	Remarks
Enters the all commands mode.	**display ip route** [*ip-address* [*mask*] | static | rip | ospf]	
Enters the all commands mode.	**display ip route ecmp** [*ip-address* [*mask*] | static | rip | ospf]	

Parameter description:

ip-address: destination address, in dotted decimal notation;

mask: accompany an IP address to specify a destination network segment, in dotted decimal notation;

static: to display all static routing entries;

rip: to display all RIP routing entries;

ospf: to display all OSPF routing entries

Chapter 42 RIP

42.1 RIP Overview

Routing Information Protocol (RIP) is a routing protocol based on the Distance-Vector (D-V) algorithm and has seen wide deployment. It exchanges routing information by sending route update packets over the User Datagram Protocol (UDP) every 30 seconds. If having not received a route update packet from the peer router within 180 seconds, the local router marks all the routes from the peer router as unreachable. If no update packet is received from the peer router yet in 120 seconds after a route is marked as unreachable, the local router deletes the route from its routing table.

RIP uses Hop Count as a routing metric to measure the distance from a destination host. In a RIP network, Hop Count is 0 if a router is directly connected with a network and 1 if a route needs to traverse a router before reaching the destination network, and so on. To restrain the route convergence time, RIP stipulates that Hop Count is an integer ranging from 0 to 15. The distance is considered infinite if Hop Count is larger than or equal to 16. In this case, the destination network or host is unreachable.

RIP has two versions: RIP-1 and RIP-2 (support for plaintext authentication).

To improve routing performance and avoid routing loops, RIP presents the concepts of Split Horizon and Poison Reverse.

Each RIP router manages a routing database, which contains all the destination reachable routing entries on a network. These routing entries include the following information:

Destination address: IP address of a host or network;

Next-hop address: address of a next router on the route to a destination;

Outbound interface: interface from which packets are forwarded;

Metric value: cost of a route from the local router to a destination, which is an integer from 0 to 15.

Timer: time counted from the last modification of a routing entry. The timer is zeroed every time a routing entry is modified.

The RIP startup and operation procedure is described as follows:

Upon RIP startup on a router, the router broadcasts a request packet to its neighboring routers. After receiving the request packet, the neighboring routers (with RIP started) return a response packet which contains the information about their respective local routing tables.

Upon receipt of the response packets, the router that sends the request packet modifies its local routing table.

RIP broadcasts or multicasts the local routing table to its neighboring routers every 30s. The neighboring routers maintain their local routes to select a best route and then broadcast or multicast the modification to their respective neighboring networks, so that the routing update will eventually take effect globally. RIP employs a timeout mechanism to process expired

routes, ensuring that the routes are latest and valid. As an interior routing protocol, RIP helps acquaint routers with the network-wide routing information because of these mechanisms.

RIP has been accepted as one of the standards which regulate the route transmission between a router and a host. L3 Switches forward IP packets across a LAN the same way as routers. Therefore, RIP is also widely deployed on L3 Switches. It is applicable to most campus networks and regional networks with a simple structure and good continuity but not recommended in complex large networks.

42.2 Configure RIP

42.2.1 RIP Configuration List

Configuration Task	Description	Detailed Configuration
Enabling RIP	Required	42.2.2
Specifying the IP network segment to run RIP	Required	42.2.3
Configurethe Passive interface	Required	42.2.4
Specifying the RIP version for an interface	Required	42.2.5
Configure Default Metric Value	Required	42.2.6
Enabling the Route Aggregation Function	Required	42.2.7
Configure RIP Packet Authentication	Optional	42.2.8
Configure Split Horizon	Optional	42.2.9
Setting an Additional Routing Metric	Optional	42.2.10

Defining a Prefix List	Optional	42.2.11
Configure Route Redistribution	Optional	42.2.12
Configure Route Filtering	Required	42.2.13
Display RIP Configuration	Required	42.2.14

42.2.2 Enabling RIP

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enters the rip configuration mode.	**router rip**	
Enters the global configuration mode.	**undo router rip**	

42.2.3 Specifying the IP Network Segment to Run RIP

By default, an interface does not send or receive RIP packets until the IP network segment to run RIP is specified by the administrator even if RIP is enabled on the interface.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enters the rip configuration mode.	**router rip**	
Runs the command in RIP configuration mode.	**network ip-address**	
Runs the command in RIP configuration mode.	**undo network ip-address**	

42.2.4 Configurethe Passive interface

System support to block RIP on vlan-interface, which can be implemented by passive-interface command, after using this command, the RIP update packets will not be sent out from this interface.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter RIP configuration mode	**router rip**	
Configure passive-interface	**passive-interface** { default | vlan-interface *vlanid* | supervlan-interface *vlanid*}	
Delete passive-interface	**undo key passive-interface** { default | vlan-interface *vlanid* | supervlan-interface *vlanid* }	

42.2.5 Specifying the RIP Version for an Interface

RIP has two versions: RIP-1 and RIP-2. You can specify the version of the RIP packets to be processed by an interface.

RIP-1 packets are transmitted in broadcast mode. RIP-2 packets may be transmitted in either broadcast or multicast mode. The multicast mode is used by default. In RIP-2, the multicast address is 224.0.0.9.

When the multicast mode is used, non-RIP hosts on the same network will not receive RIP broadcast packets and RIP-1 hosts will not receive or process the RIP-2 routes with a subnet mask. A RIP-2 interface can also receive the RIP-1 broadcast packets.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enters the rip configuration mode.	**router rip**	
Runs the command in vlan-interface configuration mode	**version** { **1** | **2** }	
Enter the VLAN-interface or Supervlan-interface configuration mode	**interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configure RIP receive Version	**ip rip receive version** { 1 | 2 [bcast | mcast] }	By default，Version is 2mcast
Configure RIP default receive Version	**undo ip rip receive version**	
Configure RIP send Version	**ip rip send version** { 1 | 2 [bcast | mcast] }	By default，Version is 2mcast
Configure RIP default send Version	**undo ip rip send version**	

Notes:

A RIP-1 interface can send and receive RIP-1 broadcast packets. A RIP-2 broadcast interface can receive RIP-1 packets and RIP-2 broadcast packets but not RIP-2 multicast packets. A RIP-2 multicast interface can send and receive RIP-2 multicast packets.

42.2.6 Configure Default Metric Value

This function is to set the default RIP Metric Value .

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter RIP configuration mode	**router rip**	
Configure default metric	**default-metric** *metric*	
Delete default metric	**undo default-metric**	

42.2.7 Enabling the Route Aggregation Function

Route aggregation consolidates the routes on different subnets of a natural network segment into one route with a natural mask and sends the route to another network segment. This function minimizes both the number of entries in a routing table and the amount of information that needs to be exchanged.

RIP-1 sends only the routes with a natural mask, that is, aggregate routes. RIP-2 supports the subnet mask. To broadcast all the subnet routes, you should disable the route aggregation function of RIP-2.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter RIP configuration mode	**router rip**	
Configure aggregation address	**aggregate-address** *ip-address/mask-length*	
Delete aggregation address	**undo aggregate-address** *ip-address/mask-length*	

42.2.8 Configure RIP Packet Authentication

RIP-1 does not support packet authentication. A RIP-2 interface, however, can be configured with packet authentication in plaintext or MD5.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter the VLAN-interface or Supervlan-interface configuration mode	**interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configure MD5 authentication	**ip rip authentication mode md5 key-chain** *key-string*	
Configure text authentication	**ip rip authentication mode text passwd** *passwd*	
Restores RIP packet authentication.	**undo ip rip authentication**	

42.2.9 Configure Split Horizon

Split horizon is designed to prevent the routes learned on an interface from being sent through the interface, which avoids routing loops. This function must be disabled in some special situations to ensure correct route advertisement at the cost of advertisement efficiency. By default, split horizon can be enabled on an interface.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter the VLAN-interface or	**interface** { vlan-interface |	

Supervlan-interface configuration mode	supervlan-interface } *vlan-id*	
Enable split-horizon function	**ip rip split-horizon**	By default,it is enabled
Enable split-horizon poisoned-reverse function	**ip rip split-horizon poisoned-reverse**	By default,it is disabled
Disable split-horizon function	**undo ip rip split-horizon**	
Disable split-horizon poisoned-reverse function	**undo ip rip split-horizon poisoned-reverse**	

42.2.10 Setting an Additional Routing Metric

The additional routing metric value is added to RIP routes on an inbound or outbound interface. It does not change the routing metric value of routes in the routing table but adds a designated metric value to the routes to be sent or received by an interface.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter the VLAN-interface or Supervlan-interface configuration mode	**interface** { vlan-interface | supervlan-interface } *vlan-id*	
Set additional routing metric value for inbound	**offset-list** { *ip-acl-name* | *ip-acl-number* } **in** *metric* [{ vlan-interface | supervlan-interfac } *vlan-id*]	

Delete additional routing metric value for inbound	**undo offset-list** { *ip-acl-name* | *ip-acl-number* } **in** *metric* [{ vlan-interface | supervlan-interfac } *vlan-id*]	
Set additional routing metric value for outbound	**offset-list** { *ip-acl-name* | *ip-acl-number* } **out** *metric* [{ vlan-interface | supervlan-interfac } *vlan-id*]	
Delete additional routing metric value for outbound	**undo offset-list** { *ip-acl-name* | *ip-acl-number* } **out** *metric* [{ vlan-interface | supervlan-interfac } *vlan-id*]	

42.2.11 Defining a Prefix List

A prefix list is identified by a prefix list name, and may contain multiple entries, each of which corresponds to a network prefix identified by a sequence number. The sequence number indicates the matching sequence of a network prefix.

During prefix matching, the Switch checks the entries in ascending order of sequence numbers. If an entry is matched, it is permitted by the current prefix list and will not be matched next time.

Note: By default, if more than one prefix list entry has been defined, at least one permit entry should be available. The deny entries can be defined in advance so that the routes that do not meet the condition are filtered quickly. However, if all the entries are prefixed by deny, no route will be permitted by the address prefix list. You are advised to define an entry permit 0.0.0.0/0 after defining multiple deny entries, so that all the routes meeting the condition are permitted. Alternatively, you can run the ip prefix-list default command to change the default configuration.

For details, see the description of this command in a command line manual.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter RIP configuration mode	**router rip**	
Enable sequence-number	**ip prefix-list sequence-number**	
Disable sequence-number	**undo ip prefix-list sequence-number**	
Configure prefix-list	**ip prefix-list** *list-name* **seq** *sequence-number* { deny | permit } { any | *ip-address/mask-length* [ge min-prefix-len [le max-prefix-len] }	
Delete prefix-list	**undo ip prefix-list** *list-name* [seq *sequence-number* { deny | permit } { any | *ip-address/mask-length* [ge min-prefix-len [le max-prefix-len] }]	

42.2.12 Configure Route Redistribution

Routes of protocols other than RIP can be imported into RIP.

In an Ethernet Switch, connected, static, and OSPF routes can be imported into RIP.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter RIP configuration mode	**router rip**	
Configure Route redistribution	**redistribute** { babel | bgp | connected | isis |	

	kernel | ospf | rip | static } **metric** *metric* **route-map** *route-map*	
Delete Route redistribution	**undo redistribute** { babel | bgp | connected | isis | kernel | ospf | rip | static }	

42.2.13 Configure Route Filtering

Policies and rules can be configured to filter incoming and outgoing routes based on an address prefix list. In addition, you can configure that only the RIP packets from a specific neighboring Ethernet Switch can be received.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter RIP configuration mode	**router rip**	
Set distribute-list for inbound	**distribute-list** { ip-acl-name | ip-acl-number | prefix *prefix-list* } **in** [{ vlan-interface | supervlan-interfac } *vlan-id*]	
Delete distribute-list for inbound	**undo distribute-list** { ip-acl-name | ip-acl-number | prefix *prefix-list* } **in** [{ vlan-interface | supervlan-interfac } *vlan-id*]	
Set distribute-list for outband	**distribute-list** { ip-acl-name | ip-acl-number | prefix *prefix-list* } **out** [{ vlan-interface | supervlan-interfac } *vlan-id*]	

Delete distribute-list for outband	**undo distribute-list** { ip-acl-name | ip-acl-number | prefix *prefix-list* } **out** [{ vlan-interface | supervlan-interfac } *vlan-id*]	

42.2.14 Display RIP Configuration

Operation	Command	Remarks
Displays the RIP packet statistics information.	**display ip rip**	
Displays the RIP interface configuration, such as the version and authentication information.	**display ip rip interface**	
Displays RIP routing tables.	**display ip route rip**	

Chapter 43 OSPF

43.1 OSPF Overview

Open Shortest Path First (OSPF) is an interior routing protocol, which is developed by IETF based on the link state detection and shortest path first technologies. In an IP network, OSPF dynamically discovers and advertise routes by collecting and transmitting the link states of autonomous systems (ASs). It supports interface-based packet authentication for purposes of route calculation security and employs IP multicast to send and receive packets.

Each OSPF router maintains a database that describes the topological structure of an AS. The database is a collection of link-state advertisements (LSAs) of all the routers. Every router always broadcasts the local state information across the entire AS. If two or more routers exist in a multi-access network, a designated router (DR) and a backup designated router (BDR) must be elected. The DR is responsible for broadcasting the LSAs of the network. With a DR, a multi-address access network may require less neighbor relationships to be established between routers. OSPF allows an AS to be divided into areas, between which routing information is further abstracted. As a result, smaller network bandwidth will be occupied.

OSPF uses four types of routes, which are listed in order of priority as follows:

Intra-area routes

Inter-area routes

Type 1 external routes

Type 2 external routes

Intra-area and inter-area routes describe the network structure of an AS, while external routes depict how routes are distributed to destinations outside an AS. Generally, type 1 external routes are based on the information imported by OSPF from other interior routing protocols and comparable to OSPF routes in routing cost; type 2 external routes are based on the information imported by OSPF from exterior routing protocols and the costs of such routes are far greater than those of OSPF routes. Therefore, route calculation only takes the external costs into consideration.

Based on the link state database (LSDB), each router builds a shortest path tree with itself as the root, which presents the routes to every node in an AS. An external route emerges as a leaf node and can also be marked by the router that broadcasts the external route so that additional information about an AS is recorded.

All the OSPF areas are connected to the backbone area, which is identified by 0.0.0.0. OSPF areas must be logically continuous. To achieve this end, virtual connection is introduced to the backbone area to ensure the logical connectivity of areas even if they are physically separated.

All the routers in an area must accept the parameter settings of the area. Therefore, the configuration of routers in the same area must be performed in consideration of the parameter settings of the area. A configuration error may lead to the failure of information transfer between adjacent routers and even routing failures or routing loops.

43.2 Configure OSPF

43.2.1 OSPF Configuration List

Configuration Task	Description	Detailed Configuration
EnableOSPF	Required	43.2.2
ConfigureOSPF Parameter	Required	43.2.3
Configure OSPF Interface	Required	43.2.4
Configure OSPF Area	Required	43.2.5

43.2.2 Enable OSPF

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enters global configuration mode.	**router ospf**	
Enters global configuration mode.	**undo router ospf**	

43.2.3 Configure OSPF Parameter

OSPF divides an AS into different areas, based on which routers are logically classified into different groups. Area border routers (ABRs) may belong to different areas. A network segment belongs to only one area, that is, the homing area of an OSPF interface must be specified. An area is identified by an area ID. Routes between areas are transmitted by ABRs.

In addition, all the routers in an area must unanimously accept the parameter settings of the area. Therefore, the configuration of routers in the same area must be performed in

consideration of the parameter settings of the area. A configuration error may lead to the failure of information transfer between adjacent routers and even routing failures or routing loops.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enters global configuration mode.	**router ospf**	
Enters global configuration mode.	**router id** *router-id*	
Enters global configuration mode.	**undo router id**	
Runs the command in OSPF configuration mode.	**network** *ipaddress wildcard-mask* **area** *area-id*	
Runs the command in OSPF configuration mode.	**undo network** *ipaddress wildcard-mask* **area** *area-id*	
Configures the authentication type for an area.	**area** *area-id* **authentication** [message-digest]	
Restores the authentication type of an interface to no authentication.	**undo area** *area-id* **authentication**	

43.2.4 Configure OSPF Interface

OSPF calculates routes based on the topological structure of the network adjacent to the local router. Each router describes the topology of its adjacent network and transmits it to the other routers. According to the link layer protocol, OSPF classifies networks into the following four types:

Broadcast networks: When Ethernet or FDDI is used as the link layer protocol, OSPF considers that the network type is broadcast by default.

Non Broadcast MultiAccess (NBMA) networks: When ATM is used as the link layer protocol, OSPF considers that the network type is NBMA by default.

Point-to-Multipoint networks: This network type will be considered as default in no case. It is always a substitute of other network types through forcible change. An NBMA network that is not fully meshed is often changed to a point-to-multipoint network.

Point-to-Point networks: When PPP, LAPB, or POS is used as the link layer protocol, OSPF considers that the network type is Point-to-Point by default.

The ATM network is a typical NBMA network. A polling interval can be configured to specify the interval of sending Hello packets before a router establishes a neighbor relationship with its neighboring router.

On a broadcast network incapable of multi-address access, you can configure the interface type to nonbroadcast.

If some routers are not directly reachable on an NBMA network, you can configure the interface type to point-to-multipoint.

If a router has only one peer router on an NBMA network, you can set the interface type to point-to-point.

The differences between an NBMA network and a point-to-multipoint network are as follows:

In OSPF, an NBMA network refers to a non-broadcast multi-access network that is fully meshed. A point-to-multipoint network may not be fully meshed.

A DR and a BDR must be elected on an NBMA network but are not involved on a point-to-multipoint network.

NBMA is a default network type. For example, if the link layer protocol is ATM, OSPF considers that the network type is NBMA by default no matter whether the network is fully meshed. Point-to-multipoint is not a default network type. No link layer protocol is viewed as a point-to-multipoint protocol. You can use this network type through a forcible change. An NBMA network that is not fully meshed is often changed to a point-to-multipoint network.

On an NBMA network, packets are transmitted in unicast mode, which requires you to configure neighbor relationship manually. On a point-to-multipoint network, packets are transmitted in multicast mode.

An Ethernet Switch uses Ethernet as the link layer protocol, so OSPF regards that the network type is broadcast. Do not change the network type of an Ethernet Switch at discretion.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter the VLAN-interface or Supervlan-interface configuration mode	**interface** { vlan-interface | supervlan-interface } *vlan-id*	
Sets the network type of an	**ip ospf network** { broadcast | non-broadcast	

interface.	| point-to-multipoint | point-to-point }	
Restores the network type of an interface to the default value.	**undo ip ospf network**	
Sets the cost of sending packets through a VLAN interface.	**ip ospf cost** *cost*	
Restores the packet sending cost of a VLAN interface to the default value.	**undo ip ospf cost**	
Sets the priority of an interface in DR election.	**ip ospf priority** *value*	
Restores the default priority of an interface.	**undo ip ospf priority**	
Sets the interval of sending Hello packets for an interface.	**ip ospf hello-interval** *seconds*	
Restores the interval of sending Hello packets for an interface to the default value.	**undo ip ospf hello-interval**	
Sets the timeout time of the neighboring router.	**ip ospf dead-interval** *seconds*	
Restores the timeout time of the neighboring router to the default	**undo ip ospf dead-interval**	

value.		
Sets the interval of LSA retransmission between two adjacent routers.	**ip ospf retransmit-interval** *seconds*	
Restores the interval of LSA retransmission between two adjacent routers to the default value.	**undo ip ospf retransmit-interval**	
Sets the time for sending a link state update packet.	**ip ospf transmit-delay** *seconds*	
Restores the time for sending a link state update packet to the default value.	**undo ip ospf transmit-delay**	
Sets the authentication type	**ip ospf authentication** [null | *ipaddress* | message-digest [*ipaddress*]]	
Restores the authentication type	**undo ip ospf authentication** [*ipaddress*]	
Sets a password for plaintext authentication.	**ip ospf authentication-key** *password* [*ipaddress*]	
Disables plaintext authentication.	**undo ip ospf authentication-key** [*ipaddress*]	
Sets a password for MD5	**ip ospf message-digest-key** *key-id* **md5**	

authentication.	*key* [*ipaddress*]	
Disables MD5 authentication.	**undo ip ospf message-digest-key** *key-id* [*ipaddress*]	

43.2.5 Configure OSPF Area

A stub area is a special LSA area in which ABRs do not distribute the external routes they have received. In stub areas, both the size of routing tables and the amount of the routing information are drastically reduced.

Any area that meets certain conditions can be configured into a stub area. Generally, a stub area is located at the border of an AS. It may be a non-backbone area with only one ABR or a non-backbone area with multiple ABRs between which no virtual connection is configured.

To make a stub area reachable for other ASs, the ABR in the stub area generates a default route (0.0.0.0) and advertises it to non-ABR routers in this area.

When Configure a stub area, note the following points:

-A backbone area cannot be a stub area and a virtual connection is not allowed in a stub area.

-All the routers in a stub area must be configured to indicate that they are located in a stub area.

-No ASBR is allowed in a stub area, that is, routes from outside the AS where the stub area resides cannot be advertised within the stub area.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enters global configuration mode.	**router ospf**	
Configures a stub area.	**area** *area-id* **stub** [no-summary]	
Cancels the stub area configuration.	**undo area** *area-id* **stub** [no-summary]	
Configures the cost of the default route to a stub area.	**area** *area-id* **default-cost** *cost*	
Cancels the cost configuration for the default route to a stub area.	**undo area** *area-id* **default-cost**	
Configures an NSSA area.	**area** *area-id* **nssa** [no-summary]	
Cancels the NSSA area configuration.	**undo area** *area-id* **nssa** [no-summary]	
Configures the cost of the default route to an NSSA area.	**area** *area-id* **default-cost** *cost*	
Cancels the cost configuration for the default route to an NSSA area.	**undo area** *area-id* **default-cost**	
Configures route aggregation in an OSPF area.	**area** *area-id* **range** *ip-address/mask-length* [advertise | notadvertise] [substitute *p-address/mask-length*]	
Removes route aggregation in an OSPF area.	**undo area** *area-id* **range** *ip-address/mask-length* [substitute *p-address/mask-length*]	

Creates and configures a virtual connection.	**area** *area-id* **virtual-link** *router-id* [{ hello-interval *seconds* | retransmit- interval *seconds* | transmit-delay *seconds* | dead-interval *seconds* | { authentication-key *password* | message-digest-key *keyid* md5 *key* } } *]	
Cancels a virtual connection.	**undo area** *area-id* **virtual-link** *router-id*	
Imports routes of other protocols into OSPF.	**redistribute** { babel |bgp | connected | isis | kernel | rip | static } [metric *metric-value*] [metric-type { 1 | 2 }] [route-map *map-name*]	
Disables the import of routes of other protocols into OSPF.	**undo redistribute** { babel |bgp | connected | isis | kernel | rip |static } [metric *metric*] [metric-type { 1 | 2 }] [route-map *map-name*]	
Imports the default route to OSPF.	**default-information originate** [always] [metric *metric-value*] [metric-type { 1 | 2 }] [route-map *map-name*]	
Disables the import of the default route.	**undo default-information originate** [always] [metric *metric-value*] [metric-type { 1 | 2 }] [route-map *map-name*]	

Configures a default metric value for reception of external routes.	**default-metric** *metric-value*	
Cancels the default metric value configuration for reception of external routes.	**undo default-metric**	
Configures distribute-list	**distribute-list** { *ip-acl-name* | *ip-acl-number* } **out** { babel | bgp | connected | isis | kernel | rip | static }	
Delete distribute-list	**undo distribute-list** { *ip-acl-name* | *ip-acl-number* } **out** { babel | bgp | connected | isis | kernel | rip | static }	
Enter the VLAN-interface or Supervlan-interface configuration mode	**interface** { vlan-interface | supervlan-interface } *vlan-id*	
Enables BFD for link state monitoring.	**ip ospf bfd**	
Disables BFD.	**undo ip ospf bfd**	

Chapter 44 BGP

44.1 BGP Overview

Border Gateway Protocol (BGP) is a dynamic routing protocol deployed between autonomous systems (ASs). It automatically exchanges loop-free routing information between ASs and builds up the topological structure of ASs through exchange of network reachability information with the AS Path attribute.

BGP normative references include RFC1105 (BGP-1), RFC1163 (BGP-2), RFC1267 (BGP-3), RFC1771 (BGP-4), and RFC4271 (BGP-4). RFC1771 has seen the widest application and RFC4271 is the latest issue. BGP is suitable for a distributed network and supports Classless InterDomain Routing (CIDR). With BGP, users can customize policies. BGP-4 is becoming a matter-of-factor standard for Internet exterior routing protocols. BGP is usually deployed between ISPs.

BGP has the following features:

Interior routing protocols such as OSPF and RIP are designed to discover and calculate routes. As an exterior routing protocol, BGP focuses on control of route distribution and selection of the best route.

The AS Path attribute is added to BGP routes to eliminate the routing loop problem.

With TCP as the transport layer protocol, BGP presents better protocol reliability.

Support for CIDR is a significant characteristic of BGP-4 compared with BGP-3. The CIDR technology does not categorized IP addresses into class A, class B, and class C IP addresses. For example, 192.168.0.0 (2555.255.0.0) is naturally an invalid class C IP address. This IP address, however, is expressed as 192.168.0.0/16 in CIDR and becomes a valid network address. /16 indicates that the subnet mask is composed of the first 16 bits counted from the left of the IP address. CIDR also simplifies route aggregation, which is a process of consolidating several different routes. With the route aggregation technology, multiple routes are advertised as one route, which reduces the overhead of BGP tables and network bandwidth usage.

In the case of route updates, BGP transmits only incremental routes and substantially reduces the bandwidth used by BGP route transmission. Therefore, BGP is appropriate when a large number of routes need to be transmitted on Internet.

In consideration of management and security, each AS expects to control its incoming and outgoing routes. BGP-4 provides abundant routing policies for flexible route filtering and selection. In addition, BGP-4 is easy to expand and conducive to network development.

BGP runs on a specific router as an upper-layer protocol. Upon startup of BGP, the BGP router sends the entire BPG table to its peer for routing information exchange and then only Update messages are exchanged between them for processing of changed routes. BGP detects the connection between routers by sending and receiving Keepalive messages.

The router sending a BGP message is called the BGP speaker, which constantly receives or generates new routing information and advertises it to other BGP speakers. After receiving a

new route advertisement from another AS, the BGP speaker distributes the route advertisement to all the other BGP speakers in the same AS if the route is better than the current one or has not been received ever. If two BGP speakers are exchanging messages, they call each other the peer.

BGP runs on a router in either of the following modes:

Internal BGP (IBGP)

External BGP (EBGP)

BGP is regarded as IBGP when deployed within an AS and as EBGP when deployed between ASs.

BGP running is driven by messages, which are classified as follows:

Open message

Update message

Notification message

Keepalive message

An Open message is the first message to be sent after setup of a TCP connection and used to establish a BGP peer relationship. A Notification message is sent when there is an error. A Keepalive message is sent to detect the validity of a connection. As the most important message in BGP, an Update message is transmitted between BGP peers for routing information exchange. It consists of three parts at most: unreachable route, path attributes,

and Network Layer Reachability Information (NLRI).

44.2 Configure BGP

44.2.1 BGP Configuration List

Configuration Task	Description	Detailed Configuration
Enable BGP	Required	44.2.2
ConfigureBGP peers	Required	44.2.3
Configure BGP Parameters	Required	44.2.4
Monitoring and Maintain BGP	Required	44.2.5

44.2.2 Enable BGP

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Runs the command in global configuration mode.	**router bgp** *as-number*	
Runs the command in global configuration mode.	**undo router bgp** *as-number*	
Configures the local route to be advertised by BGP.	**network** *ip-address* [mask *address-mask*]	
Cancels the local route to be advertised by BGP.	**undo network** *ip-address* [mask *address-mask*]	

Establishes a neighbor relationship and sets the AS number of the peer.	**neighbor** *neighbor-name* **peer-group**	
Cancels neighbor relationship	**undo neighbor** *neighbor-name* **peer-group**	

44.2.3 Configure BGP Peers

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Runs the command in global configuration mode.	**router bgp** *as-number*	
Establishes a neighbor relationship and sets the AS number of the peer.	**neighbor** { *neighbor-address* | *neighbor-name* } **remote-as** *as-number*	
Deletes the established neighbor relationship.	**undo neighbor** { *neighbor-address* | *neighbor-name* } **remote-as**	
Configures peer-group member	**neighbor** *neighbor-address* **peer-group** *neighbor-name*	
Delete peer-group member	**undo neighbor** *neighbor-address* **peer-group** *neighbor-name*	
Configures that a connection can be established with an EBGP peer on an indirectly-connected	**neighbor** { *neighbor-address* | *neighbor-name* } **ebgp-multihop** [*ttl*]	

network.		
Configures that a connection can be established only with an EBGP peer on a directly-connected network.	**undo neighbor** { *neighbor-address* | *neighbor-name* } **ebgp-multihop**	
Configures the Keepalive interval and hold timer of a BGP peer.	**neighbor** { *neighbor-address* | *neighbor-name* } **timers** *keepalive-interval hold-time*	
Restores the Keepalive interval and hold timer of a BGP peer to the default values.	**undo neighbor** { *neighbor-address* | *neighbor-name* } **timers**	
Configures the interval a BGP peer waits before sending a route update message.	**neighbor** { *neighbor-address* | *neighbor-name* } **advertisement-interval** *seconds*	
Restores the interval a BGP peer waits before sending a route update message to the default value.	**undo neighbor** { *neighbor-address* | *neighbor-name* } **advertisement-interval**	
Configures that its own address is used as the next hop during route advertisement.	**neighbor** { *neighbor-address* | *neighbor-name* } **next-hop-self**	
Cancels the configuration that its	**undo neighbor** { *neighbor-address* |	

own address is used as the next hop during route advertisement.	*neighbor-name* } **next-hop-self**	
Configures an IP ACL-based route filtering policy for the peer.	**neighbor** { *neighbor-address* | *neighbor-name* } **distribute-list** { ip-acl-name | ip-acl-number } { in | out }	
Deletes an IP ACL-based route filtering policy of the peer.	**undo neighbor** { *neighbor-address* | *neighbor-name* } **distribute-list** { ip-acl-name | ip-acl-number } { in | out }	
Configures an AS Path-based route filtering policy for the peer.	**neighbor** { *neighbor-address* | *neighbor-name* } **filter-list** *aspath-list-number* { in | out }	
Deletes an AS Path-based route filtering policy for the peer.	**undo neighbor** { *neighbor-address* | *neighbor-name* } **filter-list** *aspath-list-number* { in | out }	
Configures an IP-Prefix list route filtering policy for the peer.	**neighbor** { *neighbor-address* | *neighbor-name* } **prefix-list** *list-name* { in | out }	
Deletes an IP-Prefix list route filtering policy for the peer.	**undo neighbor** { *neighbor-address* | *neighbor-name* } **prefix-list** *list-name* { in | out }	

44.2.4 Configure BGP Parameters

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Runs the command in global configuration mode.	**router bgp** *as-number*	
Runs the command in BGP configuration mode.	**timers bgp** *keepalive-interval hold-time*	
Restores the default value of the timer.	**undo timers bgp**	
Disable sending connection request packet	**neighbor** { *neighbor-address* | *neighbor-name* } **passive**	
Enable sending connection request packet	**undo neighbor** { *neighbor-address* | *neighbor-name* } **passive**	
Shutdown the neighbor connection	**neighbor** { *neighbor-address* | *neighbor-name* } **shutdown**	
Open the neighbor connection	**undo neighbor** { *neighbor-address* | *neighbor-name* } **shutdown**	
Configures a local priority.	**bgp default local-preference** vlaue	
Restores the default local priority.	**undo bgp default local-preference**	
Compares the MED values of neighbors from different ASs.	**bgp always-compare-med**	
Compares the MED values of neighbors from different ASs.	**undo bgp always-compare-med**	

Configures local route aggregation.	**aggregate-address** { *ip-address mask* | *ip-address/mask-length* } [summary-only] [as-set]	
Disables local route aggregation.	**undo aggregate-address** { *ip-address mask* | *ip-address/mask-length* }	
Imports IGP routes into BGP.	**redistribute** { babel | connected | isis | kernel | ospf | rip | static } [**metric** *metric* [**route-map** *route-map*]]	
Cancels the import of IGP routes into BGP.	**undo redistribute** { babel | | connected | isis | kernel | ospf | rip | static }	

44.2.5 Monitoring and Maintain BGP

Operation	Command	Remarks
Displays the detailed information of BGP peers.	**display ip bgp neighbors** *neighbor-address* [vpn-instance *instance*]	
Displays the brief information of BGP peers.	**display ip bgp summary** [vpn-instance *instance*]	

Chapter 45 BFD

45.1 BFD Overview

Bidirectional Forwarding Detection (BFD) periodically checks the status of the peers of a session and notifies a routing protocol of a fault if any immediately. Then the routing protocol responds with a fast reroute action. Generally, the BFD interval is shorter than 1s and therefore the convergence time of routing protocols is reduced. For this reason, BFD can help routing protocols such as OSPF, RIP, and BGP to detect the reachability of neighbors or link failures, which realizes fast reroute and ensures link reliability.

45.2 Configure BFD

45.2.1 BFD Configuration List

Configuration Task	Description	Detailed Configuration
Enable BFD	Required	45.2.2
Configure BFD Parameters and Mode	Optional	45.2.3
Display and Maintain BFD Configurations	Optional	45.2.4

45.2.2 Enable BFD

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	

Enable bfd function	**bfd enable**	
Disable bfd function	**bfd disable**	
Enter the VLAN-interface or Supervlan-interface configuration mode	**interface** { vlan-interface | supervlan-interface } *vlan-id*	
Enable bfd function	**ip ospf bfd**	
Disable bfd function	**undo ip ospf bfd**	OSPF BFD is disabled by default. Currently, only OSPF BFD is supported.

45.2.3 Configure BFD Parameters and Mode

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter the VLAN-interface or Supervlan-interface configuration mode	**interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configures the desired minimum transmission interval of BFD.	**bfd min-transmit-interval** *interval*	
Restores the desired minimum	**undo bfd min-transmit-interval**	The default value

transmission interval of BFD to the default value.		is 400 ms.
Configures the minimum request receiving interval of BFD.	**bfd min-receive-interval** *interval*	
Restores the minimum request receiving interval of BFD to the default value.	**undo bfd min-receive-interval**	The default value is 400 ms.
Configures the BFD multiplier.	**bfd detect-multiplier** *value*	
Restores the BFD multiplier to the default value.	**undo bfd detect-multiplier**	
Configures whether BFD sessions can enter the demand mode.	**bfd demand on**	
Restores the configuration of whether BFD sessions can enter the demand mode to the default value.	**bfd demand off**	The default value is off (not allowed).
Configures the initial mode of BFD sessions.	**bfd session init-mode active**	The default value is active.
Restores the initial mode of BFD sessions to the default value.	**bfd session init-mode passive**	
Clears the statistics of the sent and received packets in BFD sessions	**clear bfd session statistics**	

through an interface.		

Notes:

value: desired minimum packet transmission interval of an interface. It ranges from 200 to 1000 ms and is 400 ms by default.

Packet transmission interval = max(Desired minimum transmission interval, Minimum receiving interval) x a percentage (from 70% to 90%)

45.2.4 Display and Maintain BFD Configurations

Operation	Command	Remarks
Views the information of all the BFD sessions.	**display bfd session** [verbose]	
Views the BFD configuration of each interface.	**display bfd interface** [verbose]	

Chapter 46 VRRP

46.1 VRRP Overview

On a TCP/IP network, routes must be configured between two devices without a physical connection to ensure their communication. Currently, routes can be specified through dynamic learning by means of a routing protocol (such as RIP and OSPF) or static configuration. It is impractical to run a dynamic routing protocol on every terminal. Most client operating systems do not support the dynamic routing and they are still under the restraint of management overhead, convergence degree, and security even if they can be configured with a routing protocol. Usually, static routes are configured for IP terminals by specifying one or more default gateways. Static routing simplifies network management and reduces the communication overhead of terminals. However, if a Switch functioning as a default gateway is damaged, the communication in which the Switch is used as the next-hop host will inevitably be interrupted. A terminal will not be Switched to a new gateway even if there are multiple default gateways until it is restarted. Virtual Router Redundancy Protocol (VRRP) can rectify the defect of static routing.

VRRP introduces two pairs of concepts: VRRP Switch and virtual Switch, master Switch and backup Switch. A VRRP Switch is a real Switch where VRRP runs, while a virtual Switch is a logical Switch created by VRRP. A group of VRRP Switches form a virtual Switch, which is also called a backup group. The virtual Switch is represented as a logical Switch with a unique

IP address and MAC address. Switches in a VRRP group are classified into master Switches and backup Switches. A VRRP group has only one master Switch and one or more backup Switches. VRRP selects a master Switch from the Switch group. The master Switch responds to ARP requests and forwards IP packets, and the other Switches are standby as a backup. If the master Switch is faulty due to some reason, a backup Switch will become the master one within several seconds. Such a Switchover is completed very quickly without requiring you to change the IP address or MAC address, and therefore it is transparent to terminal users.

46.2 Configure VRRP

46.2.1 VRRP Configuration List

Configuration Task	Description	Detailed Configuration
Enable VRRP	Required	46.2.2
Configure VRRP Parameters	Optional	46.2.3
Displays and Maintain VRRP Configurations	Optional	46.2.4

46.2.2 Enable VRRP

The ip vrrp vrid vip command is used to assign a virtual Switch (or a backup group) an IP address on the local network segment. The no form of this command is used to remove the virtual IP address of a backup group from the virtual IP address list.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	

Enter the VLAN-interface or Supervlan-interface configuration mode	**interface** { vlan-interface | supervlan-interface } *vlan-id*	
Configures VRRP virtual IP address	**ip vrrp** *vridvip*	
Deletes VRRP virtual IP address	**undo ip vrrp** *vrid* [*vip*]	

Description:

The backup group number ranges from 1 to 255. A virtual address can be an unassigned IP address on the network segment where the backup group resides or the IP address of an interface belonging to the backup group. A maximum of 255 backup groups can be configured. The IP address of the Switch itself can be configured. In this case, the Switch is known as an IP address owner. When the first IP address is assigned to a backup group, VRRP creates the backup group. Other virtual IP addresses configured for the backup group will only be added to the virtual IP address list of the backup group. A backup group can be configured with eight IP addresses at most. A backup group will be deleted together with the last virtual IP address. That is, this backup group does not exist on the interface and all configurations of the backup group will no longer take effect.

46.2.3 Configure VRRP Parameters

The master Switch in a backup group will not be replaced unless it is faulty even if another Switch is configured with a higher priority later. However, if the preemption mechanism is applied, a Switch will become the master Switch if its priority is higher than that of the master

Switch and the original master Switch will become a backup Switch accordingly. When preemption is enabled, you can set the delay of preemption. Then a backup Switch becomes master after the delay. A backup Switch will become the master Switch if it does not receive a packet from the original master Switch. However, if a network has unstable performance, a backup Switch may not receive a packet due to network congestion but the master Switch is still working properly. In this situation, the backup Switch will receive a packet from the master Switch after waiting a short time. As a result, frequent Switchovers can be avoided. The delay ranges from 0 to 255 seconds.

The master Switch sends VRRP packets within the VRRP backup group at an interval specified by adver_interval to indicate that it is working properly. If the backup Switch does not receive a VRRP packet from the master Switch within a period of time specified by master_down_interval, it regards that the master Switch is faulty and changes its state to Master.

You can modify the value of adver_interval by running a timer setting command. The value of master_down_interval is three times that of adver_interval. An abnormal Switchover may occur in the event of extremely large traffic or variance in timer settings between Switches. To solve this problem, you can set adver_interval to a greater value or modify the preemption delay. The value of adver_interval is in the unit of second.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter the VLAN-interface or	**interface** { vlan-interface |	

Supervlan-interface configuration mode	supervlan-interface } *vlan-id*	
Configures VRRP priority	**vrrp priority** *vridpriority*	The priority ranges from 0 to 255. A larger value indicates a higher priority.
Restores the VRRP priority r to the default value.	**undo vrrp priority** *vrid*	By default,it is 100
Configures VRRP preempt mode	**vrrp preempt** *vrid*	
Restores the preempt mode to the default value.	**undo vrrp preempt** *vrid*	By default, preempt is disabled
Configures VRRP preempt delay time	**vrrp preempt** *vrid* [**delay** *delay*]	
Restores the delay time to the default value.	**undo vrrp preempt** *vrid*	By default, it is 0 second
Configures VRRP advertise interval time	**vrrp timer** *vrid adver-interval*	
Restores the advertise interval to the default value.	**undo vrrp timer** *vrid*	By default, it is 1 second

Configures VRRP track function	**vrrp track** *vrid* { vlan-if | supervlan-if } *vlan-id* [reduced *priority*]	By default, it is disabled
Deletes VRRP track function	**undo vrrp track** *vrid* { all | vlan-if | supervlan-if }	

Note: The priority of the IP address owner cannot be changed and is always 255.

Parameter description:

vrid: virtual group ID, in the range of 1 to 255;

vlan-id: ID of the VLAN to which a VLAN interface belongs;

supervlan-id: ID of the super VLAN to which a superVLAN interface belongs;

pri-value: priority to be reduced if the interface under monitoring is down.

46.2.4 Displays and Maintain VRRP Configurations

Operation	Command	Remarks
Runs the command in any mode.	**display vrrp** [vlan-interface | supervlan-interface *vlan-id* [*vrid*]	

Chapter 47 DLF-Control

47.1 DLF-Control Overview

Unknown packets are classified into unknown unicast packets and unknown multicast packets.

Unknown unicast packets are packets that cannot find the destination MAC addresses in the MAC table.

Unknown multicast packets are packets that cannot find the destination MAC addresses of the multicast packets in the multicast MAC table.

47.2 Configure DLF-Control

47.2.1 DLF-Control Configuration List

Configuration Task	Description	Detailed Configuration
Configure DLF-forward unicast	Required	47.2.2
Configure DLF-forward unicast	Optional	47.2.3
Displays and Maintain DLF-forward Configurations	Optional	47.2.4

47.2.2 Configure DLF-forward unicast

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	

Enable dlf-forward unicast	**dlf-forward unicast**	Enabled by default.
Disable dlf-forward unicast	**undo dlf-forward unicast**	

47.2.1 Configure DLF-forward multicast

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enable dlf-forward multicast	**dlf-forward multicast**	Enabled by default.
Disable dlf-forward multicast	**undo dlf-forward multicast**	

47.2.2 Displays and Maintain DLF-forward Configurations

Operation	Command	Remarks
Displays theunicast dlf-forward control	**display dlf-forward interface** [ethernet *interface-num*]	
Displays themulticastdlf-forward control	**display dlf-forward global**	

Chapter 48 SLF-Control

48.1 SLF-Control Overview

Whether the Switch forwards the packet with an unknown source MAC address requires the network administrator to plan according to the security policy. The Switch defaults to forward the packet with an unknown source MAC address. You can disable the forwarding function of packet with an unknown source MAC address by setting the commands. After disable this function, if the device receives the packets, it will check whether the source mac exists in the mac table. If it does not exist, the packets will be discarded, that is, the Switch only forwards the packet with the source MAC address being known.

48.2 Configure SLF-Control

48.2.1 SLF-Control Configuration List

Configuration Task	Description	Detailed Configuration
Configure SLF-forward unicast	Required	48.2.2
Displays and Maintain SLF-forward Configurations	Optional	48.2.3

48.2.2 Configure SLF-forward unicast

Generally, this function is used when the MAC address learning function is disabled or MAC address limit function is disabled.

Operation	Command	Remarks
Enter the global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-numt*	
Enable Slf-forward	**slf-forward**	
Disable Slf-forward	**undo slf-forward**	Disabled by default.

48.2.3 Displays and Maintain SLF-forward Configurations

Operation	Command	Remarks
Displays the slf-forward control	**display slf-forward interface** [ethernet *interface-num*]	

Chapter 49 BPDU-Discard

49.1 BPDU-Discard Overview

The Discard-bpdu function is used to drop spanning tree message. If the device does not want to receive BPDU message from other networks and cause the Switch spanning tree to vibrate. This function can be opened.

This function is usually enabled on the edge port.

The Discard-BPDU function is disabled by default. Global configuration and port configuration are mutually exclusive: globally, all ports are enabled. If you only need to enable certain designated ports and other ports are not enabled, you need not configure them globally to directly enter the specified port enabling function.

49.2 Configure BPDU-Discard

49.2.1 BPDU-Discard Configuration List

Configuration Task	Description	Detailed Configuration
Configure BPDU-Discard	Required	49.2.2
Displays and Maintain BPDU-Discard Configurations	Optional	49.2.3

49.2.2 Configure BPDU-Discard

Operation	Command	Remarks

Enter the global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Enable BPDU-Discard	**bpdu-discard**	
Disable BPDU-Discard	**undo bpdu-discard**	Disabled by default.

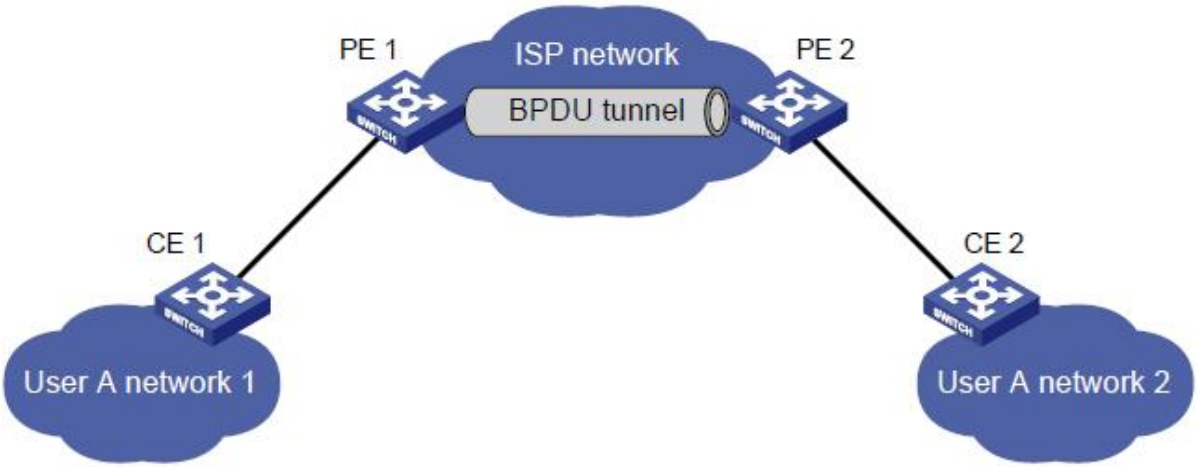
49.2.3 Displays and Maintain BPDU-Discard Configurations

Operation	Command	Remarks
Displays the BPDU-Discard configuration	**display bpdu-discard interface** [ethernet *interface-num*]	

Chapter 50 BPDU-Tunnel

50.1 BPDU-Tunnel Overview

L2TP (Layer 2 Tunneling Protocol) is a Layer 2 tunneling technology, L2TP enables Layer 2 protocol packets from geographically dispersed customer networks to be transparently transmitted over specific tunnels across a service provider network.



With L2TP, Layer 2 protocol packets from customer networks can be transparently transmitted in the service provider network:

1. After receiving a Layer 2 protocol packet from User A network 1, PE 1 in the service provider network encapsulates the packet, replaces its destination MAC address with a specific multicast MAC address, and then forwards the packet in the service provider network.

2. The encapsulated Layer 2 protocol packet (called bridge protocol data unit, BPDU for short) is forwarded to PE 2 at the other end of the service provider network, which de-encapsulates the packet, restores the original destination MAC address of the packet, and then sends the packet to User A network 2.

50.2 Configure BPDU-Tunnel

50.2.1 BPDU-tunnel Configuration List

Configuration Task	Description	Detailed Configuration
Configure BPDU-Tunnel Packet	Required	50.2.2
Configure BPDU-TunnelDestination MAC	Optional	50.2.3
Displays and Maintain BPDU-Tunnelconfiguration	Optional	50.2.4

50.2.2 Configure BPDU-Tunnel Packet

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Configure the L2-tunnel packet	**bpdu-tunnel** [cdp | lacp | pagp | stp | udld | vtp]	

50.2.3 Configure BPDU-Tunnel Destination MAC

By default, L2TP destination mac is 01:00:0c:cd:cd:d0

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Configure the rate for up to cpu	**bpdu-tunnel dmac** *mac-address*	

50.2.4 Displays and Maintain BPDU-Tunnel Configuration

After finishing above configuration, user can check the configurations by command below.

Operation	Command	Remarks
Display L2TP configuration	**display bpdu-tunnel interface** [ethernet *interface-num*]	

Chapter 51 Local-Switch

51.1 Local-Switch Overview

Normally, packets coming from port A are not forwarded from port A by the Switch. However, it may require packets coming from the A port are forwarded from the A port sometimes. In this case, you can use the local-Switch.

51.2 Configure Local-Switch

51.2.1 Local-switch Configuration List

Configuration Task	Description	Detailed Configuration
Enable local-switch	Required	51.2.2
Displays and Maintain local-switch Configurations	Optional	51.2.3

51.2.2 Enable local-switch

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter interface configuration mode	**interface ethernet** *interface-num*	
Enable local-switch	**local-switch**	
Disable local-switch	**undo local-switch**	Disabled by default.

51.2.3 Displays and Maintain Local-switch Configurations

Operation	Command	Remarks
Displays the local-switch control	**display local-switch interface** [ethernet *interface-num*]	

Chapter 52 Port&CPU Utilization Alarm

52.1 Port&CPU Utilization Alarm Overview

The device utilization alarm is used to monitor port bandwidth, CPU occupation and alarm when congestion in order to administrator aware the running status between the network and device.

Exceed: when port bandwidth utilization over “exceed”, it triggers congestion alarm.

Normal: when port bandwidth utilization less “exceed”, it triggers recover alarm CPU utilization alarm also can set two trigger values, details as below:

Busy: when CPU utilization over “busy”, it triggers alarm of CPU busyness

Unbusy: when CPU utilization less “busy”, it triggers alarm of CPU idle Notes, all alarms will show in the list of Syslog..

52.2 Configure Port&CPU Utilization Alarm

52.2.1 Port & CPU Utilization Alarm Configuration List

Configuration Task	Description	Detailed Configuration
Configure Port Utilization Alarm	Required	52.2.2

Configure CPU Utilization Alarm	Required	52.2.3
Display and Debugging Device Utilization Alarm	Optional	52.2.4

52.2.2 Configure Port Utilization Alarm

Using below commands to configure port utilization. Enable port utilization in system and port mode by default. The “exceed” value equals 850M, the “normal” value equals 600M.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable(disable)port utilization alarm with system mode	[**undo**] **alarm all-packets**	
Enter port configuration	**interface ethernet** *interface-num*	
Enable(disable)port utilization alarm with port mode	[**undo**] **alarm all-packets**	
Configure alarm value	**alarm all-packets threshold** { **exceed** *thresold* | **normal** *thresold* }	

52.2.3 Configure CPU Utilization Alarm

Using below commands to configure CPU utilization. Enable CPU utilization by default. The “busy” value equals 90%, the “unbusy” value equals 60%.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable(disable) CPU utilization alarm	[**undo**] **alarm cpu**	

Configure congestion value	**alarm cpu threshold** { **busy** *thresold* | **unbusy** *thresold* }	

52.2.4 Display and Debugging Device Utilization Alarm

After finishing above configuration, you can show configuration by below commands.

Operation	Command	Remarks
Display the enable status and alarm value of CPU utilization alarm	**display alarm cpu**	
Display port utilization in system mode	**display alarm all-packets**	
Display port utilization and value in port mode	**display alarm all-packets interface** [**ethernet** *interface-num*]	