GPON OLT

CLI User Manual

Version: 1.0

Date: 2024-07-16

www.wireless-tek.com

Content

Chapter 1 Access OLT devices 24

1.1 command-line interface 24

1.1.1 Command line view 25

1.1.2 Understanding command syntax 27

1.1.3 Command Syntax Help 28

1.1.4 Symbols in the command 30

1.1.5 Command Parameter Type 30

1.1.6 Historical Command Recording Function 31

1.1.7 Command line error messages 31

1.1.8 Command Line Editing Functions 31

1.2 user management 32

1.2.1 System default user account 32

1.2.2 Add user account 32

1.2.3 Change user password 33

1.2.4 Modify user privileges 33

1.2.5 Delete user account 34

1.2.6 Viewing User Account Configuration 34

1.2.7 View online user information 34

1.2.8 Kicking online telnet users 34

1.3 Managing the OLT Pathway 35

1.3.1 Manage OLTs via serial port 35

1.3.2 OLT management via Telnet 36

1.3.3 OLT management via WEB 36

1.3.4 Managing OLTs via SNMP 36

1.4 Remote authentication of administrative users 37

1.4.1 Enabling RADIUS/TACACS+ Remote Authentication 37

1.4.2 Show Authentication Method Configuration 37

1.4.3 TACACS+ Remote Server Configuration 37

1.4.4 Display TACACS+ configuration 37

Chapter 2 OLT management and maintenance 39

2.1 System maintenance 39

2.1.1 View system status information 39

2.1.2 Setting the System Clock 40

2.1.3 Setting the system host name 40

2.1.4 Network Connection Ping Test Command 40

2.1.5 Route Trace Tracert Test Command 41

2.1.6 Port Loopback Test Command 41

2.1.7 Line Detection VCT Command 42

2.1.8 Managing IP address restrictions 43
2.1.9 Login Privileged User View Telnet User Count Limitation 43
2.1.10 CPU-CAR Commands 44
2.2 Configuration file management 44
2.2.1 Edit Configuration File 44
2.2.2 Modifying and saving the current configuration 44
2.2.3 Erase Configuration 45
2.2.4 Executing a Saved Configuration 45
2.2.5 Displaying Saved Configurations 45
2.2.6 Display the current running configuration 46
2.3 Load the upgrade program online 46
2.3.1 Uploading and downloading files via TFTP 46
2.3.2 Upload and download files via FTP 47
2.3.3 Downloading files via Xmodem 48
2.4 Reboot device 48
2.5 Telnet Client Features 49
Chapter 3 Port Configuration 50
3.1 Port Profile 50
3.2 Port Configuration 50
3.2.1 Port Related Configuration Task List 50
3.2.2 Enter port view 50
3.2.3 Enter the port group view 51
3.2.4 Open or close the specified port 51
3.2.5 Configuring Ethernet Port Duplex Mode and Speed 51
3.2.6 Configuring Port Priority 52
3.2.7 Configuring Port Descriptions 52
3.2.8 Enable or disable VLAN incoming packet filtering on the port 52
3.2.9 Configure the port's receive frame type 53
3.2.10 Enable or disable flow control for ports 53
3.2.11 Configure the port type 54
3.2.12 Configure the port's default VLAN ID 54
3.2.13 Add the port to the specified VLAN 55
3.2.14 Displaying port information 55
3.2.15 Display and clear port statistics 56
Chapter 4 port mirroring 58
4.1 Introduction to Port Mirroring 58
4.2 Port Mirroring Configuration 58
4.2.1 Port Mirroring Configuration Task List 58
4.2.2 Configuring the Mirror Destination Port 58

4.2.3 Configuring the Mirror Source Port 58
4.2.4 Show port mirroring 59
Chapter 5 port aggregation 60
5.1 Introduction to Port Aggregation 60
5.2 Port Aggregation Configuration 60
5.2.1 Port Aggregation Configuration Task List 60
5.2.2 Configure/delete aggregation groups 60
5.2.3 Adding/deleting convergence group members 61
5.2.4 Configuring an Aggregation Group Load Balancing Policy 61
5.2.5 Configure the LACP priority of the system 61
5.2.6 Display LACP configuration information 62
5.2.7 Clearing Aggregation Group Statistics 62
Chapter 6 Port isolation 64
6.1 Introduction to Port Isolation 64
6.2 Port Isolation Configuration 64
6.2.1 Port Isolation Configuration Task List 64
6.2.2 Add/remove uplink ports 64
6.2.3 Display Port Isolation Configuration 64
Chapter 7 Port Storm Suppression 65
7.1 Introduction to Port Storm Suppression 65
7.2 Port Storm Suppression Configuration 65
7.2.1 Port Storm Suppression Configuration Task List 65
7.2.2 Configure/remove port storm suppression 65
7.2.3 Show Port Storm Suppression Configuration 66
Chapter 8 VLAN Configuration 67
8.1 Introduction to VLANs 67
8.1.1 VLAN Overview 67
8.1.2 VLAN Benefits 68
8.1.3 VLAN Principle 68
8.1.4 VLAN Layer 3 interface 70
8.1.5 VLAN Type 70
8.2 Port-based VLAN Configuration 70
8.2.1 Port-based VLAN Configuration Task List 70
8.2.2 Create/Delete VLANs 70
8.2.3 Add/remove VLAN ports 71
8.2.4 Specify/delete VLAN descriptors 73
8.2.5 Configure the port type 74
8.2.6 Configure the port default VLAN ID 76
8.2.7 Configuring Hybrid Port Tag vlan 76

8.2.8 Display VLAN information 76
8.3 MAC-based VLAN Configuration 77
8.3.1 Introduction to MAC-based VLANs 77
8.3.2 MAC-based VLAN Configuration Task List 77
8.3.3 Create/delete MAC-based VLAN table entries 77
8.3.4 Display MAC-based VLAN table entries 78
8.4 Protocol-based VLAN Configuration 78
8.4.1 Introduction to protocol-based VLANs 78
8.4.2 Protocol-based VLAN Table Entry Configuration List 78
8.4.3 Create/delete VLANs based on protocol 78
8.4.4 Display protocol-based VLAN configuration 79
8.5 IP subnet-based VLAN configuration 79
8.5.1 Introduction to VLANs based on IP subnets 79
8.5.2 IP Subnet Based VLAN Configuration Task List 80
8.5.3 Create/delete IP subnet-based VLAN table entries 80
8.5.4 Configure whether IP subnet VLANs take precedence over MAC-VLAN table entries 80
8.5.5 Display IP subnet-based VLAN table entry configuration 81
Chapter 9 QinQ Configuration 82
9.1 QinQ Features 82
9.1.1 QinQ Function Introduction 82
9.1.2 Introduction to Static QinQ Functions 82
9.1.3 Introduction to Flexible QinQ Features 83
9.2 QinQ Function Configuration 85
9.2.1 QinQ Configuration Task List 85
9.2.2 Turn on/off the port QinQ function 85
9.2.3 Configure the port internal/external TPID 85
9.2.4 Configuring Port Flexible QinQ Insert Rules 86
9.2.5 Configuring Port Flexible QinQ Pass-through Rules 86
9.2.6 Configuring Port Flexible QinQ Swap Rules 87
9.2.7 Displaying QinQ Configuration Information 87
Chapter 10 MAC address management 89
10.1 Introduction to MAC Address Table Management 89
10.2 MAC address table management configuration 89
10.2.1 MAC Address Table Management Configuration Task List 89
10.2.2 Setting the MAC address aging time 89
10.2.3 Display MAC address aging time 90
10.2.4 Add/delete MAC address table entries 90
10.2.5 Display MAC address table entries 91
10.2.6 Enable/disable MAC address learning switch 91
10.2.7 Display MAC address learning switch 92

10.2.8 Configure the number of MAC addresses allowed to be learned for a port and VLAN 92
10.2.9 Display the number of MAC addresses allowed to be learned 93
Chapter 11 STP Configuration 94
11.1 Introduction to the STP protocol 94
11.2 STP Function Configuration 94
11.2.1 STP Function Configuration Task List 94
11.2.2 Enable/disable device STP function 95
11.2.3 Enable/disable port STP function 95
11.2.4 Configure the device's spanning tree protocol mode 95
11.2.5 Configure the device STP priority 96
11.2.6 Configuring the Device Forward Delay Feature 96
11.2.7 Configuring the Device Hello Time Feature 97
11.2.8 Configuring the Device Max Age Feature 97
11.2.9 Configure port-specific path overhead 98
11.2.10 Configuring STP Priority for a Specific Port 98
11.2.11 Configure specific ports to force the sending of RSTP messages 99
11.2.12 Configure the link type for a specific port 99
11.2.13 Configure the border port state for a specific port 100
11.2.14 Configure the rate limit for sending BPDUs on a specific port 100
11.2.15 Display STP status and configuration parameter information 100
Chapter 12 MSTP Configuration 101
12.1 Introduction to MSTP Protocol 101
12.2 MSTP Feature Configuration 101
12.2.1 MSTP Feature Configuration Task List 101
12.2.2 Configure the device's spanning tree mode to MSTP 101
12.2.3 Configuring MSTP Timer Parameter Values 102
12.2.4 Configure the configuration identifier for MSTP 102
12.2.5 Configuring MSTP Bridge Priorities 103
12.2.6 Configure the border port state of an MSTP port 103
12.2.7 Configure the link type of the MSTP port 104
12.2.8 Configure MSTP ports for path spending 104
12.2.9 Configuring MSTP Port Priority 104
12.2.10 Display MSTP configuration information 105
Chapter 13 Remote Loop Detection Function Configuration 106
13.1 Introduction to Remote Loop Detection Function 106
13.2 Remote Loop Detection Function Configuration 106
13.2.1 Remote Loop Detection Function Configuration Task List 106
13.2.2 Enable/disable remote loop monitoring 106
13.2.3 Configure the remote loop detection processing policy 107
13.2.4 Configuring the Remote Loop Detection Message Transmission Interval 107

13.2.5 Configuring Remote Loop Detection Port Recovery Time....107
13.2.6 Display remote loop detection status information....107
Chapter 14 ACL Configuration....109
14.1 ACL Introduction....109
14.1.1 ACL Overview....109
14.1.2 ACL Classification....109
14.2 ACL Configuration....110
14.2.1 ACL Configuration Task List....110
14.2.2 ACL Match Order Configuration....110
14.2.3 Time Period Configuration....111
14.2.4 Configuring Standard ACLs....111
14.2.5 Configuring Extended ACLs....113
14.2.6 Configuring Layer 2 ACLs....114
14.2.7 Activate Access Control Lists....115
14.2.8 ACL monitoring and maintenance....115
Chapter 15 QoS Configuration....116
15.1 Introduction to QoS....116
15.2 QoS Configuration....118
15.2.1 QoS Configuration Task List....118
15.2.2 Configuring Traffic Supervision....119
15.2.3 Configuration of two-speed three-color marking....119
15.2.4 Configuring Priority Marking....120
15.2.5 Configuring Flow Mirroring....121
15.2.6 Configuring Traffic Statistics....121
15.2.7 Configuring Message Redirection....121
15.2.8 Configuration message copy to CPU....122
15.2.9 Configuring Queue Scheduling....122
15.2.10 Configure the mapping of hardware priority queues to 802.1P protocol priorities....123
15.2.11 Configure the mapping of DSCP to hardware priority queues....124
15.2.12 Configuring Egress Bandwidth Limiting....125
15.2.13 Configuring Ingress Bandwidth Limiting....125
15.2.14 QOS Monitoring and Maintenance....125
15.3 QACL Configuration Example....126
15.3.1 Using QACL for bandwidth control....126
15.3.2 Deny all packet expect using QACLs....127
15.3.3 Using QACL Anti-Virus....127
Chapter 16 SSH Configuration....129
16.1 Introduction to SSH....129
16.2 SSH Configuration....129

16.2.1 SSH Configuration Task List 129
16.2.2 Enable/disable SSH function 129
16.2.3 Configuring SSH Keys 129
16.2.4 Clearing the key configuration 130
16.2.5 Configure a limit on the number of SSH user logins 130
16.2.6 SSH Monitoring and Maintenance 131
Chapter 17 SNMP Configuration 132
17.1 Introduction to SNMP 132
17.2 SNMP Configuration 133
17.2.1 SNMP Configuration Task List 133
17.2.2 Configuring SNMP Access Group Names 133
17.2.3 Configure the administrator contact sysContact 134
17.2.4 Configure device location 135
17.2.5 Configure the device name 135
17.2.6 Configure the notification target host address 135
17.2.7 Enabling Notification and Configuring Notification Sending Methods 136
17.2.8 Configuring the Trap Source Address 137
17.2.9 Configuring the Engine ID 137
17.2.10 Configure the maximum SNMP message length 137
17.2.11 configuration view 138
17.2.12 Configuring Access Control Groups 139
17.2.13 Configure Users 139
17.2.14 Display SNMP configuration information 140
Chapter 18 Info-center Configuration 142
18.1 Introduction to Info-center 142
18.2 Info-center Configuration 142
18.2.1 Info-center configuration task list 142
18.2.2 Enable/disable the device Info-center function 143
18.2.3 Configuring Info-center Serial Number Display 143
18.2.4 Configuring the Info-center timestamp type 143
18.2.5 Configuring Info-center terminal output 144
18.2.6 Configuring Info-center History Buffer Outputs 144
18.2.7 Configuring Info-center Flash Memory Outputs 145
18.2.8 Configuring Info-center Log Host Output 145
18.2.9 Configuring Info-center SNMP Agent Outputs 146
18.2.10 Configuration Module Debug Switch 147
18.2.11 Display Info-center related configuration information 147
Chapter 19 Three-tier functional configuration 148
19.1 Three-Layer Functional Profile 148
19.2 Three-tier functional configuration 148

19.2.1 Layer 3 Functional Configuration List 148
19.2.2 Create VLAN and VLAN Layer 3 interfaces 148
19.2.3 Create/delete common VLAN Layer 3 interfaces 148
19.2.4 Create/delete SuperVLAN Layer 3 interfaces 149
19.2.5 Adding/Removing SuperVLAN Sub-VLANs 149
19.2.6 Configure/delete loopback interfaces 150
19.2.7 Configure/delete Layer 3 interface IP addresses 150
19.2.8 Configuring the Layer 3 Interface ARP Proxy 151
19.2.9 Displaying Layer 3 Interface Configuration 152
19.2.10 Configuring Layer 3 Message Forwarding Mode 152
19.2.11 Configure the destination host unknown message forwarding mode 153
Chapter 20 ARP Function Configuration 154
20.1 ARP Function Introduction 154
20.2 ARP Function Configuration 154
20.2.1 ARP Feature Configuration Task List 154
20.2.2 Adding and deleting ARP table entries 154
20.2.3 Bind dynamic ARP table entries to static ARP table entries 154
20.2.4 Display ARP table entries 155
20.2.5 Configure and restore ARP aging time 155
20.2.6 Display ARP aging time 155
Chapter 21 Anti-ARP attack function 157
21.1 Introduction to Anti-ARP Attack Function 157
21.2 Configuration of Anti-ARP Attack Function 157
21.2.1 Anti-ARP Attack Feature Configuration Task List 157
21.2.2 Enable/disable protection against ARP flooding attacks 157
21.2.3 Configure the anti-ARP flood attack resistance action type and rate thresholds 158
21.2.4 Configuring Anti-ARP Flood Attack Banned MAC Auto Recovery Time 158
21.2.5 Manual recovery of banned MACs against ARP flooding attacks 159
21.2.6 Display anti-ARP flooding attack information 159
21.2.7 Bind the black hole MAC generated by the anti-ARP flooding attack to the general black hole MAC 159
21.2.8 Enable/disable ARP anti-spoofing attack 160
21.2.9 Configuring an Anti-Unknown ARP Message Spoofing Policy 160
21.2.10 Enable/disable ARP message source MAC consistency checking 160
21.2.11 Enable/disable ARP anti-gateway impersonation 161
21.2.12 Display anti-ARP spoofing attack information 161
21.2.13 Configuring Trusted Ports for Anti-ARP Attacks 161
Chapter 22 DHCP-Relay Function 163
22.1 DHCP-Relay Function Introduction 163
22.2 DHCP-Relay Function Configuration 163
22.2.1 DHCP-Relay Function Configuration List 163

22.2.2 Enable/disable DHCP-Relay function....163
22.2.3 Configuring the DHCP Server....164
22.2.4 Layer 3 Interface Binding DHCP Server....164
22.2.5 Displaying DHCP Server Configuration....165
22.2.6 Hide DHCP server....165
22.2.7 Configuring the DHCP Option82 Feature....165
Chapter 23 DHCP S nooping function....166
23.1 Introduction to DHCP Snooping Features....166
23.2 DHCP Snooping Function Configuration....167
23.2.1 DHCP Snooping Feature Configuration List....167
23.2.2 Enable/disable DHCP Snooping function....167
23.2.3 Configuring DHCP Snooping Trusted Ports....167
23.2.4 Configuring the Maximum Number of Clients for DHCP Snooping....168
23.2.5 Configuring the DHCP Snooping Port linkdown Fast Aging Table Entry Function....168
23.2.6 Enable/disable port IP-source-guard function....169
23.2.7 Configuring IP-source-guard Static Binding Table Entries....169
23.2.8 Display DHCP Snooping configuration information....169
23.2.9 Display DHCP Snooping user information....170
23.2.10 Delete the DHCP Snooping table entry....170
Chapter 24 Local IP address pool configuration....171
24.1 Local IP Address Pool Introduction....171
24.2 Local IP address pool configuration....171
24.2.1 Local IP Address Pool Configuration Task List....171
24.2.2 Enter IP address pool view....171
24.2.3 Configure the local IP address pool gateway and subnet masks....172
24.2.4 Configure local IP address pool segments....172
24.2.5 Disable/activate the specified IP address in the local IP address pool....172
24.2.6 Configuring the Local IP Address Pool Lease Period....173
24.2.7 Configuring Local IP Address Pool DNS....173
24.2.8 Configuring the Local IP Address Pool WINS....174
24.2.9 Display the local IP address pool configuration....174
24.2.10 Configuring the dhcp-client bind function....174
24.2.11 Show dhcp-client bind configuration....175
24.2.12 Add/remove dhcp-client client list....175
24.2.13 Display dhcp-client client list configuration information....175
Chapter 25 IGMP Snooping Configuration....176
25.1 Introduction to IGMP Snooping Protocol....176
25.2 IGMP Snooping Configuration....176
25.2.1 IGMP Snooping Configuration Task List....176
25.2.2 Enable/disable the IGMP Snooping function....177

25.2.3 Configuring IGMP Snooping Member Port Aging Time 177
25.2.4 Configuring Maximum Response Time for IGMP Snooping Queries 177
25.2.5 Configuring the IGMP Snooping Port Fast Leave Function 178
25.2.6 Configuring IGMP Snooping Port Learning Multicast Number Limits 178
25.2.7 Configuring IGMP Snooping Black and White Lists 178
25.2.8 Configuring the IGMP Snooping Route Port Forwarding Function 179
25.2.9 Configuring the IGMP Snooping Querier Switch 179
25.2.10 Configuring the IGMP Snooping Querier Send Message Interval 180
25.2.11 Configuring IGMP Snooping Generic Query Message Sending VLANs 180
25.2.12 Configuring IGMP Snooping General Query Maximum Response Time 180
25.2.13 Configuring IGMP Snooping Generic Query Message Source IP Addresses 181
25.2.14 Configuring IGMP Snooping Route Port Aging 181
25.2.15 Add/Remove IGMP Snooping Routing Ports 181
25.2.16 Configuring Multicast VLANs for IGMP Snooping Ports 182
25.2.17 Display IGMP Snooping configuration information 182
25.2.18 Enable/disable IGMP Snooping multicast preview function 183
25.2.19 Configuring IGMP Snooping Multicast Preview Control Parameters 183
25.2.20 Configuring IGMP Snooping Multicast Preview Channels 183
25.2.21 Display IGMP Snooping Multicast Preview Information 184
25.2.22 Create/Delete IGMP Snooping profile 184
25.2.23 Configuring IGMP Snooping profile type and address range 184
25.2.24 Reference IGMP Snooping profile configuration 185
25.2.25 Configuring IGMP Snooping MVR Features 186
25.2.26 Display IGMP Snooping profile configuration information 186
25.2.27 Display the multicast table entries learned by IGMP Snooping 187
Chapter 26 MLD Snooping Configuration 188
26.1 MLD Snooping Protocol Profile Configuration 188
26.2 MLD Snooping Configuration 188
26.2.1 MLD Snooping Configuration Task List 188
26.2.2 Enable/disable the MLD Snooping function 188
26.2.3 Configuring MLD Snooping Member Port Aging Time 189
26.2.4 Configuring the Maximum Response Time for MLD Snooping Queries 189
26.2.5 Configuring the MLD Snooping Port Fast Leave Function 189
26.2.6 Configuring MLD Snooping Port Learning Multicast Number Limits 190
26.2.7 Configuring MLD Snooping Black and White Lists 190
26.2.8 Configuring the MLD Snooping Route Port Forwarding Function 191
26.2.9 Configuring the MLD Snooping Querier Switch 191
26.2.10 Configuring the MLD Snooping Querier Send Message Interval 192
26.2.11 Configuring the Maximum Response Time for MLD Snooping Generic Queries 192
26.2.12 Configuring MLD Snooping Route Port Aging 192

26.2.13 Add/Remove MLD Snooping Routing Ports 193
26.2.14 Configuring Multicast VLANs for MLD Snooping Ports 193
26.2.15 Display MLD Snooping configuration information 193
26.2.16 Displaying MLD Snooping Learned Multicast Table Entries 194
Chapter 27 Static Multicast Configuration 195
27.1 Introduction to Static Multicast 195
27.2 Static Multicast Configuration 195
27.2.1 Static Multicast Configuration Task List 195
27.2.2 Create/delete static multicast groups 195
27.2.3 Add/remove static multicast group member ports 195
27.2.4 Add/remove static multicast groups based on IP addresses 196
27.2.5 Display static multicast group configuration information 196
Chapter 28 IGMP Configuration 197
28.1 Introduction to IGMP 197
28.2 IGMP Configuration 197
28.2.1 IGMP Configuration Task List 197
28.2.2 Enable Multicast Protocol 198
28.2.3 Specifies that the interface is running the IGMP protocol 198
28.2.4 Configure the version number of the interface running IGMP 199
28.2.5 Configure the time interval for sending generic query messages 199
28.2.6 Configure the interval for sending last member queries 199
28.2.7 Configuring robustness variables 200
28.2.8 Configure the interface to limit the number of multicast groups that can be joined 200
28.2.9 Configuring IGMP Maximum Query Response Time 201
28.2.10 Configuring Interface Access Control Lists 201
28.2.11 Configure static IP multicast table entries 202
28.2.12 Configure a port to statically join a multicast group 203
28.2.13 Configuring the IGMP-Proxy Function 203
28.2.14 Configuring the SSM-Mapping Function 203
28.2.15 Enter IGMP view 204
28.2.16 Configuring SSM-Mapping Static Group Address Mapping Rules 204
28.2.17 IGMP Monitoring and Maintenance 205
Chapter 29 PIM Configuration 206
29.1 Introduction to the PIM protocol 206
29.1.1 How PIM-DM works 206
29.1.2 How PIM-SM works 207
29.1.3 How PIM-SSM works 209
29.2 PIM Configuration 210
29.2.1 PIM Configuration Task List 210
29.2.2 Enable Multicast Protocol 210

29.2.3 Specifies that the interface runs the PIM-DM protocol 210
29.2.4 Specifies that the interface runs the PIM-SM protocol 211
29.2.5 Configure the PIM protocol Hello message sending interval 211
29.2.6 Configuring BSR Boundaries 212
29.2.7 Enter the PIM view 212
29.2.8 Configuring Multicast Source Filtering 212
29.2.9 Configuring PIM Neighbor Filtering 213
29.2.10 Configure the maximum number of PIM neighbors for an interface 213
29.2.11 Configuring Static RP 214
29.2.12 Configuring candidate BSRs 214
29.2.13 Configuring candidate RPs 215
29.2.14 Configuring the SPT switching threshold 215
29.2.15 Configuring SSM Multicast Group Scope 216
29.2.16 PIM Monitoring and Maintenance 217
Chapter 30 SNTP Client Configuration 218
30.1 Introduction to SNTP Protocol 218
30.2 SNTP Client Configuration 218
30.2.1 SNTP Client Configuration Task List 218
30.2.2 Enable/disable SNTP client function 219
30.2.3 Configure how the SNTP client works 219
30.2.4 Configuring Unicast Servers for SNTP Clients 220
30.2.5 Configure the broadcast delay for SNTP clients 220
30.2.6 Configure the polling interval for SNTP clients 220
30.2.7 Configure the timeout retransmission count and retransmission interval for SNTP clients 221
30.2.8 Configure the list of legitimate servers for SNTP clients 221
30.2.9 Configuring MD5 Authentication for SNTP Clients 221
30.2.10 Configuring Daylight Saving Time for SNTP Clients 222
30.2.11 Display SNTP client configuration information 222
Chapter 31 802.1X Configuration 224
31.1 802.1X Protocol Introduction 224
31.2 AAA View Configuration 224
31.2.1 AAA view configuration task list 224
31.2.2 Enter AAA view 225
31.2.3 Configure the device to restart the user re-authentication function 225
31.2.4 Enable/disable the H3C Cams compatibility feature 225
31.2.5 Configure the uplink/downlink bandwidth attribute number 226
31.2.6 Enable/disable sending client's version information to RADIUS server function 226
31.2.7 Enable/disable billing 226
31.2.8 Enable/disable billing message unresponsive cut-off user function 227
31.2.9 Enable/disable port 802.1P priority extension attributes 227

31.2.10 Enable/disable port PVID extended attributes 228
31.2.11 Enable/disable the port MAC address number limit extended attribute 228
31.2.12 Enable/disable port bandwidth control extended attributes 228
31.2.13 Modify the extended attribute number 229
31.2.14 Configuring the default domain name 230
31.3 RADIUS server configuration 230
31.3.1 RADIUS Server Configuration Task List 230
31.3.2 Create and enter the RADIUS server view 231
31.3.3 Configure the IP address and authentication port of the master/slave authentication server 231
31.3.4 Configure the IP address and authentication port of the master/slave billing server 231
31.3.5 Configure the shared key between the device and the RADIUS authentication server 232
31.3.6 Configure a shared key between the device and the RADIUS billing server 232
31.3.7 Configure the NAS_IPAddress value sent to the RADIUS server 233
31.3.8 Configure the system to pass messages to the RADIUS server with or without a domain name. 233
31.3.9 Configuring Real-Time Billing for RADIUS Servers 234
31.3.10 Display RADIUS server configuration information 234
31.4 domain configuration 235
31.4.1 Domain Configuration Task List 235
31.4.2 Create and enter the domain view 235
31.4.3 Configuring Domain Binding RADIUS Servers 235
31.4.4 Configure the maximum number of users allowed to authenticate through the domain 236
31.4.5 Activate/deactivate domains 236
31.4.6 Displaying Domain Configuration Information 237
31.5 802.1X Configuration 237
31.5.1 802.1X Configuration Task List 237
31.5.2 Enable/disable 802.1X authentication function 237
31.5.3 Configure the port to send 802.1X watchdog messages 238
31.5.4 Configure the protocol type between the device and the RADIUS server 238
31.5.5 Configuring the Reauthentication Function 239
31.5.6 Configure the control mode of an 802.1X port 239
31.5.7 Configure the maximum number of users allowed to authenticate on a port 240
31.5.8 Delete the specified online user 240
31.5.9 Configuring Heartbeat Detection 241
31.5.10 Configuring the Silent Function 241
31.5.11 Configuring the Guest VLAN Function 242
31.5.12 Configure host mode under port-based authentication 242
31.5.13 Configuring EAPOL Message Passthrough 243
31.5.14 Monitoring and Maintenance of 802.1X 243
Chapter 32 LLDP Configuration 245
32.1 Introduction to the LLDP Protocol 245

32.2 LLDP Function Configuration 245
32.2.1 LLDP Feature Configuration Task List 245
32.2.2 Enable/disable global LLDP function 245
32.2.3 Configuring Hello-time for LLDP 246
32.2.4 Configuring Hold-time for LLDP 246
32.2.5 Configure the LLDP Chassis-id 246
32.2.6 Configure the port LLDP message sending and receiving mode 247
32.2.7 Configure the management IP address interface for LLDP messages 247
32.2.8 Display LLDP information 248
Chapter 33 PPPoE Plus Configuration 249
33.1 Introduction to PPPoE Plus 249
33.2 PPPoE Plus Feature Configuration 249
33.2.1 PPPoE Plus Feature Configuration Task List 249
33.2.2 Enable/disable PPPoE Plus function 249
33.2.3 Configuring the PPPoE Plus Message Format Type 250
33.2.4 Configuring the PPPoE Plus Message Format 250
33.2.5 Configuring the PPPoE Plus Message Separator 250
33.2.6 Configuring the PPPoE Plus Label Replacement Policy 251
33.2.7 Configure the PPPoE Plus port type 251
33.2.8 Configure a custom Circuit ID 252
33.2.9 Configuring the Discard PPPoE Messages Function 252
33.2.10 Show PPPoE Plus Configuration 253
Chapter 34 CFM Configuration 254
34.1 CFM Protocol Introduction 254
34.1.1 CFM Protocol Introduction 254
34.1.2 CFM Basic Concepts 254
34.1.3 Introduction to CFM Functions 254
34.2 CFM Functional Configuration 255
34.2.1 CFM Functional Configuration Task List 255
34.2.2 Create/Delete Maintenance Domain MD 255
34.2.3 Configuring Maintenance Domain MD Parameters 256
34.2.4 Create/Delete Maintenance Set MA 256
34.2.5 Configuring Maintenance Set MA Parameters 257
34.2.6 Create/delete maintenance endpoint MEPs 258
34.2.7 Create/Delete Remote Maintenance Endpoint RMEPs 258
34.2.8 Create/Delete Maintenance Intermediate Point MIP 259
34.2.9 CFM loopback detection 259
34.2.10 CFM Link Tracing 260
34.2.11 Monitoring and Maintenance of CFM 260
Chapter 35 EFM Configuration 262

35.1 Introduction to the EFM Protocol 262
35.1.1 Introduction to the EFM Protocol 262
35.1.2 EFM Basic Concepts 262
35.1.3 EFM Operational Mechanism 264
35.2 EFM Functional Configuration 264
35.2.1 EFM Function Configuration Task List 264
35.2.2 Enable/disable EFM function 265
35.2.3 Configure the port's EFM operating mode 265
35.2.4 Configuring the EFM Discovery Cycle 266
35.2.5 Configure the timeout for EFM discovery 266
35.2.6 Configuring the EFM Response Timeout 267
35.2.7 Configuring Link Monitor Event Parameters 267
35.2.8 Enable/disable remote failure indication 268
35.2.9 Enable/disable the link monitoring function 269
35.2.10 Enable/disable remote MIB variable fetch function 269
35.2.11 Enable/disable remote loopback function 269
35.2.12 Enable/disable remote loopback 270
35.2.13 Configure the processing policy for remote loopback request messages 270
35.2.14 EFM Monitoring and Maintenance 271
Chapter 36 ERRP Configuration 273
36.1 Introduction to the ERRP Protocol 273
36.1.1 Introduction to the ERRP Protocol 273
36.1.2 ERRP Basic Concepts 273
36.1.3 ERRP Protocol Principles 274
36.2 ERRP Function Configuration 276
36.2.1 ERRP Feature Configuration Task List 276
36.2.2 Enable/disable ERRP function 277
36.2.3 Configuring ERRP Timer Parameters 277
36.2.4 Create and enter ERRP domain view 277
36.2.5 Configure the operating mode of the ERRP domain 278
36.2.6 Configuring Control VLANs for ERRP Domains 278
36.2.7 Create/delete ERRP rings and nodes within rings 279
36.2.8 Activation/de-activation of ERRP rings 279
36.2.9 Configuring ERRP to Trigger Multicast Query Message Delivery 280
36.2.10 Configuring ERRP Topology Collection 280
36.2.11 Display ERRP configuration information 281
Chapter 37 FlexLink Configuration 282
37.1 Introduction to FlexLink 282
37.1.1 Introduction to FlexLink 282
37.1.2 FlexLink Basic Concepts 282

37.1.3 FlexLink Basic Principles 283
37.2 FlexLink Function Configuration 284
37.2.1 FlexLink Function Configuration Task List 284
37.2.2 Creating/Deleting FlexLink Groups 284
37.2.3 Add/Remove Flexlink Master Ports 284
37.2.4 Add/Remove Flexlink Slave Ports 285
37.2.5 Configuring the FlexLink Group Preemption Method 285
37.2.6 Configuring the FlexLink Group Preemption Delay Time 286
37.2.7 Configuring the FlexLink Flush Function 286
37.2.8 Display FlexLink configuration information 287
Chapter 38 Monitorlink Configuration 288
38.1 About Monitorlink 288
38.1.1 About Monitorlink 288
38.1.2 Monitorlink Basic Concepts 288
38.1.3 Monitorlink Basic Principles 289
38.2 Monitorlink Function Configuration 289
38.2.1 Monitorlink Function Configuration Task List 289
38.2.2 Configure the Monitorlink group function of a port 290
38.2.3 Configuring Monitorlink Group Functions for Aggregation Groups 290
38.2.4 Display Monitorlink configuration information 290
Chapter 39 Static Route Configuration 292
39.1 Introduction to Static Routing 292
39.2 Static Routing Feature Configuration 292
39.2.1 Static Route Configuration Task List 292
39.2.2 Add/delete static routing table entries 292
39.2.3 Display routing table information 293
Chapter 40 RIP configuration 295
40.1 Introduction to RIP 295
40.1.1 Basic Concepts of RIP 295
40.1.2 RIP's routing database 295
40.1.3 RIP startup and operation process 295
40.1.4 Protocol Versions of RIP 296
40.2 RIP Feature Configuration 296
40.2.1 RIP Feature Configuration Task List 296
40.2.2 Enable/disable the RIP function 297
40.2.3 Specifies that the IP interface is running the RIP protocol 297
40.2.4 Specifies the RIP version for the interface 297
40.2.5 Configuring RIP Message Authentication 298
40.2.6 Configuration level segmentation and toxicity reversal 299

40.2.7 Configuring a Publication Aggregation Route 299
40.2.8 Configuring Additional Routes Rights 300
40.2.9 Configuring Default Route Weights 301
40.2.10 Configuring RIP Routing Administrative Distance 301
40.2.11 Configuring Route Filtering 302
40.2.12 Configure the introduction of external routes 302
40.2.13 Configuring Default Route Redistribution 303
40.2.14 Configure the specified interface to block RIP packets 303
40.2.15 Configuring RIP Timer Parameters 304
40.2.16 Create/delete RIP keychain keychain 304
40.2.17 Create/delete RIP keychain keychain-key 305
40.2.18 Configure the parameters related to the keychain-key of the RIP keychain 305
40.2.19 Monitoring and Maintenance of RIP 306
Chapter 41 OSPF Configuration 307
41.1 Introduction to OSPF 307
41.1.1 Basic concepts of OSPF 307
41.1.2 Protocol flow of OSPF 313
41.2 Configuration of OSPF 314
41.2.1 OSPF Configuration Task List 314
41.2.2 Enable/disable OSPF function 315
41.2.3 Configure the RID of the router 315
41.2.4 Specify that the IP interface is running the OSPF protocol 316
41.2.5 Configure the authentication type of the zone 316
41.2.6 Configure the interface type 317
41.2.7 Configure the interface to ignore MTU checks 318
41.2.8 Configuring Interface Overhead 318
41.2.9 Configuring Interface DR Priority 318
41.2.10 Configure the interface Hello message sending interval 319
41.2.11 Configure the failure time between neighboring routers of an interface 320
41.2.12 Configure the interface neighbor router retransmission LSA interval 321
41.2.13 Configure the transmission delay time for LSU messages sent by the interface 321
41.2.14 Configuring Interface Message Authentication Function 322
41.2.15 Configuring the Interface BFD Monitoring Link Status Function 322
41.2.16 Configure the STUB area for OSPF 323
41.2.17 Configure the NSSA area for OSPF 324
41.2.18 Configuring OSPF Area Route Aggregation 324
41.2.19 Configuring OSPF Virtual Connections 325
41.2.20 Configure OSPF to introduce external routes 326
41.2.21 Configure OSPF to introduce default routes 327
41.2.22 Configuring OSPF to Introduce External Routes Default Spend 327

41.2.23 Configuring OSPF Route Filtering 328
41.2.24 Configuring OSPF Routing Administrative Distance 328
41.2.25 Configuring OSPF Neighbor Routers for Interconnected NBMA Networks 329
41.2.26 OSPF Monitoring and Maintenance 330
Chapter 42 BGP Configuration 331
42.1 BGP Introduction 331
42.1.1 Introduction to the BGP Protocol 331
42.1.2 Overview of BGP operation 331
42.1.3 Routing Policies for BGP 332
42.2 Configuration of BGP 332
42.2.1 BGP Configuration Task List 332
42.2.2 Enable/disable the BGP feature 333
42.2.3 Configure network routes for local BGP announcements 334
42.2.4 Create/delete BGP peer groups 334
42.2.5 Configuring BGP Peers Autonomous System Number 334
42.2.6 Add/remove BGP peer group members 335
42.2.7 Configure to allow connections to EBGP peers on networks that are not directly connected to each other 336
42.2.8 Configuring the BGP Peer Timer 336
42.2.9 Configure the interval at which BGP peers send routing update messages 337
42.2.10 Configure a BGP peer to use its own address as the next hop when it advertises a route 337
42.2.11 Configuring BGP Peer Route Filtering Policies Based on IP Prefix Control Lists 338
42.2.12 Configuring BGP Peer Route Filtering Policies Based on IP Access Control Lists 338
42.2.13 Configuring BGP Peer Route Filtering Policies Based on AS Path Lists 339
42.2.14 Configuring Route-map-based Route Mapping Policies for BGP Peers 340
42.2.15 Configure whether BGP peers do not actively send connection requests 340
42.2.16 Shutting down BGP peer connections 341
42.2.17 Configuring BGP Global Timer 341
42.2.18 Configuring BGP Local Priority 342
42.2.19 Configure whether BGP compares MED values of different ASes 342
42.2.20 Configuring BGP Route Aggregation 343
42.2.21 Configure BGP to introduce IGP protocol routes 343
42.2.22 Configure the BGP Router ID 344
42.2.23 Monitoring and Maintenance of BGP 344
Chapter 43 BFD Functional Configuration 345
43.1 Introduction to BFD 345
43.1.1 Introduction to the BFD Protocol 345
43.1.2 BFD Protocol Flow 345
43.2 BFD Functional Configuration 347
43.2.1 BFD Function Configuration Task List 347
43.2.2 Enable/disable BFD function 347

43.2.3 Enable/disable OSPF BFD function 348
43.2.4 Configure the minimum sending interval of control messages expected by BFD 348
43.2.5 Configure the minimum receive interval for BFD control messages 348
43.2.6 Configure the detection multiplier for BFD control messages 349
43.2.7 Configuring BFD Session Mode 349
43.2.8 Configuring BFD Detection Mode 350
43.2.9 Clear BFD session packet statistics 350
43.2.10 BFD Monitoring and Maintenance 350
Chapter 44 VRRP Configuration 352
44.1 Introduction to VRRP 352
44.1.1 Introduction to VRRP Protocol 352
44.1.2 VRRP Basic Concepts 352
44.2 VRRP Configuration 352
44.2.1 VRRP Feature Configuration Task List 352
44.2.2 Add/remove virtual IP addresses 353
44.2.3 Configure the priority of the backup group 353
44.2.4 Configure the preemption method and delay time for backup groups 354
44.2.5 Configuring Timers for Backup Groups 354
44.2.6 Configure the monitor interface for the backup group 355
44.2.7 VRRP Monitoring and Maintenance 355
Chapter 45 DLF Message Forwarding Control 357
45.1 Introduction to DLF Message Forwarding Control 357
45.2 DLF Message Forwarding Control Configuration 357
45.2.1 DLF Message Forwarding Control Configuration Task List 357
45.2.2 Configure unknown unicast message forwarding control 357
45.2.3 Configure unknown multicast message forwarding control 357
45.2.4 Display the DLF message forwarding control configuration 358
Chapter 46 BPDU message forwarding control 359
46.1 Introduction to BPDU message forwarding control 359
46.2 BPDU Message Forwarding Control Configuration 359
46.2.1 BPDU Message Forwarding Control Configuration Task List 359
46.2.2 Configure global BPDU message forwarding control 359
46.2.3 Configure port BPDU message forwarding control 359
46.2.4 Display the BPDU message forwarding control configuration 360
Chapter 47 bpdu-tunnel configuration 361
47.1 Introduction to bpdu-tunnel 361
47.2 bpdu-tunnel configuration 361
47.2.1 bpdu-tunnel configuration task list 361
47.2.2 Enable/disable bpdu-tunnel function 361

47.2.3 Configure the bpdu-tunnel message destination MAC 361
47.2.4 Display bpdu -tunnel configuration information 362
Chapter 48 Local-Switch Function 363
48.1 Local-Switch Function Introduction 363
48.2 Local-Switch Function Configuration 363
48.2.1 Local-Switch Configuration Task List 363
48.2.2 Enable/disable Local-Switch function 363
48.2.3 Displaying Local-Switch Configuration Information 363
Chapter 49 Port Utilization Alerts 364
49.1 Introduction to Port Utilization Alerts 364
49.2 Port Utilization Alert Configuration 364
49.2.1 Port Utilization Alert Configuration Task List 364
49.2.2 Global open/close port utilization alerts 364
49.2.3 Port Enable/Disable Port Utilization Alert 364
49.2.4 Configure the overrun and normal thresholds for port utilization alarms 364
49.2.5 Display port utilization alarm configuration information 365
Chapter 50 CPU Utilization Alerts 366
50.1 Introduction to CPU Utilization Alerts 366
50.2 CPU Utilization Alert Configuration 366
50.2.1 CPU Utilization Alert Configuration Task List 366
50.2.2 Enable/disable CPU utilization alarm 366
50.2.3 Configuring Busy Thresholds and No-Busy Thresholds for CPU Utilization Alerts 366
50.2.4 Display CPU utilization alert configuration information 367
Chapter 51 IS-IS Function Configuration 368
51.1 IS-IS Functional Overview 368
51.1.1 basic concept 368
51.1.2 IS-IS region 369
51.1.3 IS-IS network types 371
51.1.4 IS-IS messages 372
51.2 IS-IS Function Configuration 374
51.2.1 IS-IS Feature Configuration Task List 374
51.2.2 Enable IS-IS 374
51.2.3 Configure the Level level of the router and the link adjacency type of the interface 375
51.2.4 Configure the interface network type 375
51.2.5 Configuring the IS-IS Link Overhead Type 375
51.2.6 Configuring IS-IS Link Overhead 376
51.2.7 Configure the Hello message sending interval 376
51.2.8 Configure the number of Hello message failures 376
51.2.9 Configuring Hello Message Filling 377

51.2.10 Configuring the CSNP message sending interval 377
51.2.11 Configure the PSNP message sending interval 377
51.2.12 Configure the DIS priority of the interface 378
51.2.13 Disables the interface from sending and receiving IS-IS messages 378
51.2.14 Configuring LSP Parameters 378
51.2.15 Configuring SPF Parameters 379
51.2.16 Configure the LSDB overload flag bit 379
51.2.17 Configuring IS-IS Hostname Mapping 379
51.2.18 Configure output switches for neighbor state changes 380
51.2.19 Configuring Neighborhood Authentication 380
51.2.20 Configuration area validation 380
51.2.21 Configuring Routing Domain Authentication 381
51.2.22 Display and maintenance of IS-IS 381
Chapter 52 ERPS configuration 382
52.1 Introduction to the ERPS protocol 382
52.1.1 Introduction to the ERRP Protocol 382
52.1.2 ERPS Basic Concepts 382
52.1.3 ERPS Ring Protection Mechanism 383
52.2 ERPS Functional Configuration 384
52.2.1 ERPS Function Configuration Task List 384
52.2.2 Enable/disable ERPS function 384
52.2.3 Configuring an ERPS Instance 384
52.2.4 Configuring ERPS Link Connectivity Detection 385
52.2.5 Configure ERPS-related timers 386
52.2.6 ERPS Display and Maintenance 387
Chapter 53 ONT Discovery Configuration 388
53.1 ONT Discovery Overview 388
53.2 ONT Discovery Configuration 388
53.2.1 ONT Discovery Configuration 388
53.2.2 [GPON]ont-autofind interface gpon 2/1 388
53.2.3 Config success: 1, failed: 0. 388
53.2.4 ONT Silent Configuration 388
Chapter 54 ONT Template Configuration 389
54.1 ONT Templates Overview 389
54.2 Alarm Template Configuration 389
54.3 DBA Template Configuration 389
54.4 VLAN Template Configuration 389
54.5 Upstream Template Configuration 390
54.6 Downstream Template Configuration 390

54.7 Multicast Template Configuration 390
54.8 Specific template configuration 391
54.9 Line Template Configuration 392
54.10 Rule Template Configuration 393
Chapter 55 system management 395
55.1 Overview of system administration 395
55.2 System Management Configuration 395
55.2.1 Reboot ONT 395
55.2.2 Upgrade ONT 395
55.2.3 Activate/Deactivate ONT 395
55.2.4 Auto-configuration of ONT 396
55.2.5 ont auto-config { name *name* | *num* } all-ont smart-match 396
55.2.6 Reset ONT 396
55.3 ONT Log Management 396
55.4 PON protection 397
Chapter 56 ONT Information View 398
56.1 ONT Message View Overview 398
56.2 View ONT Optical Power 398
56.3 View ONT traffic statistics 398
56.4 Check ONT port status 398
56.5 View ONT Multicast 398
56.6 View ONT details 398
56.7 View ONT Templates 399
56.8 View ONT description 399
56.9 View ONT Upgrade Status 399
56.10 View ONT version 399
56.11 View ONT MAC 399
56.12 View ONT Competency Levels 399
56.13 View ONT PoE Features 399
56.14 View Rogue ONT Detection 399

Chapter 1 Access OLT devices

The GPON OLT Operator's Manual is divided into two main sections, including:

- Device management and maintenance and switching features configuration
- Configuration of PON-related features

Chapter 1 focuses on some of the basics needed to manage OLT equipment, including:

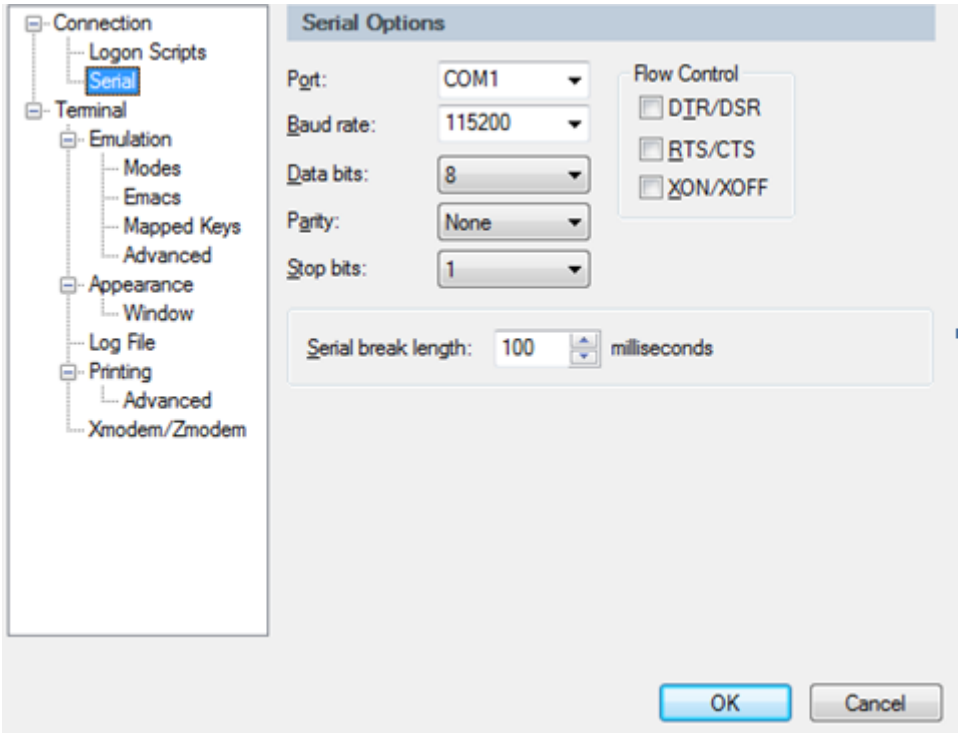
- Command-line interface
- User management
- Ways to manage equipment
- Remote authentication of administrative users

1.1 command-line interface

The command line interface is the interactive interface between the device and the user. Through the command line interface, the user can enter commands to configure the device and can confirm the configuration results by viewing the output.

Command line configuration management can be performed in the following ways:

1, through the Console port for local configuration, the serial port baud rate of 115200, set the following chart:



2. Local or remote configuration via Telnet/SSH;

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

1.1.1 Command line view

The command line of the system adopts a hierarchical protection method to prevent unauthorized users from illegal intrusion. Each command view is realized for different configuration requirements, and there are connections and differences between them. For example, when successfully logging on to the system, any level of user can enter the general user view, which can only complete the simple function of viewing system operation information; administrators can then type enable to enter the privileged user view; under the privileged user view, type system-view to enter the system view; under the system view, type different configuration commands to enter the corresponding configuration view. Under system view, type different configuration commands to enter the corresponding configuration view. For example, type vlan *vlan-list* to enter the VLAN configuration view. You can jump directly between configuration views. If each configuration view contains subviews, you can also jump directly between subviews. Details of the functional characteristics of each command view and the commands to enter each view are shown in the following table:

command-line mode	functionality	prompt	entry command	exit command
General User View	Viewing device operation information	GPON>	Establish a connection with the device, enter the login username and password and then enter the	QUIT disconnects from the device
privileged user view	View equipment operation information and perform system management	<GPON>	In normal user view, type enable	quit returns to the normal user view
system view	Configuring global parameters	[GPON]	Under privileged user view, type system-view	quit, end return to privileged user view
port view	Configuring Ethernet Port Parameters	[GPON-ethernet-0/0/1]	In system view, type interface ethernet 0/0/1	quit returns to the system view end returns the privileged user view
port group view	Configure a set of Ethernet port parameters	[GPON-port-range]	Type interface range ethernet 0/0/1 to ethernet 0/0/4 in system view.	
VLAN view	Configuring VLAN Parameters	[GPON-vlan-2]	In system view, type vlan 2	
AAA View	Create Domain	[GPON-aaa]	Type aaa in system view	
RADIUS Server View	Configuring RADIUS Server Parameters	[gpon-aaa-radius-test]	In system view, type radius host test	quit returns to the AAA view end returns the privileged user view
Domain Configuration View	Configuring Domain Parameters	[GPON-aaa-domain-test.com]	In AAA view, type domain test.com	
VLAN interface view	Configuring VLAN Layer 3 Interfaces	[GPON-vlanInterface-1]	In system view, type interface vlan-interface 1	quit returns to the system view end returns the privileged user view

SuperVLAN interface view	Configuring SuperVLAN Layer 3 Interfaces	[GPON-superVLANInterface-128]	In system view, type interface supervlan-interface 128	quit returns to the system view end returns the privileged user view
LoopBack Interface View	Configure the loopback Layer 3 interface	[GPON-loopBackInterface-0]	In system view, type interface loopback-interface 0	quit returns to the system view end returns the privileged user view
RIP view	Configure RIP-related parameters	[GPON-router-rip]	In system view, type router rip	quit returns to the system view end returns the privileged user view
RIPNG view	Configure RIPNG-related parameters	[GPON-router-ripng]	In system view, type router ripng	quit returns to the system view end returns the privileged user view
OSPF view	Configure OSPF-related parameters	[GPON-router-ospf]	In system view, type router ospf	quit returns to the system view end returns the privileged user view
BGP view	Configure BGP-related parameters	[GPON-router-bgp]	In system view, type router bgp 1	quit returns to the system view end returns the privileged user view
ISIS view	Configure ISIS-related parameters	[GPON-router-isis]	In system view, type router isis	quit returns to the system view end returns the privileged user view
PIM View	Configure PIM-related parameters	[GPON-router-pim]	In system view, type mroute pim	quit returns to the system view end returns the privileged user view
IGMP view	Configure IGMP-related parameters	[GPON-router-igmp]	In system view, type mroute igmp	quit returns to the system view end returns the privileged user view

Standard ACL view	Configure standard ACL-related parameters based on name identification	[GPON-std-nacl-testst]	In system view, type acl standard testst	quit returns to the system view end returns the privileged user view
Extended ACL view	Configure parameters related to extended ACLs based on name identity	[GPON-ext-nacl-testex]	In system view, type acl extended testex	quit returns to the system view end returns the privileged user view
Layer 2 ACL view	Configure name identity-based Layer 2 ACL-related parameters	[GPON-link-nacl-testli]	In system view, type acl link testli	quit returns to the system view end returns the privileged user view
Time Period Configuration View	Configure time period related parameters	[GPON-timerange-test]	In system view, type time-range test	quit returns to the system view end returns the privileged user view
Flexlink Group View	Configure Flexlink group related parameters	[GPON-flex-link-group-0]	In system view, type flex-link-group 0	quit returns to the system view end returns the privileged user view
IP Address Pool View	Configuring IP address pool parameters	[GPON-ip-pool-test]	In system view, type ip pool test	quit returns to the system view end returns the privileged user view

1.1.2 Understanding command syntax

This section focuses on the steps to take when accessing the command line for configuration. Please read this section and the sections that follow for more information on using the command line interface.

The login authentication of the OLT console mainly performs identity verification of the operating user, and allows or denies the login of the user by matching and identifying the user name and password of the operating user.

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

Login.

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

*****

After entering the login password, if it is correct, you can enter the normal user view with the prompt:

GPON>

In the OLT system, there are two different privileges, one for administrator privileges and the other for ordinary user privileges. Ordinary users generally can only see the configuration information of the OLT and do not have the right to modify it, but administrators can use specific commands to manage the configuration of the OLT.

If you are logged in as a system administrator, go from the normal user view to the privileged user view:
GPON>enable
Step 2: Type the command name
If the typed command does not contain parameters that require user input, then skip directly to step three. If the typed command contains parameters that require user input, then continue with the following steps:
If the command requires a parameter value, enter the parameter value. When entering the parameter value, you may have to enter keywords. The parameter value portion of the command generally specifies what kind of parameter should be entered, whether it is a value in a range, or a string, or an IP address, if there is something you do not understand, you can enter "?" if there is something you don't understand, you can type "?", and follow the prompt to enter the correct value. The keyword refers to the object to be operated in the command. If the command needs more than one parameter value, please input the keyword and each parameter value in turn according to the prompt of the command, until "<enter>" appears in the prompt message, press the Enter key until the message appears.
Step 3: After typing the complete command, please press the enter key
Example:
! The user does not need to enter parameters
[GPON]quit
"quit" is a command with no parameters. The name of the command is quit, and the command is executed when you press the Enter key after typing this command.
! The user needs to enter the parameters
[GPON]vlan 100
"vlan 100" is a command with parameters and keywords. Where the command keyword is vlan and the parameter value is 100.

1.1.3 Command Syntax Help

The command line interface has built-in syntax help. If you are unsure about the syntax of a command, in any command mode, type "?" or use thehelp command to get a brief description of all the commands in that command mode; type the command string you want followed by "?" to list all keywords that begin with that string, followed by a space followed by "?". If the "?" location for the keyword, then list all the keywords and their simple description, if the parameter, then list the relevant parameter description, you can continue to enter commands according to the prompts, until the prompt command is "〈enter〉", directly enter the execution of the command.
Example:
1. Type "?" directly in the privileged user view.
<GPON>?

Commands of system mode.
---
clear clear erps-ring's statistics
cls clear screen
display display running system information
2. Type "?" immediately after the keyword.
[GPON]interf?
interface
3. Type a space followed by "?" after the command line string.
[GPON]stp ?
forward-time config delaytime

hello-time config hellotime
max-age config max agingtime
priority config priority
<enter> The command end.
4. Range or format of parameters
[GPON]stp forward-time ?
INTEGER<4-30> delaytime: <4-30>(second)
5. Prompting for the end of the command line
[GPON] stp ?
<enter> The command end.
All the above help information can be switched between English and Chinese display by executing the following command under the privileged user view:
language mode { chinese | english }

1.1.4 Symbols in the command

You may see various symbols in the command syntax that simply indicate how you should enter the command, but are not part of the command itself. The following table summarizes these symbols.

notation	descriptive
Vertical straight line |	Vertical lines indicate juxtaposition; this symbol is used in conjunction with [ ] or { }.
Brackets [ ]	The part enclosed in parentheses indicates that this part of the command you can choose to enter either one or none. For example, the command: display vlan [*vlan-id*]
curly brackets { }	Curly brackets are generally used in conjunction with vertical lines. The part enclosed in curly brackets indicates that this part of the command has several options separated by vertical lines, one of which you must choose to enter. For example, the command: stp mode { rstp | stp | mstp }

1.1.5 Command Parameter Type

There are five types of command parameters for the system.

1. Numerical ranges

When the two values in the pointed brackets are connected by an underscore, it means that the parameter takes a value in the range of some number between the two values.

For example, INTEGER<1-10> means that the user can enter any integer greater than or equal to 1 and less than or equal to 10, such as 5 is a legal number.

2. IP address

When the prompt is A.B.C.D, it means that the parameter is an IP address and you must enter a legal IP address value.

For example, 192.168.1.2 is a legal IP address value.

3. MAC address

When the prompt is H:H:H:H:H:H, it means that the parameter is a MAC address and you must enter a legal MAC address value. If you want to enter a multicast MAC address, you will be prompted accordingly.

For example, 00:02:03:04:05:06 is a legitimate MAC address value.

4. Port List

Port list is generally prompted STRING <3-4>, port parameter interface-num by the port type + port number, the port type is ethernet, port number is device/slot-num/port-num, device means stacking device, the value range of 0 to 7, are currently defaulted to 0! The port number is device/slot-num/port-num, device means for stacking device, the value range is 0 to 7, and the default is 0. slot-num means slot number, the value range is 0 to 1, and port-num means the port number in the slot, the value range is 1 to 48; the port parameter interface-list means multiple ports, and the consecutive ports of the same kind can be connected by "to", but the port number immediately following "to" is "to", and the port number is "to". The port number immediately in front of "to" must be smaller than the port number immediately after "to", and this form is allowed to be repeated at most 3 times. If there is any special case for the port parameter interface-list, it will be explained in the command.

For example, display stp interface ethernet 0/0/1 ethernet 0/0/3 means to display spanning tree information for Ethernet ports 1 and 3.

5. Strings

When the prompt is STRING<1-19>, it means that the parameter is to be typed as a string of length 1 to 19, specifically you can type "?" See the command description for this parameter.

1.1.6 Historical Command Recording Function

The Command Line Interface automatically saves the history of commands typed by the user. The user can recall the history of commands saved by the Command Line Interface at any time and repeat the execution. The command line interface can save up to 100 historical commands for each user. To access the previous command, you can type "Up" or "Ctrl+P", and to access the next command, you can type "Down" or "Ctrl+N". Ctrl+N".

 Description:

- Use the cursor keys to access the history commands. When using Windows 9X HyperTerminal, the ↑ and ↓ cursor keys will be ineffective due to the different interpretations of the two keys in Windows 9X HyperTerminal, and you can replace the ↑ and ↓ cursor keys with the key combinations <Ctrl+P> and <Ctrl+N> to achieve the same purpose. For Windows 2000/XP/2003 HyperTerminal's cursor keys can be used normally;
- When a user enters the same command multiple times in a row, only one command is saved as a history command by the command line interface;

1.1.7 Command line error messages

All commands typed by the user can be executed correctly only if they pass the syntax check, otherwise an error message is reported to the user, and common error messages are shown in the following table.

English Error Messages	Cause of error
Incomplete command	Incomplete command entered
Invalid parameter	Input parameter error
Unrecognized command	No command found.
	No keywords found
error detected at '^' marker	Error found at "^" position

1.1.8 Command Line Editing Functions

The command line interface provides basic command line editing functions and supports multi-line editing. The maximum length of each command, including keywords, spaces, specific parameters, etc., cannot exceed 512 characters in total, including the following table.

keystrokes	functionality
Ordinary keys	If the command length does not reach 512 characters, it is inserted at the current cursor position and moves the cursor to the right
Backspace	Deletes the previous character at the cursor position and moves the cursor forward
Left Cursor Key ← or <Ctrl+B>	The cursor moves one character position to the left
Right Cursor Key→ or <Ctrl+F>	The cursor moves one character position to the right
<Ctrl+A>	The cursor moves left to the start of the command line
<Ctrl+E>	The cursor moves right to the end of the command line
Upper Cursor Key ↑ or <Ctrl+P> Down cursor key ↓ or <Ctrl+N>	Show History Commands
<Tab> key	After inputting an incomplete keyword and pressing the Tab key, the system automatically performs partial help: if the keyword matching the input letter is unique, the system replaces the original input with this complete keyword; if the

	keyword matching the input letter is not unique, press the <Tab> key repeatedly, and the terminal screen displays the complete keyword matching the letter on new lines in turn; if the parameter of the command word does not match, the system does not make any modification and displays the original input on new lines again. If the parameter of the command word does not match, the system does not make any modification and displays the original input on new lines again.

1.2 user management

The system provides two types of user rights:

- ADMINISTRATOR
- NORMAL Ordinary users

When an ordinary user logs into the OLT, he or she can only enter the ordinary user view, not the privileged user view, and therefore can only view system information but not configure it. Administrators have access to all modes to query and configure the system parameters.

1.2.1 System default user account

The system has a default built-in account admin with an initial password of admin. It is recommended that you change the password for the admin user when you first log in to the device to avoid password leakage. This account can not be deleted, administrator privileges can not be modified, and has the privilege to manage other users. Please remember your modified password.

1.2.2 Add user account

First, log in with the system administrator admin account, enter the privileged user view, then enter the system view, by using the terminal user command according to the system prompts, respectively, enter the user name, user privileges, password to increase the user account, you can see the following table description to increase the user account.

manipulate	command	clarification
Enter privileged user view	enable	
Go to System View	system-view	
Add user account	terminal user *username* [privilege *level*] { password *encryption-type password* }	
View User Accounts	display terminal user	

username: the username of the new user, the length is 1~32 characters, must be a print character and cannot contain '/',':', '*', '? ,'\\\,''<','>','|','"" and so on.

privilege: user privilege, the value range is 0 to 15. 0 to 1 means ordinary user; 2 to 15 is administrator.

encryption-type: the value is 0 or 7, 0 means the password is set in plaintext, 7 means the password is set in ciphertext.

password: Indicates the login password of the new user, the length is 1 to 16 characters.

If you do not enter user privileges, the system defaults the user level created to normal user. The system supports up to 8 users.

[Example]

! Create administrator user test with password test and permission 15

[GPON]terminal user test privilege 15 password 0 test

Attention:

- The system is case-insensitive for user names and case-sensitive for passwords;

- Only the system administrator, admin user, can delete users; other users cannot delete users;
- The system administrator, admin, can change his or other users' passwords, while other admin users can only change their own passwords;
- When you set 7 ciphertext password, the input is actually in ciphertext, that is, you need to confirm the plaintext password first, and then convert the plaintext password to ciphertext by the password calculator tool, and then input it in ciphertext, so please be careful to configure the ciphertext form of the password;

1.2.3 Change user password

In system view, the system administrator admin can use the following commands to change his or other users' passwords, while other administrators can only use it to change their own passwords, the operation commands are described in the following table.

manipulate	command	clarification
Enter privileged user view	enable	
Go to System View	system-view	
Change user password	terminal user change-password	

[Example]

! Change the password of user test to 1234

[GPON]terminal user change-password

please input your 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 privileges

In system view, only the system administrator admin can modify other user privileges with the following commands, as described in the following table.

manipulate	command	clarification
Enter privileged user view	enable	
Go to System View	system-view	
Modify user privileges	terminal user *username* [privilege *level*] { password *encryption-type password* }	

username: username of an existing user, 1 to 32 characters long, must be printable and cannot contain characters such as '/', ':', '*', '? , '\\\', '<', '>', '|', "" and other characters must be printable and cannot contain '/', ':', '*', '?', '\\\', '<', '>', '|', "" and other characters. If the entered user name does not exist yet, the user will be added.

Privilege: Modify the privilege of the existing user (admin user can not be modified) to this privilege, the value range is 0 to 15. 0 to 1 means ordinary users; 2 to 15 for administrators

encryption-type: value is 0 or 7, 0 means no encryption, 7 means encryption.

password: change the login password of the existing user to this password, which is 1~16 characters or numbers.

If you do not enter a user privilege, that user privilege remains unchanged.

[Example]

! Modify the permissions of the existing administrator user test to 1 and the password to test

[GPON]terminal user test privilege 1 password 0 test

1.2.5 Delete user account

The system administrator, admin, can delete user accounts under System View, as described in the following table:

manipulate	command	clarification
Enter privileged user view	enable	
Go to System View	system-view	
Delete user account	undo terminal user *username*	Username is the username to be deleted

[Example]

! Delete user test

[GPON]undo terminal user test

1.2.6 Viewing User Account Configuration

Execute the display command in any view to view user account configuration information.

manipulate	command	clarification
View User Information	display terminal user [*username*]	When username is specified, the command displays information about the specified user. When username is not specified, the command displays information about all users.

[Example]

! Show information about user test

[GPON]display terminal user test

1.2.7 View online user information

Execute the following command in any view to view the user information of the logged-in device.

manipulate	command	clarification
View User Information	display login-users	

[Example]

! Show information about user test

[GPON]display login-users

1.2.8 Kicking online telnet users

The system supports forcibly kicking off the online telnet login user function, please perform this operation in the privileged user view.

manipulate	command	clarification
Enter privileged user view	enable	
Kicking online telnet users	remote-stop *username*	

[Example]

! Eliminate telnet user test from online logins

<GPON>remote-stop test

Description:

- Only the system default admin user supports kicking out the online telnet user operation, the rest of the users do not support this operation.
- The stop operation takes effect only for telnet users, but not for serial port login users.

1.3 Managing the OLT Pathway

The system provides the following main management paths:

- Command Line Interface (CLI) to access the device via HyperTerminal
- Management system via Telnet
- Manage the system through a web browser, such as Internet Explorer.
- Management system via SNMP

1.3.1 Manage OLTs via serial port

Use HyperTerminal (or faux-terminal software) to connect to the Console port of the device so that you can access the system's command line interface (CLI) through HyperTerminal.

Setting method: In the interface of HyperTerminal, open the "File"->"Properties" menu, a window will pop up, enter the configuration, restore the default value, click the "Settings" tab. Click the "Settings" tab, select "Auto Detect" in the "Terminal Emulation" drop-down list, and then click [OK]. Once connected successfully, you can configure the device through the command line interface after seeing the operating system login interface in the terminal. The steps are as follows:

Step 1: Connect the device's Console port to the computer's serial port;

Step 2: Power up the device and wait for the system to boot up successfully, then you can see the login prompt message: Login.

Step 3: Enter the correct user name, press Enter, and then enter the appropriate password at the prompt. If this is the first time you are logging into the switch, you should log in using the default username admin, at which point you enter the login password admin to operate as the system administrator. If you have been assigned your own user name and password, then you can log in with your own user name and password;

Step 4: After successfully logging in the device, the system displays the following message:

GPON>

Step 5: As a system administrator, after entering the privileged user view, you can save the configuration with the save command

<GPON>save current-config

When the following message appears:

Config in flash will be updated, confirm to do this?(y/n)[n]:y

Start to do this, please wait...

Indicates that the system is saving the configuration, please wait, then prompt:

Save config successfully.

Indicates that the system saved the current configuration successfully.

The system boots up with the following message:

Prepare to restore config from flash, press CTRL+C to cancel or ENTER to run now: iphone.com.hk, iphone.com.hk, iphone.hk, iphone.com.hk

Entering Enter will enable the configuration saved in the above steps, and entering CTRL+C will restore the system's default configuration.

Step 6: The administrator user can use the timeout interrupt connection function in both normal user view and privileged user view. Type the command idle-timeout to permit the privileged user timeout to interrupt the connection for 20 minutes. the undo idle-timeout command sets the timeout to interrupt the connection to never time out.

Step 7: Once you have finished operating the device, type the command:

<GPON>quit

Exit the user interface.

1.3.2 OLT management via Telnet

Step 1: Establish the configuration environment by simply connecting your computer to the device's port over the network;
Step 2: Run the Telnet program on your computer;
Step 3: Power on the device, type the IP address of the device on the computer, establish a connection with the device, enter the login password that has been set according to the prompts, and then the command line prompt appears (e.g. GPON>). For security reasons, if there is no input within 1 minute after the command line prompt appears, the link will be disconnected after a timeout; if the user name and password are wrong 5 times in a row, the link will be disconnected; if the prompt "Sorry, session limit reached." appears, please connect again later (the system allows up to 5 telnet users to log in at the same time). (the system allows up to 5 telnet users to log in at the same time);
Step 4: Use the appropriate commands to configure the device system parameters or view the device operation status. To access the privileged user view, the user must have administrator-level privileges. Feel free to type "?" if you need help. for specific commands, please refer to the following chapters;
Step 5: To exit the telnet login, use the quit command to exit the login in normal user view, or use the quit command to exit the login step by step in other modes, and use "ctrl+]" to exit the login at any time. Alternatively, the system administrator can force the telnet logged in user to log out by using the remote-stop username command in privileged user view.

1.3.3 OLT management via WEB

Use a PC connected to the Ethernet port of the OLT to manage the OLT via a WEB page.
Step 1: Set up the configuration environment by connecting the PC to the device's port over the network;
Step 2: Configure an IP address on the OLT for management and maintenance purposes;
Step 3: Access the IP address of the OLT through a WEB browser on your computer, and then log in to manage the OLT with your username and password;

1.3.4 Managing OLTs via SNMP

Step 1: Set up the configuration environment by connecting the PC to the device's port over the network;
Step 2: Configure an IP address on the OLT for management and maintenance purposes;
Step 3: Manage the OLT through SNMP network management software on the computer, such as MIB Browser, connecting to the IP address of the OLT for management and configuration;

1.4 Remote authentication of administrative users

Users managing the OLT can be saved in the OLT local database or centrally stored in the RADIUS/TACACS+ server. users authenticate themselves to the RADIUS/TACACS+ server via the RADIUS/TACACS+ protocol when logging in. the system uses the local database by default.

After the authentication is passed, the user's privileges are ordinary user privileges by default, and the user's privileges are managerial privileges only if the returned Authentication Accepted RADIUS message contains the Service-Type field and the value of this field is Administrative.

In case of TACACS+ remote authentication, when the authorization operation is not used, the privilege after the authentication passes is the administrator privilege, while when the authorization operation is used, the privilege is determined by the priv_lvl returned by the remote server (if not returned then it is the administrator privilege), and the privilege is the normal user privilege if the authorization fails.

 Attention:

The admin user is a reserved user and only supports the local database authentication method.

1.4.1 Enabling RADIUS/TACACS+ Remote Authentication

The following command can be used in system view:

manipulate	command	clarification
Go to System View	system-view	
Enabling Radius/Tacacs Authentication	user-auth { local | { radius *radiusname* { pap | chap } [local] } } | { tacacs+ [author] [account] [local] }	Default is local authentication

You can configure the authentication method that uses only RADIUS/TACACS+ remote authentication or the authentication method that enables RADIUS/TACACS+ remote authentication first, and then uses the local database if there is no response due to the failure of the RADIUS/TACACS+ server connection or other reasons. The billing for TACACS+ is the start/end billing operation.

1.4.2 Show Authentication Method Configuration

You can execute the display command in any view to display the authentication method configuration.

manipulate	command	clarification
Viewing Authentication Method Configuration	display user-auth	

1.4.3 TACACS+ Remote Server Configuration

The Tacacs+ Remote Server can be configured under system view, as described in the following table:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Tacacs+ Remote Server	tacacs+ { priamary | secondary } server *ipaddress* [key *keyvalue*] [port *portnum*] [timeout *timevalue*]	The default value for port is 49 and the default timeout time is 5 seconds

1.4.4 Display TACACS+ configuration

Execute the display command in any view to display the authentication method configuration.

manipulate	command	clarification
View Tacacs+ Configuration	display tacacs+	

Chapter 2 OLT management and maintenance

2.1 System maintenance

2.1.1 View system status information

The system supports viewing the system status and system information through the display command, and the information is roughly divided into the following categories:

- Commands to Display System Configuration Information
- Commands that display the system's operational status
- Commands to display system statistics

You can use the display command to view the status and system information in any view. For other display commands related to the information of each function module, please refer to the related chapters. The following section includes only the display commands for system information.

manipulate	command	clarification
Display system version information	display version	Version information includes software and hardware version information, CPU model, device MAC address, device SN number, etc.
Displays logged-in administrative user information	display local-user	Displays information for configured administrative users
Display logged-in administrative user information	display login-users	Displayed as logged-in administrative user information, including login method and login time, etc.
Display system memory information	display memory	Displays total system memory and current remaining memory
Display system clock	display time	Displays the current system clock, including year, month, day, hour, minute, second, week, and time zone
Display system CPU utilization	display cpu-info	

[Example]

! Show system version

[GPON]display version

2.1.2 Setting the System Clock

The system supports setting the clock, including year, month, day, hour, minute and second. After the system clock is set, it will run according to the newly set clock and record the related log alarm information, etc. The related configurations are as follows:

manipulate	command	clarification
Enter privileged user view	enable	
Setting the System Clock	time HH:MM:SS YYYY/MM/DD	The system clock is not written to the configuration file as a configuration
Go to System View	system-view	
Setting the clock time zone	time zone name hour minute	
View system time	display time	

[Example]

! Setting the system clock to October 1, 2020 at 8:30:0 seconds

<GPON>time 08:30:0 2020/10/01

! Set clock time zone to Beijing time

[GPON] time zone CCT 8 0

2.1.3 Setting the system host name

The system supports setting the host name, and the related configurations are as follows:

manipulate	command	clarification
Enter privileged user view	enable	
Go to System View	system-view	
Configure the host name	sysname *sysname*	sysname is the system command line interface prompt string, the length of 1 to 32 characters, must be printable characters and can not contain '/',':','*','?' ,'\\\','<','>','|',"","" and so on.
Delete hostname	undo sysname	

[Example]

! Setting the command line interface prompt for a system as GPON-ABCD

[GPON]sysname GPON-ABCD

[GPON-ABCD]

2.1.4 Network Connection Ping Test Command

The system supports checking the network connection and whether the host is reachable through the ping command. The ping command can be executed from any view:

manipulate	command	clarification
Ping command test	ping [-c count] [-s packetsize] [-t timeout] host-ip	

[Parameter Description]

-c count: number of messages sent.

-s packetsize: is the length of the sent message in bytes.

-t timeout: the timeout, in seconds, to wait for a response after sending a message.

[Example]

! Find out if 192.168.0.100 is reachable

<GPON>ping 192.168.0.100

PING 192.168.0.100: with 32 bytes of data.

reply from 192.168.0.100: bytes=32 time<10ms TTL=127

reply from 192.168.0.100: bytes=32 time<10ms TTL=127

reply from 192.168.0.100: bytes=32 time<10ms TTL=127

reply from 192.168.0.100: bytes=32 time<10ms TTL=127

reply from 192.168.0.100: bytes=32 time<10ms TTL=127

----1 ----.168.0.100 PING Statistics----

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

round-trip (ms) min/avg/max = 0/0/0

2.1.5 Route Trace Tracert Test Command

The system supports route tracing and checking network connections through the tracert command. The tracert command can be executed from any view:

manipulate	command	clarification
tracert command test	tracert [-u | -c] [-p udpport | -f first_ttl | -h maximum_hops | -w time_out] target_name	

[Parameter Description]

-u: Indicates sending udp messages;

-c: Indicates to send echo message of icmp, default is -c mode;

-p udpport: destination port address for sending udp messages, value range 1-65535, default port 62929;

-f first_ttl: initial ttl value of the sent message, value range 1-255, default value is 1;

-h maximum_hops: the maximum to ttl value for sending messages, value range 1-255, default value is 30;

-w time_out: timeout for waiting for a response after sending a message, value range 10-60 seconds, default value is 10 seconds;

target_name: target host or router address

[Example]

! Trace the route through which 192.168.1.2 can be reached

<GPON>tracert 192.168.1.2

2.1.6 Port Loopback Test Command

The system supports the loopback test function for Ethernet ports, which is used to test the internal and external connectivity of Ethernet ports. The test is divided into two modes: inner loopback test and outer loopback test. For outer loopback test, the outer loopback cable must be plugged into the port (the transceiver cable of RJ45 is directly connected). When using the loopback command for testing, the port will not be able to forward packets correctly, and the loopback test will end automatically after a certain period of time. If the port executes the shutdown command, the loopback test cannot be performed. During the loopback test, the system will disable the operations of speed, duplex and shutdown on the port.

Use the following command in global mode or port view to perform a loopback test:

manipulate	command	clarification
Go to System View	system-view	
Loopback test on all ports	loopback { internal | external }	System view performs a loopback test on all ports. Port view tests the specified port.
Enter port view	interface { { ethernet interface-num } | interface-name }	
Loopback testing of individual ports	loopback { internal | external }	

 Attention:

- The outer ring RJ45 header must be unplugged immediately after the outer ring test is completed to avoid causing the device to loop resulting in abnormal communication;
- For 1000M Category 5 connections, use 8-core cables, and for 100M and below, use 4-core cables;

2.1.7 Line Detection VCT Command

VCT is used to detect Ethernet port cable normal (NORMAL), open circuit (OPEN), short circuit (SHORT), impedance mismatch (IMPEDANCE MISMATCH) and other errors. Normal connection of the network cable is NORMAL, the network cable is disconnected as OPEN, the network cable appears short-circuit SHORT, impedance mismatch (IMPEDANCE MISMATCH) is generally found in the two different impedance of the network cable is connected together. If an error is found, the location of the error can be detected. The system supports VCT automatic testing.

The VCT detection test command is as follows:

manipulate	command	clarification
Go to System View	system-view	
VCT for all ports	vct run	System view performs a VCT test on all ports. Port view performs a VCT test on the specified port.
Enter Ethernet port view	interface { { ethernet interface-num } | interface-name }	
VCT for individual ports	vct run	

[Example]

! Perform VCT on Ethernet port 1

[GPON-ethernet-0/1]vct run

 Description:

VCT detection is only performed for Category 5 cable Ethernet ports, and VCT detection for fiber optic ports is not supported.

2.1.8 Managing IP address restrictions

The management IP address restriction can restrict the IP address of the host or a certain network segment of the web, telnet, and snmp agent that logs into the OLT respectively, and other IP addresses outside the matching configuration cannot manage the device.

By default all 3 servers have an all-0 address segment, so users with any IP address can manage the switch. Different IP addresses or masks indicate different information. When the mask is 255.255.255.255, it indicates the host address, otherwise it indicates the network segment. Table entries with all 0s must be deleted first when enabling configuration. When the server receives a message, it determines whether the IP address belongs to the range of the management IP address, and discards the message if it does not, and closes the connection if it is telnet.

manipulate	command	clarification
Go to System View	system-view	
Configuring Management IP Address Limits	login-acl { web | snmp | telnet } *ip-address wildcard*	
Remove administrative IP address restrictions	undo login-acl { all | { web | snmp | telnet { all | *ip-address wildcard* } } }	The all parameter can be selected to delete all restriction table entries.
Display management IP address restriction configuration information	display login-acl	This display command can be executed in any view.

web indicates the IP address limit for web server access.

snmp indicates the access IP address limit for the snmp agent.

telnet indicates the IP address limit for telnet server access.

ipaddress is the IP address, wildcard is the IP address mask, using the inverse mask to indicate that 0 means masking this bit, 1 means not masking this bit, when wildcard is 0.0.0.0 indicates the host address.

[Example]

! Configure to allow only addresses in the 192.168.0.0/255.255.0.0 network segment to access the device via telnet

[GPON] login-acl telnet 192.168.0.1 0.0.255.255

[GPON]undo login-acl telnet 0.0.0.0 255.255.255.255.255

! Display the configuration for managing ip address restrictions

[GPON]display login-acl

 Attention:

Since there exists a default all-0 restriction table entry in the system, which indicates that it matches all IP addresses, if you need to use a new configuration table entry, you must first delete the system's default all-0 table entry; otherwise, all IP addresses can match the all-0 table entry, and all of them can still manage the device.

2.1.9 Login Privileged User View Telnet User Count Limitation

The system supports configuration of the maximum number of Telnet users allowed to enter the privileged user view at the same time. This feature limits the number of users that can log on via Telnet and enter the privileged user view at the same time. The number of users logging in via Telnet without entering the privileged user view is not limited, but is still subject to the maximum number of Telnet users allowed to log in to the system. Administrators and Super Users can always log in through the serial port and enter the Privileged User view without this limitation.

manipulate	command	clarification
Go to System View	system-view	

Configuring Login Privileged User View Telnet User Count Limits	telnet-server limit *limit-num*	The number of users is limited to 0-5, with 0 meaning that no telnet user is allowed to log into the privileged user view
Removing the Login Privileged User View Telnet User Count Limit	undo telnet-server limit	
To display login privileged user view Telnet user count limit configuration information	display telnet-server	This information can be viewed in any view, and the display contains information about the user limit configuration

[Example]

! Configure to allow only 2 Telnet users to enter the privileged user view at the same time

[GPON] telnet-server limit 2

2.1.10 CPU-CAR Commands

CPU-CAR is mainly used to set the rate at which the cpu receives messages to limit the number of messages sent to the CPU per second, to protect the CPU and prevent the CPU from being impacted by a large number of messages resulting in an overly busy system.

manipulate	command	clarification
Go to System View	system-view	
Configuring CPU-CAR	cpu-car target_rate	The cpu-car configuration range is 1-10000, and the default value is 600pps
Restore the default CPU-CAR value	undo cpu-car	
Show CPU-CAR Configuration	display cpu-car	This information can be viewed in any view

[Example]

! Set the rate at which the cpu receives messages to 100pps

[GPON]cpu-car 100

2.2 Configuration file management

2.2.1 Edit Configuration File

The configuration file is in text format and can be uploaded from the device to PC via FTP, TFTP protocols, please use text editing tools (such as windows notepad, etc.) to edit the uploaded configuration file.

By default, the system executes the configuration file in system view, so the configuration file will have the following two initial commands: "enable", "system-view". Each command should be followed by a carriage return line feed.

2.2.2 Modifying and saving the current configuration

Users can modify and save the current configuration of the system through the command line interface. In order for the current configuration to be used as the starting configuration for the next system startup, the current configuration needs to be saved. When the current startup configuration exists, execute the save configuration command, and the original startup configuration will be completely cleared and overwritten. Use this command in privileged user view.

manipulate	command	clarification
Enter privileged user view	enable	
Modifying and saving	save current-	This command modifies the startup configuration when the current

configuration files	config	startup configuration exists.

2.2.3 Erase Configuration

The system supports erasing configuration files that have been saved by the system. After erasing the saved configuration of the system, use the reboot command to reboot the system, and the system will be restored to the factory configuration after booting. Use this command in privileged user view.

manipulate	command	clarification
Enter privileged user view	enable	
Erase Configuration File	clear saved-config	

2.2.4 Executing a Saved Configuration

Users can restore the current configuration of the system to the saved configuration through the command line interface. In order to restore the current configuration to the saved configuration, you need to execute the saved configuration file with the command update current-config. When executing the configuration file, if you encounter a command that cannot be executed, you will be prompted with "[Line:xxxx]invalid: %s". If the command fails, it will prompt "[Line:xxxx]failed: %s". If the length of the command exceeds 512 characters, the command will not be executed, "[Line:xxxx]failed: too long command: "%s"" will be prompted and only the first 16 characters of the command will be displayed, ending with " ...". Where "xxxx" indicates the line number where the command is located, and "%s" indicates the command string. Non-executable commands include commands with syntax errors and commands with pattern mismatches. Please use this command in the privileged user view.

manipulate	command	clarification
Enter privileged user view	enable	
Executing a Saved Configuration	update current-config	

[Description]

Execution of the saved configuration is equivalent to the saved configuration file commands issued manually, the current running configuration of the system is not empty, but on the basis of the original running configuration, and then add the startup configuration file into the

2.2.5 Displaying Saved Configurations

You can view the system save configuration in any view.

manipulate	command	clarification
Show saved configurations	display saved-config [*module-list*]	If module-list is not selected, the contents of all configuration files are displayed. If module-list is selected, the corresponding module configuration is displayed.

[Example]

! Show all contents of configuration file

<GPON>display saved-config

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

<GPON>display saved-config garp oam

2.2.6 Display the current running configuration

The current running configuration of the system can be viewed in any view.

manipulate	command	clarification
Display the current running configuration	display current-config [*module-list*] [perlines *num*]	If module-list is not selected, the contents of all configuration files are displayed. If module-list is selected, the corresponding module configuration is displayed. perlines is used to specify the number of lines per screen to display the configuration.

[Example]

! Displays all configuration information for the current system

<GPON>display current-config

Display vlan-related configuration information in the current system! Displays vlan-related configuration information on the current system

<GPON>display current-config vlan

2.3 Load the upgrade program online

The system supports online upgrade of application programs and loading of configuration files through TFTP, FTP, and Xmodem download methods, i.e., downloading the corresponding upgrade files and configuration files to the device.

The system supports uploading configuration files, log files, and alarm information via TFTP and FTP, i.e., uploading system configuration, logs, alarms, and other information to the local server.

2.3.1 Uploading and downloading files via TFTP

Please execute the tftp upload download file command in privileged user view:

manipulate	command	clarification
Enter privileged user view	enable	
Uploading files	upload { configuration | info-center } tftp { inet | inet6 } *tftpserver-ip filename*	configuration is the system startup configuration file. info-center is the system log file. tftpserver-ip supports IPv4 and IPv6.
Download file operations	load { configuration | host | bootrom | cpld-image | http { private-key | server-certificate } | ont-image } tftp { inet | inet6 } *tftpserver-ip filename*	configuration is the system startup configuration file. host is the device upgrade host program. bootrom starts the bootrom program for the device. cpld-image is a cpld file. http is a web server related file. ont-image is the version upgrade file. tftpserver-ip supports IPv4 and IPv6.

Where tftpserver-ip is the IP address of the TFTP server, filename is the name of the file to be uploaded, filename cannot be a system reserved word (e.g., con cannot be used as a filename under windows operating system). Before entering the command, you should open the TFTP server and set the destination path of the file to be uploaded.

[Example]

! Upload the configuration file via TFTP, name the configuration file config.txt

<GPON>upload configuration tftp 192.168.1.100 config.txt

After a successful upload, the file config.txt in the computer with the IP address 192.168.1.100 saves the current configuration.

! Download the configuration file config.txt, via TFTP.

<GPON>load configuration tftp 192.168.1.100 config.txt

After a successful download and a reboot of the system, the system will use the new configuration file config.txt.

! Upload the log file via TFTP, name the log file log.txt

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

! Download the upgrade file host.bin via TFTP

<GPON>load host tftp 192.168.1.100 host.bin

After a successful download and reboot of the system, the newly downloaded application will run.

! Downloading bootrom program boot.bin via TFTP

<GPON>load bootrom tftp 192.168.1.100 boot.bin

2.3.2 Upload and download files via FTP

Please execute the tftp upload and download file command in privileged user view:

manipulate	command	clarification
Enter privileged user view	enable	
Uploading files	upload { configuration | info-center } ftp { inet | inet6 } *ftpserver-ip filename usename password*	configuration is the system startup configuration file. info-center is the system log file. ftpserver-ip supports IPv4 and IPv6.
Download file operations	load { configuration | host | bootrom | cpld-image | http { private-key | server-certificate } | ont-image } ftp { inet | inet6 *}ftpserver-ip filename usename password*	configuration is the system startup configuration file. host is the device upgrade host program. bootrom starts the bootrom program for the device. The bootrom is the bootrom program for the device. cpld-image is a cpld file. http is a web server related file. ont-image is the ONT version upgrade file. ftpserver-ip supports IPv4 and IPv6.

Where ftpserver-ip is the IP address of the FTP server, filename is the name of the file to be uploaded, the filename can not be a system reserved word (such as in the windows operating system con can not be used as a filename). username, userpassword for the FTP server to set up the user name and password. Before entering the command, you should open the FTP server and set the user name, password and the destination path of the file to be uploaded.

The following specific example assumes that the ip address of the FTP server is 192.168.1.100. First, open the FTP server on the computer, set up the file path, and set the user name and password to admin and 123 respectively.

[Example]

! Upload the configuration file via FTP, name the configuration file config.txt

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

After a successful upload, the file config.txt saves the current configuration.

! Download configuration file via FTP

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

After a successful download and a reboot of the system, the new configuration file config.txt will be used.

! Download the upgrade file host.bin via ftp

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

After a successful download and reboot of the system, the newly downloaded application will run.

! Upload the log file via FTP, name the log file log.txt

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

! Download the bootrom program boot.bin via FTP

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

2.3.3 Downloading files via Xmodem

The system supports downloading configuration files and upgrade files via Xmodem, configured as follows:

manipulate	command	clarification
Enter privileged user view	enable	
Download file operations	load { configuration | host | bootrom } xmodem	

After entering the command, select "Transfer" -> "Send File" in the menu of Hyper Terminal, in the pop-up "Send File" dialog box, enter the full path and file name in the "File Name" column, select Xmodem in the "Protocol" drop-down list, and then click the [Send] button. In the pop-up "Send File" dialog box, enter the full path and file name of the file in the "File Name" column, select Xmodem in the "Protocol" drop-down list, and then click the [Send] button. After successful download and reboot of the system, the new configuration file or host upgrade program will be used.

[Example]

! Downloading host programs via Xmodem

<GPON>load host xmodem

After inputting the command, select "Transfer" -> "Send File" in the menu of Hyper Terminal, in the pop-up "Send File" dialog box, enter the full path and file name in the "File Name" column, and select Xmodem in the "Protocol" drop-down list, and then [Send] button. In the pop-up "Send File" dialog box, enter the full path and file name of the file in the "File Name" column, select Xmodem in the "Protocol" drop-down list, and then [Send] button. After successful download and system restart, the new host program will run.

2.4 Reboot device

The system supports software reset for OLT and ONT, including immediate restart and timed restart functions. Automatic restart can be set for a specific time, such as restarting at the hour, minute and second of a certain year, month and day, or at the hour, minute and second of a certain day of the week, or it can be set to restart after a period of time of operation, and the related configurations are as follows:

manipulate	command	clarification
Enter privileged user view	enable	
Immediate OLT restart command	reboot	Enter the reboot command and go back to the car, it will prompt whether you need to reboot or not, choose Y then the system reboot immediately, choose N or do not choose to go back to the car directly, or do not choose to wait for 5 seconds after the reboot will be automatically abandoned.
Go to System View	system-view	
Setting up a timed restart of the OLT	auto-reboot { in { minutes *min* | hours hour} | at { *YYYY/MM/DD hh:mm:ss* | *hh:mm:ss* daily | *hh:mm:ss weekday* weekly } }	

Setting up a timed restart of ONT	auto-reboot-ont { [*pon-id* | *ont-id*] in { minutes *min* | hours hour} | at { *YYYY/MM/DD hh:mm:ss* | *hh:mm:ss* daily | *hh:mm:ss weekday* weekly } }	Restart all ONTs when pon-id and ont-id are not configured.
Eliminate timed reboot function	undo auto-reboot	

[Example]

! Setting up the system for a reboot on May 15th, 2015, 03:30:30

[GPON] auto-reboot at 03:30:30 2015/05/15

! Set the system to reboot every Monday at 03:30:30 am

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

 Attention:

- Auto restart OLT is restart control according to the system clock, so you need to confirm the current system clock when setting the auto restart function, the relevant settings are described in section 2.1.2.
- The auto-restart OLT configuration can be written to decompile, so be careful to clear this configuration in a timely manner if repeated restarts are not required.

2.5 Telnet Client Features

After logging in to the OLT through the serial port or telnet, users can log in to other devices or other standard Telnet servers through the Telnet client on the OLT.

Please use the Telnet client command with the following command in privileged user view or system view:

manipulate	command	clarification
Enter privileged user view	enable	
Logging in to an IP address using the telnet client function	telnet-client *ip-address* [*port-num*] [timeout *num*]	Support for privileged user view and system view using telnet client commands

ip-address is the IP address of the Telnet server.

port-num is the port number of the Telnet server, the default is 23.

[Example]

! Telnet to the other device via the device with IP address 192.168.1.100

<GPON>telnet 192.168.1.100

 Description:

- Only the system default admin user can forcibly terminate a running client program, the rest of the users do not support this operation.
- After the telnet client has logged in to another device, you can use the "Ctrl+]" keys to enter the "telnet>" view and then use quit to exit the telnet client directly.

Chapter 3 Port Configuration

3.1 Port Profile

The Ethernet ports of OLT support 10/100/1000Base-T, and the ports can work in half-duplex and full-duplex modes, which can negotiate with other network devices to determine the working mode and rate, and automatically select the most suitable working mode and rate, simplifying system configuration and management. The Gigabit optical port only supports 1000Mbps full-duplex rate mode. The 10 Gigabit optical port supports 1000M and 10000Mbps full duplex rate mode, while the PON port is fixed rate and does not support rate configuration.

3.2 Port Configuration

3.2.1 Port Related Configuration Task List

Configuring port-related characteristic parameters first requires entering the port view before you can configure the related attributes. In order to quickly and easily configure ports, the system provides an interface to configure a group of ports, which requires only one command entry to configure the port members of the entire group. This group exists dynamically, and a command to enter the group specifies which ports are currently included in the group, and the dynamic group is automatically cleared after you exit the configuration of the group. All commands under the port can be used under the port group. For a configuration command, if a port in the group fails to be configured, only an alarm is issued, and the configuration of subsequent ports is not affected. The list of major port configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enter port view	compulsory	3.2.2
Enter port group view	selectable	3.2.3
Open or close the specified port	selectable	3.2.4
Configure port duplex mode and rate	selectable	3.2.5
Configuring Port Priority	selectable	3.2.6
Configuring Port Descriptions	selectable	3.2.7
Enable or disable VLAN incoming packet filtering on the port	selectable	3.2.8
Configure the port's receive frame type	selectable	3.2.9
Enable or disable flow control for ports	selectable	3.2.10
Configure the port type	selectable	3.2.11
Configure the default VLAN ID for the port	selectable	3.2.12
Adding a port to a specified VLAN	selectable	3.2.13
Displaying port information	selectable	3.2.14
Display or clear port statistics	selectable	3.2.15

3.2.2 Enter port view

To configure a port, first enter port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	

interface-num: is the Ethernet port, expressed as device-num/slot-num/port-num, device-num indicates the stacking device number, the default is 0, and the range of values is 0 to 7, slot-num indicates the slot number, and the range of values is 0

to 1, and port-num indicates the port number in the slot. The range of values is 1 to 48.

Interface-name: A combination of the port type abbreviation (e.g., Ethernet port, which can be ethernet or any consecutive character from e) and the port number (same as interface-num), e.g., Ethernet port 0/0/2, which can be e0/0/2 or ethernet 0/0/2.

3.2.3 Enter the port group view

You can enter the Ethernet port group view as follows:

manipulate	command	clarification
Go to System View	system-view	
Enter port group view	interfacerange { { ethernet *interface-list* } | *interface-name* }	interface-list represents multiple ports, consecutive ports of the same type can be connected by "to", but the port number immediately before "to" must be smaller than the port number immediately after "to". The port number immediately before "to" must be smaller than the port number immediately after "to", and this form can be repeated up to 3 times.

[Example]

! Enter Ethernet interface group view, this group includes Ethernet 1~3

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

[GPON-port-range]

3.2.4 Open or close the specified port

After the system starts, all ports are open by default. The status of each port can be configured according to actual needs. Use the following commands to open or close the current port in port view:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Shut down the port	shutdown	
Open the port	undo shutdown	

[Example]

! Open Ethernet port 1

[GPON-ethernet-0/0/1]undo shutdown

! Shut down Ethernet port 1

[GPON-ethernet-0/0/1]shutdown

3.2.5 Configuring Ethernet Port Duplex Mode and Speed

By default, the operating mode of the Gigabit power ports is self-negotiation. Users can also set them manually. The speed can be configured with the speed command and the operating mode with the duplex command.

The 10 Gigabit optical port supports 1000Mbps and 10000Mbps rates and only full duplex mode.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring Port Rate Mode	speed { 10 | 100 | 1000 | 10000 | auto }	
Restore port rate mode	undo speed	

Configuring Port Duplex Mode	duplex { full | half }	

[Example]

! Set Ethernet port 1 to 100M full duplex mode

[GPON-ethernet-0/0/1] speed 100

[GPON-ethernet-0/0/1]duplex full

3.2.6 Configuring Port Priority

The port has 8 priority levels from 0 to 7. The default port priority is 0. The higher the priority value, the higher the priority, then the data messages received by this port will be processed more quickly. If a port is connected to a device that handles more data or handles more urgent data, then you can set the priority of this port to high priority.

Configure it in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring Port Priority	priority priority-num	
Restore port default priority	undo priority	

3.2.7 Configuring Port Descriptions

The following commands can be used to describe the ports as necessary to distinguish between individual ports.

Please configure it in Ethernet port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring Port Descriptions	description description-list	
Delete port description	undo description	

[Example]

! Configure the description of Ethernet port 3 as port-3

[GPON-ethernet-0/0/3] description port-3

! Displays the port description for Ethernet port 3

[GPON]display description interface ethernet 0/0/3

3.2.8 Enable or disable VLAN incoming packet filtering on the port

When the port's VLAN packet filtering function is enabled, 802.1Q packets received by the port that do not belong to the port's VLAN will be dropped. When this feature is disabled, the packets are not dropped.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable port VLAN incoming	ingress filtering	VLAN incoming packet filtering is enabled on

packet filtering		the port by default
Disable port VLAN incoming packet filtering	undo ingress filtering	

[Example]

! Turn on VLAN input filtering on Ethernet port 5

[GPON-ethernet-0/0/5]ingress filtering

! Disable VLAN input filtering on Ethernet port 5

[GPON-ethernet-0/0/5]undo ingress filtering

3.2.9 Configure the port's receive frame type

Configuring the Receive Frame Type of a Port Allows the port to receive all types of messages or only tagged type messages.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Setting the port frame reception type	ingress acceptable-frame { all | tagged }	
Cancel the port frame reception type setting	undo ingress acceptable-frame	The default frame reception type for the port is all

[Example]

! Setting Ethernet port 5 to receive only tagged messages

[GPON-ethernet-0/0/5]ingress accetable-frame tagged

3.2.10 Enable or disable flow control for ports

If the incoming traffic of a port is relatively large, it needs to be controlled to avoid causing network congestion and loss of packets. After enabling the port flow control function, when the outgoing port is congested with packets, the device generates a flow control Pause frame to discover the upstream device, informing the peer device that there is a packet congestion on this device, and the peer device, if it supports the flow control function, reduces the rate of packet sending until the congestion ends.

Use the following commands in port view to turn on or off the flow control function for the current port:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable port flow control	flow-control	
Disable port flow control	undo flow-control	
Display Port Flow Control Function	display flow-control interface [ethernet *interface-num*]	When no port number is specified, the flow control configuration for all ports is displayed

[Example]

! Turn on flow control for Ethernet port 5

[GPON-ethernet-0/0/5] flow-control

! Disable flow control on Ethernet port 5
[GPON-ethernet-0/0/5]undo flow-control
! Displays the flow control status of Ethernet port 5
[GPON-ethernet-0/0/5]display flow-control interface ethernet 0/0/5

3.2.11 Configure the port type

There are three types of ports: trunk, hybrid and access. Trunk ports are all tagged in the VLAN to which they belong, and messages sent through them are all tagged; hybrid ports can be either tagged or untagged in the VLAN to which they belong, and messages sent from VLANs with tagged status are all tagged, while messages sent from VLANs with untagged status are not tagged; access ports can only belong to one VLAN, and the VLANs with untagged status are not tagged; access ports can only belong to one VLAN. VLANs in the tagged state send messages with tag headers, while VLANs in the untagged state send messages without tag headers; access ports can only belong to one VLAN, which is the default VLAN for the port and is in the untagged state in that VLAN.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Setting the Port Type	port mode { trunk | hybrid | access }	
Restore port default type	undo port mode	The default type of port is Hybrid

[Example]
! Setting Ethernet port 1 as trunk port
[GPON-ethernet-0/0/1] port mode trunk

3.2.12 Configure the port's default VLAN ID

Each port has a default confirmed VLAN ID, also called port PVID. When a message enters the port without a VLAN, the port sends this message to be forwarded within the VLAN identified by the default VLAN ID. message sending and receiving follow the IEEE 802.1Q standard. The default default VLAN ID value of the device is 1. Please configure the default VLAN ID under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Set the port default vlan id	port default *vlanvlan-id*	The value of vlan-id ranges from 1 to 4094.
Restore port default vlan id	undo port default vlan	The default default VLAN for the port is 1

[Example]
! Set the default VLAN ID of port Ethernet0/1 to 5
[GPON-ethernet-0/0/1] port default vlan 5

3.2.13 Add the port to the specified VLAN

In port view, you can join a port to a specified VLAN.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the port mode to access	port mode access	
Add the Access port to the specified vlan	port default vlan *vlan-id*	Access ports can only be in one VLAN, so set the port's default VLAN to add the access port to the specified VLAN.
Configure the port mode to Hybrid	port mode hybrid	
Add the Hybrid port to the specified vlan and set it to the tagged attribute	port hybrid tagged vlan { all | *vlan-list* }	You can join specific VLANs, or join to all VLANs, and these VLANs are tagged out on the outgoing ports.
Add the Hybrid port to the specified vlan and set it to the untagged attribute	port hybrid untagged vlan { all | *vlan-list* }	You can join specific VLANs, or join to all VLANs, and these VLANs are untagged out of the port.
Remove the Hybrid port from the specified vlan	undo port hybrid vlan { all | *vlan-list* }	
Configure the port mode to Trunk	port mode trunk	
Add the Trunk port to the specified vlan	port trunk allowed vlan { all | *vlan-list* }	
Remove trunk ports from a specified VLAN	undo port trunk allowed vlan { all | *vlan-list* }	

 Description:

There are two ways to join a port to an enforced VLAN, one is to configure it under port view by joining the port to the specified VLAN. The other is in VLAN view, where the port is directly joined to that VLAN (see VLAN Configuration in Chapter 3).

3.2.14 Displaying port information

You can use the command display interface ethernet [interface-num] to display information about a specified port or all ports. The port display information mainly includes the following (including but not limited to the following):

- Port enable status (port open or closed, enable means open)
- Port connection status (port linkup, or linkdow)
- Port rate and mode of operation (set and actual rate and duplex status of the port)
- Port Default VLAN ID
- port priority
- Port type (trunk, hybrid or access port)
- Port VLAN information (VLAN where the port is located and tagged/untagged attributes of the

outgoing VLAN port)

- Port Message Statistics
- Port SFP Module Information

In any view mode, view the port information by using the command display command.

manipulate	command	clarification
Displaying port information	display interface [ethernet *interface-num*]	When a port number is specified, the specified port information is displayed, and when no port is specified, all port information is displayed.
Display all port summary information	display interface brief	
Display port sfp information	display interface sfp [ethernet *interface-num*]	When a port number is specified, the specified port SFP module information is displayed, and when no port is specified, all port SFP module information is displayed.

3.2.15 Display and clear port statistics

You can display the following information for a specified port or all ports with the command display statistics in either mode:

- Number of 64-byte messages
- Number of 65 to 127 byte messages
- Number of 128 to 255 byte messages
- Number of 256 to 511 byte messages
- Number of 512 to 1023 byte messages
- Number of 1024 to 1518 byte messages
- Total messages received
- Total bytes received
- Number of messages discarded in the receive direction
- Number of unicast messages received
- Number of multicast messages received
- Number of broadcast messages received
- Number of error messages received
- Number of FCS error messages received
- Number of data symbol error messages received
- Number of false carriers detected
- Number of ultra-small messages received (less than 64 bytes)
- Number of oversized messages received (greater than 1518 bytes)
- Number of frames received for streaming
- Total messages sent
- Total bytes sent
- Number of messages discarded in the send direction
- Number of unicast messages sent
- Number of multicast messages sent
- Number of broadcast messages sent
- Number of error messages sent
- Number of messages delayed

- Number of collisions
- Number of late collisions

manipulate	command	clarification
Display port statistics	display statistics interface [ethernet *interface-num*]	When a port number is specified, the specified port statistics are displayed. When no port is specified, all port statistics are displayed.
Displaying All Port Statistics in a Nutshell	display statistics interface brief	
Displays real-time send/receive rates and bandwidth utilization for all ports	display utilization interface	
Go to System View	system-view	
Clear port statistics in system view	clear interface [ethernet *interface-num* }]	When a port number is specified, clears the specified port statistics. When no port is specified, all port statistics are cleared.
Enter port view	interface { { ethernet interface-num } | interface-name }	
Clear port statistics in port view	clear interface	Clear only the port statistics

Chapter 4 port mirroring

4.1 Introduction to Port Mirroring

The system provides port-based mirroring function, which can copy messages from one or more specified ports to different monitoring ports for message analysis and monitoring. The system supports up to 4 mirroring destination ports, and can copy messages from different ports to different mirroring ports. The system also supports CPU port mirroring, which can copy messages received and sent by CPU ports to the specified monitoring ports. For example, messages from Ethernet port 0/0/1 and CPU port can be copied to Ethernet port 0/0/2 of the specified monitoring port, and messages from Ethernet port 0/0/3 can be copied to Ethernet port 0/0/4 of the specified monitoring port, which can be tested and analyzed and monitored by the protocol analyzer connected to the mirrored destination ports 0/0/2 and 0/0/4.

4.2 Port Mirroring Configuration

4.2.1 Port Mirroring Configuration Task List

Port mirroring is configured in the form of a group. the mirrored source port messages in the same group are copied to the mirrored destination port in the same group. the port mirroring-related configuration tasks are as follows.

Configuration tasks	clarification	Detailed Configuration
Configuring the Mirror Destination Port	compulsory	4.2.2
Configuring the Mirror Source Port	compulsory	4.2.3
Display of port mirroring	selectable	4.2.4

4.2.2 Configuring the Mirror Destination Port

The mirrored destination port is configured as follows:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Mirror Destination Port	mirror group *group-id* destination-interface ethernet *interface-num*	group-id indicates the mirroring group, port mirroring is configured in the form of a group, and the mirrored source port messages in the same group will be copied to the mirrored destination port in the same group.
Delete the mirrored destination port	undo mirrorgroup { all | *group-id* destination-interface ethernet *interface-num* }	When the parameter all is selected, all mirror groups are deleted.

4.2.3 Configuring the Mirror Source Port

The mirrored source ports are configured as follows:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Mirror Source Port	mirror group *group-id* source-interface { ethernet | cpu } *interface-list* { both | egress | ingress }	both represents mirroring both ingress and egress of a port, egress represents mirroring egress of a port, and ingress represents mirroring ingress of a port. interface-list represents one or port Ethernet port.

Delete the mirrored source port	undo mirror group { all | *group-id* source-interface { cpu | *interface-list* } }	When the parameter all is selected, all mirror groups are deleted.

[Example]

! Configure Ethernet ports 1 and 2 as mirrored ports

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

4.2.4 Show port mirroring

You can view port mirroring information in any view mode by using the command display command.

manipulate	command	clarification
Display port mirroring information	display mirror group { all | *group-id* }	When group-id is specified, a single mirror group configuration is displayed, and when all is specified, all mirror group configurations are displayed.

[Example]

! Show mirrored port settings

<GPON>display mirror group all

Chapter 5 port aggregation

5.1 Introduction to Port Aggregation

The OLT device supports the Ethernet port aggregation function.

Port aggregation is the aggregation of multiple Ethernet ports together to form an aggregation group to achieve traffic load sharing among the member ports. When a link is unavailable, the traffic on that link is automatically switched to another link, thus ensuring uninterrupted service traffic, and an aggregation group is like a port.

The basic port aggregation configurations are:

- Supports static and dynamic aggregation channel groups, aggregation groups support up to 8 port members in each group. Each group is defined as a channel group, and the command line is configured around this channel group.
- It supports configuring global load balancing policy and load balancing policy for source MAC, destination MAC, source and destination MAC, source IP, destination IP, source and destination IP, and the default load balancing policy is source MAC.
- It supports configuring the LACP priority of systems and ports, which is mainly used for dynamic aggregation when both sides of the interconnected devices negotiate the aggregation master and slave ports based on the priority. The default system priority is 32768 and the default port priority is 128.

5.2 Port Aggregation Configuration

5.2.1 Port Aggregation Configuration Task List

The list of port aggregation configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Configure/delete aggregation groups	compulsory	5.2.2
Adding/deleting convergence group members	compulsory	5.2.3
Configuring an Aggregation Group Load Balancing Policy	selectable	5.2.4
Configuring LACP Priority	selectable	5.2.5
Display LACP configuration information	selectable	5.2.6
Clearing Aggregation Group Statistics	selectable	5.2.7

5.2.2 Configure/delete aggregation groups

Port aggregation group configuration and deletion are as follows. please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Configuring an Aggregation Group	channel-group channel-group-number	channel-group-number is 0 to 7.
Deleting an aggregation group	undo channel-group channel-group-number	

[Example]

! Create a converged channel group with index 0

[GPON]channel-group 0

5.2.3 Adding/deleting convergence group members

Port aggregation group members are added and deleted as follows. please configure them in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port or port group view	interface [range] { { ethernet *interface-num* } | *interface-name* }	You can enter port group view and add or delete multiple aggregation group members in one configuration
Configuring an Aggregation Group	channel-group *channel-group-number* mode { active | passive | on }	When an aggregation group member port is in on mode, it can only interface with on mode. Both ends of an aggregation group cannot work in passive mode at the same time.
Deleting an aggregation group	undo channel-group channel-group-number	

[Example]

! Add Ethernet port 3 to the third channel and specify this port in active mode.

[GPON-ethernet-0/0/3] channel-group 3 mode active

! Remove Ethernet port 3 from the third channel.

[GPON-ethernet-0/0/3]undo channel-group 3

Description:

Add an aggregation group member under port view to add the current port to the aggregation group and specify the aggregation group mode for this port. If the specified aggregation channel is not previously configured, the system automatically creates this aggregation group.

5.2.4 Configuring an Aggregation Group Load Balancing Policy

The system supports globally configured load balancing policies, and all aggregation groups support only the same configured load balancing policy. That is, all configured aggregation groups use the same load balancing policy.

manipulate	command	clarification
Go to System View	system-view	
Configuring an Aggregation Group Load Balancing Policy	channel-group load-balance { dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac }	The system defaults to the src-mac policy

[Example]

! Configure the load balancing policy as the destination MAC

[GPON]channel-groupload-balance dst-mac

5.2.5 Configure the LACP priority of the system

The system supports global and port configuration of LACP priority with the following configuration commands:

manipulate	command	clarification
Go to System View	system-view	
Configure the global LACP priority	lacp system-priority *system-priority-value*	system-priority-value ranges from 1 to 65535, and the default value is 32768.

Restore the default global LACP prioritization	undo lacp system-priority	
Enter port or port group view	interface [range] { { ethernet *interface-num* } | *interface-name* }	You can enter port group view and configure multiple aggregation group members at once
Configure the LACP priority of the port	lacp port-priority *port-priority-value*	port-priority-value ranges from 1 to 65535, and the default value is 128.
Restore the default port LACP priority	undo lacp port-priority	

[Example]

! Configure the system LACP priority to 4096.

[GPON]lacp system-priority 4096

! Configure the LACP priority of Ethernet port 2 to 12345.

[GPON-ethernet-0/0/2] lacp port-priority 12345

5.2.6 Display LACP configuration information

In any view mode, view LACP-related configuration information, including system lacp id information, aggregation group local information, aggregation group neighboring port information, and aggregation group statistics by using the display command.

manipulate	command	clarification
Display the lacp id of the system	display lacp sys-id	The system id consists of a 16-bit system priority and a 48-bit system MAC address
Display aggregation group local information	display lacp internal [*channel-group-id*]	When channel-group-id is not specified, all aggregation groups are displayed.
Display aggregation group neighbor port information	display lacp neighbor [*channel-group-id*]	When channel-group-id is not specified, display information about the neighboring ports of all aggregation groups.
Display aggregation group statistics	display statistics channel-group [*channel-group-id*]	Similar to displaying port statistics, when channel-group-id is not specified, all aggregation group statistics are displayed.
Dynamic display of all aggregation group statistics	display statistics dynamic channel-group	
Real-time display of send/receive rates and bandwidth utilization for all aggregation groups	display utilization channel-group	

[Example]

! Displays port-by-port membership information for channel 2

<GPON>display lacp internal 2

5.2.7 Clearing Aggregation Group Statistics

The system supports the function of clearing aggregation group statistics with the following configuration commands:

manipulate	command	clarification
Go to System View	system-view	

Clearing Aggregation Group Statistics	clear channel-group [*channel-group-id*]	Similar to clearing port statistics, if channel-group-id is not specified, all aggregation group statistics are cleared.

[Example]

! Clear the statistics for channel 2

[GPON]clear channel-group 2

Chapter 6 Port isolation

6.1 Introduction to Port Isolation

The system supports configuring port isolation, which is used to prohibit user ports from communicating with each other. In addition, configuring port isolation also prevents broadcast storms between user ports.

6.2 Port Isolation Configuration

6.2.1 Port Isolation Configuration Task List

The list of port isolation configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Add/Remove Isolated Ports	compulsory	6.2.2
Display Port Isolation Configuration	selectable	6.2.3

6.2.2 Add/remove uplink ports

The port configured as the uplink port can only send messages to the uplink port and cannot forward them to other ports. Setting two ports to be uplink ports for each other can realize isolation from all other ports. The related configurations are as follows:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface range *interface-list*	
Creating Port Uplinks	port-isolation uplink { ethernet | gpon } *interface-num*	interface-list represents multiple ports, consecutive ports of the same type can be connected with "to".
Delete port uplink	undo port-isolation [uplink { ethernet | gpon } *interface-num*]	Deleting an entire group without the port parameter

6.2.3 Display Port Isolation Configuration

You can view the port isolation configuration in any view

manipulate	command	clarification
Viewing Port Isolation Configuration	display port-isolation [ethernet *interface-list*]	When the port number is not specified, it means to view the isolated configuration of all ports

[Example]

! View all port isolation configurations

[GPON]display port-isolation

Chapter 7 Port Storm Suppression

7.1 Introduction to Port Storm Suppression

The system supports the configuration of storm control, which is used to limit the forwarding rate of broadcast, multicast, and unknown unicast messages received by a port to ensure that such unknown messages do not flood the network too much, and is used to optimize the network environment.

The system supports different rates of storm suppression based on broadcast, multicast, and unknown unicast messages respectively, i.e., different types of storm messages support the configuration of different storm suppression rate values.

7.2 Port Storm Suppression Configuration

7.2.1 Port Storm Suppression Configuration Task List

The port storm suppression configuration tasks are as follows:

Configuration tasks	clarification	Detailed Configuration
Add/Remove Port Storm Suppression	compulsory	7.2.2
Show Port Storm Suppression Configuration	selectable	7.2.3

7.2.2 Configure/remove port storm suppression

Storm control can be configured with the Storm-control command, configured as follows:

manipulate	command	clarification
Go to System View	system-view	
Enter port group view	interface [range] { { ethernet *interface-list* } | *interface-name* }	You can enter group port mode to configure storm suppression for multiple ports at once
Configuring Port Storm Suppression	storm-control { broadcast | multicast | unicast } { disable | pps *target-rate* } }	A setting of disable indicates that the port does not perform storm suppression. Corresponding to GE ports, the storm suppression range is 64-1488100. Corresponding to 10GE ports, the storm suppression range is 64-14881000.
Remove port storm suppression	undostorm-control { broadcast | multicast | unicast }	

[Example]

! Configure broadcast storm suppression on port e0/0/1 with a rate limit of 64pps

[GPON-ethernet-0/0/1]storm-control broadcast pps 64

! Configure unknown unicast storm suppression on port e0/0/1 with a rate limit of 128pps

[GPON-ethernet-0/0/1] storm-control unicast pps 128

7.2.3 Show Port Storm Suppression Configuration

You can view the port storm suppression configuration in any view

manipulate	command	clarification
Viewing Port Storm Suppression Configuration	display storm-control interface [ethernet *interface-list*]]	When no port number is specified, it means to view the storm suppression configuration for all ports

Chapter 8 VLAN Configuration

8.1 Introduction to VLANs

GPON OLT device, can be simply understood as a switch device plus a combination of GPON access device, OLT VLAN configuration operation, is mainly divided into two parts: one part for the switching chip VLAN configuration, that is, the contents of this chapter, including the principle of VLAN and configuration process; the other part of the GPON part of the VLAN configuration of the ONT, see the second half of the operating instructions for this operation manual The other part is the VLAN configuration of GPON part to ONT, please see the introduction of GPON CTC VLAN configuration part in the latter half of this operation manual.

8.1.1 VLAN Overview

VLAN (Virtual Local Area Network) is a technology that enables virtual workgroups by logically rather than physically dividing devices on a LAN into segments.The IEEE issued a draft standard for the IEEE 802.1Q protocol in 1999 to standardize the implementation of VLANs.

Traditional Ethernet is a broadcast network, all hosts in the network are connected through HUBs or switches and are in the same broadcast domain.HUBs and switches, as the basic devices for network connection, have some limitations in forwarding function: HUBs are physical layer devices without switching function, and the received messages will be forwarded to all ports except the receiving port; switches are data link layer devices with the capability of forwarding according to the destination MAC address of the message, but when receiving broadcast messages or unknown unicast messages (the destination MAC address of the message is not in the MAC address table of the switch), it will also be forwarded to the port except the receiving port. The switch is a data link layer device with the ability to forward messages according to the destination MAC address of the message, but when it receives a broadcast message or an unknown unicast message (the destination MAC address of the message is not in the MAC address table of the switch), it will also forward the message to all ports except the receiving port.

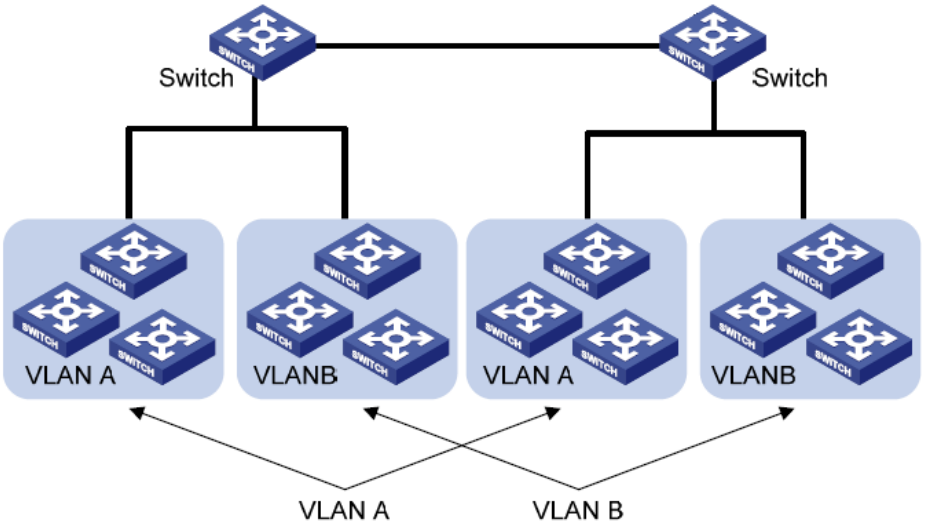
The above situation can cause the following network problems:

There may be a large number of broadcast and unknown unicast messages in the network, wasting network resources. Hosts in the network receive a large number of messages that are not destined for them, creating a serious security risk.

The fundamental solution to the above network problems is to isolate the broadcast domain. The traditional method is to use a router, because a router forwards messages based on the destination IP address and does not forward link-layer broadcast messages. However, routers are expensive and have fewer ports to carefully segment the network, so using routers to isolate broadcast domains has significant limitations. In order to solve the problem of Ethernet switches' inability to restrict broadcasts in LANs, VLAN (Virtual Local AreaNetwork) technology came into being.

VLAN technology allows network administrators to logically divide a physical LAN into different broadcast domains (or VLANs), each of which contains a group of computer workstations with the same requirements and the same attributes as the physically formed LAN. However, because it is logically rather than physically divided, individual workstations within the same VLAN do not have to be placed in the same physical space. Broadcast and unicast traffic within a VLAN is not forwarded to other VLANs, which helps control traffic, reduce equipment investment, simplify network management, and improve network security.

VLAN networking diagram:



8.1.2 VLAN Benefits

VLANs offer the following advantages over traditional Ethernet:

1. VLANs help control traffic

In traditional networks, large amounts of broadcast data are sent directly to all network devices, whether or not they are necessary, resulting in network congestion. VLANs, on the other hand, can set which devices that must communicate with each other are included in each VLAN, thereby reducing broadcasts and improving network efficiency.

2. VLANs provide higher security

Devices in each VLAN can only communicate with devices in the same VLAN. For example, if a device in the R&D VLAN must communicate with a device in the Production VLAN, it must do so through a routing device. In this way, the two departments cannot communicate directly, thus improving system security.

3. Flexible creation of virtual workgroups

Using VLANs, you can create virtual workgroups that span a physical network range, allowing users to access the network without changing the network configuration when their physical location moves within the virtual workgroup range.

8.1.3 VLAN Principle

1.VLAN Tag

In order to enable devices to distinguish between messages of different VLANs, it is necessary to add a field identifying the VLAN at the data link layer of the message, and the IEEE issued a draft standard of the IEEE 802.1Q protocol to standardize the implementation of VLANs in 1999, which provides a unified specification of the structure of the message with a VLAN tag.

Traditional Ethernet data frames encapsulate the upper layer protocol type field after the destination MAC address and source MAC address.

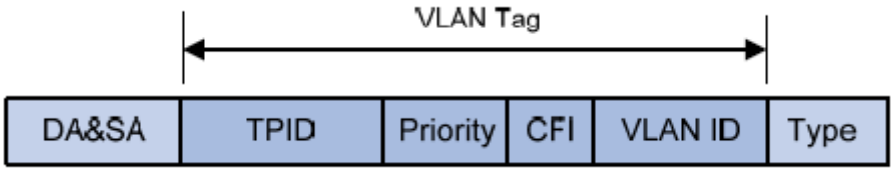
The following figure shows the traditional Ethernet frame encapsulation format:

where DA denotes the destination MAC address, SA denotes the source MAC address, and Type denotes the type field of the upper layer protocol.

The IEEE 802.1Q protocol specifies that a 4-byte VLANTag is encapsulated after the destination MAC address and the

source MAC address to identify information about the VLAN.

The constituent fields of the VLAN Tag:



As shown above, the VLAN Tag contains four fields, TPID (Tag Protocol Identifier), Priority, CFI (Canonical Format Indicator), and VLAN ID.

- TPID: Used to identify this data frame as data with VLAN Tag. The length of this field is 16bit and the default value is 0x8100 as specified by the protocol.
- Priority: Used to indicate the priority of 802.1P. The length of this field is 3 bits, please refer to the "QoS" section of this manual for the related introduction and application.
- CFI: Used to identify whether the MAC address is encapsulated in standard format. The length of this field is 1 bit, a value of 0 means that the MAC address is encapsulated in standard format, and a value of 1 means that it is encapsulated in non-standard format, the default value is 0.
- VLAN ID: The number of the VLAN to which the message belongs. The length of this field is 12 bits, and the range of values is 0 to 4095. Since 0 and 4095 are not usually used, the range of values for VLAN ID is usually 1 to 4094.

Description:

The frame format here is based on Ethernet II encapsulation for example, Ethernet also supports 802.2/802.3 encapsulation. For 802.2/802.3 encapsulation, the VLAN Tag is also encapsulated after the destination MAC and source MAC address fields.

2. MAC address learning mechanism for VLANs

The device forwards messages based on the destination MAC address of the message, so the device maintains a forwarding table that records the correspondence between the MAC address and the port to guide the device in forwarding, and this table is called the MAC address forwarding table. The device records the source MAC address and the receive port of the received message into this table for subsequent message forwarding, and this recording process is called the MAC address learning process.

After the VLAN is configured, the MAC address learning method of the device is divided into two types:

- SVL (Shared VLAN Learning): The device records all the MAC address table entries learned by the ports in all VLANs in a shared MAC address forwarding table, and the messages received from any port in any VLAN are forwarded with reference to the information in this table.
- IVL (Independent VLAN Learning): The device maintains an independent MAC address forwarding table for each VLAN. The source MAC address of a packet received by a port in a VLAN is recorded in the MAC address forwarding table of that VLAN, and the packet is forwarded only based on the information in the table.

This OLT device supports IVL learning mode.

8.1.4 VLAN Layer 3 interface

Hosts between different VLANs cannot communicate directly and need to be forwarded through network layer devices such as routers or Layer 3 switches. This OLT device supports the function of Layer 3 forwarding of messages by configuring VLAN interfaces.

A VLAN interface is a virtual interface in Layer 3 mode, which is mainly used to realize Layer 3 interworking between VLANs, and it does not exist on the switch as a physical entity. Each VLAN corresponds to a VLAN interface, which can forward messages received by ports in this VLAN at the network layer according to their destination IP addresses. Normally, since VLANs can isolate broadcast domains, each VLAN also corresponds to an IP segment, and the VLAN interface will act as a gateway for the segment to perform Layer 3 forwarding based on IP addresses for messages that need to be forwarded across the segment.

8.1.5 VLAN Type

VLANs can be categorized into five common types based on how they are segmented:

- Port-based VLANs
- MAC address-based VLAN
- Protocol-based VLANs
- VLANs based on IP subnets
- IP multicast based VLANs

The device supports VLANs based on port, MAC address, protocol type, and IP subnet.

8.2 Port-based VLAN Configuration

8.2.1 Port-based VLAN Configuration Task List

Configuration tasks	clarification	Detailed Configuration
Create/Delete VLANs	compulsory	8.2.2
Add/remove VLAN ports	compulsory	8.2.3
Specify/delete VLAN descriptors	selectable	8.2.4
Setting the Port Type	selectable	8.2.5
Configure the port default VLAN ID	selectable	8.2.6
Configuring Hybrid Port Tag vlan	selectable	8.2.7
Display VLAN information	selectable	8.2.8

8.2.2 Create/Delete VLANs

VLAN creation and deletion configuration operations, as shown below:

manipulate	command	clarification
Go to System View	system-view	
Create a single VLAN and enter VLAN view	vlan vlan-id	By default, the system has only one default VLAN 1, with a vlan-id range of 1 to 4094
Batch creation of multiple VLANs	vlan vlan-list	The composition of a vlan-list can be discrete numbers, consecutive segments of numbers, or a mixture of discrete and consecutive representations, where discrete

		numbers are separated by commas and segments of numbers are represented by minus signs, e.g., 2,5,8,10-20
Delete the specified VLAN	undo vlan *vlan-id*	
Batch Delete VLANs	undo vlan *vlan-list*	
Delete all VLANs	undo vlan all	

[Parameter Description]

The system supports the creation of 4094 VLANs, and the allowable configurable vlan-id range is from 1 to 4094.When creating a VLAN, if the VLAN already exists, it will enter the VLAN view directly; if the VLAN does not exist, this configuration task will create the VLAN first, and then enter the VLAN view. For example, if VLAN 2 has not been created, the system will automatically create VLAN 2 first and then enter VLAN view; if VLAN 2 already exists, it will enter VLAN view directly.

When deleting a VLAN, if vlan-list is specified, the corresponding VLAN is deleted. if all is selected, all created VLANs other than the default VLAN are deleted.

[Example]

! Create VLAN 2-100

```
[GPON]vlan 2-100
```

Attention:

- VLAN1 is the system's default VLAN and does not need to be created and cannot be deleted.
- If the VLAN to be deleted is the default VLAN ID of the port, the deletion of this VLAN is not allowed; if you need to delete it, you can modify the default VLAN of the port to other values first and then delete this vlan.
- When you use the vlan command to create a VLAN, if the target VLAN already exists and is a dynamic VLAN, the device automatically converts it to a static VLAN.
- If a multicast group exists in the VLAN, the deletion fails and the multicast group should be deleted before the VLAN can be deleted.

8.2.3 Add/remove VLAN ports

Ports are added within a VLAN and can be added and deleted in two ways, either in VLAN view, or in port view, adding or deleting VLANs:

VLAN view adds and removes VLAN ports:

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN view	vlan vlan-list	The composition of a vlan-list can be discrete numbers, consecutive segments of numbers, or a mixture of discrete and consecutive representations, where discrete numbers are separated by commas and segments of numbers are represented by minus signs, e.g., 2,5,8,10-20
Adding a	port ethernet	

Single Port	*interface-num*	
Adding multiple ports	port ethernet { *interface-list* | all }	interface-list is a list of selected ports, indicating one or more Ethernet ports. If all is selected, all ports in the system are added.
Deleting individual ports	undo port ethernet *interface-num*	
Delete multiple ports	undo port ethernet { *interface-list* | all }	When all is selected, all ports are deleted.

Description:

- In VLAN view, if the default VLAN ID of the port to be deleted happens to be the same as this VLAN, the port is not allowed to be deleted, and if you need to delete it, you can modify the default VLAN of the port to some other value first, and then delete this port.
- Add the port in VLAN view. the port has two states in the VLAN, tagged and untagged states. If the port is an access or hybrid port, it is added to the VLAN as untagged state. if the port is a trunk port, then set its state in the VLAN to tagged.

In port view, VLAN ports can also be added or deleted, as shown in the following tables 8-4, 8-5, and 8-6, which indicate the operations of adding and deleting VLAN ports for Access, Hybrid, and Trunk ports, respectively.

Configure Access port-based VLANs:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	interface-list indicates one or more Ethernet ports
Configure the port mode to Access	port mode access	
Adding VLAN ports	port default vlan *vlan-id*	Access ports belong to only one VLAN, so to add a vlan to an access port, simply set the port's default vlan id

Configure Hybrid port-based VLANs:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	interface-list indicates one or more Ethernet ports
Configure the port mode to Hybrid	port mode hybrid	
Add the VLAN and set the port vlan attribute to tagged	port hybrid tagged vlan { all | *vlan-list* }	The vlan-list indicates a one or port vlan, and when all is selected, all vlan is added. The vlan added at this point are set to the tagged

		attribute.
Add the VLAN and set the port vlan attribute to untagged	port hybrid untagged vlan { all | *vlan-list* }	The vlan-list indicates a one or port vlan, and when all is selected, all vlan is added. The vlan added at this point are set to the untagged attribute.
Delete vlan port	undo port hybrid vlan { all | *vlan-list* }	Remove the hybrid port from the specified VLAN list

Configure Trunk port-based VLANs:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	interface-list indicates one or more Ethernet ports
Configure the port mode to Trunk	port mode trunk	
Adding VLAN ports	port trunk allowed vlan { all | *vlan-list* }	The vlan-list indicates a one or port vlan, and when all is selected, all vlan is added. The vlan added at this point is set to the tagged attribute, except for the port default vlan, which is the untagged attribute.
Delete vlan port	undo port trunk allowed vlan { all | *vlan-list* }	Remove the Trunk port from the specified VLAN list

[Example]

! Create VLAN 100 with the addition of Ethernet port 1

```
[GPON-vlan-100]port ethernet 0/0/1
```

Description:

Since an access port can belong to only one VLAN, you can add this port to a VLAN by configuring the default VLAN ID of the port in port view.

8.2.4 Specify/delete VLAN descriptors

The description string is used to distinguish between individual VLANs. specify and delete VLAN descriptors as follows:

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN view	vlan vlan-list	The composition of a vlan-list can be discrete numbers, a consecutive segment of numbers, or a mixed representation of discrete and consecutive, where discrete numbers are separated by commas, and a segment of numbers is represented by a minus sign, such as: 2,5,8,10-20, which indicates the descriptor for configuring multiple VLANs when entering multiple VLAN views
Configuring VLAN	description *string*	string :is a string describing the VLAN, 1 to 32 characters in length, the value range is that each character is a printable character and cannot contain '/',':','*','?' ,'\\\','<','>','|','"" and so

Descriptors		on.
Deleting a VLAN Descriptor	undo description	

[Example]

! Configure the descriptor for VLAN 100 as Connet-to-E-Unit

[GPON-vlan-100] description Connet-to-E-Unit

8.2.5 Configure the port type

There are three types of Ethernet ports supported by the system:

- Access Type: The port can only belong to 1 VLAN, generally used for the connection between the device and end users;
- Trunk Type: The port can belong to multiple VLANs, can receive and send messages of multiple VLANs, and is generally used for connection between devices;
- Hybrid type: The port can belong to multiple VLANs, can receive and send messages of multiple VLANs, and can be used for connecting between devices or connecting to the user's computer.

Configure the port type operation as shown below:

Configure the port type:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	interface-list indicates one or more Ethernet ports
Configure the port type as Access	port mode access	
Configure the port type as Hybrid	port mode hybrid	
Configure the port type as Trunk	port mode trunk	

Different types of ports handle the reception and transmission of messages in different ways, see the following table for a description of the specific handling.

Processing of incoming and outgoing messages on Access ports:

Handling of incoming telegrams		Handling when sending messages
When a message is received without a Tag	When a message is received with Tag	
Receive the message and add the Tag of the default VLAN to the message.	• When the VLAN ID is the same as the default VLAN ID: receive the message • When the VLAN ID is different from the default VLAN ID: drop the message	Since the VLAN ID is the default VLAN ID, there is no need to set it, and it is sent after removing the Tag.

Trunk port send/receive message processing:

Handling of incoming telegrams		Handling when sending messages
When a message is received without a Tag	When a message is received with Tag	

Receive the message and add the Tag of the default VLAN to the message.	● When the VLAN ID is the VLAN ID that the port is allowed to pass through: receive the message ● When the VLAN ID is not the VLAN ID that the port is allowed to pass through: drop the message	● When the VLAN ID is the same as the default VLAN ID: remove the Tag and send the message ● When the VLAN ID is different from the default VLAN ID: keep the original Tag, send the message

Hybrid port send/receive message processing:

Handling of incoming telegrams		Handling when sending messages
When a message is received without a Tag	When a message is received with Tag	
Receive the message and add the Tag of the default VLAN to the message.	● When the VLAN ID is the VLAN ID that the port is allowed to pass through: receive the message ● When the VLAN ID is not the VLAN ID that the port is allowed to pass through: drop the message	When the VLAN ID carried in the message is the VLAN ID that the port is allowed to pass through, the message is sent and can be passed through the port hybrid tagged vlan/port hybrid untagged vlan command To make sure that the message is sent with a Tag (including the default VLAN, the same judgment is made).

[Example]

! Configure the port type of Ethernet port 1 as Trunk

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


Description:

- Access, Hybrid, and Trunk types of ports can coexist on a single device, and the types can be switched directly between ports. After switching, the default VLAN of the port remains unchanged, and the VLAN tag attribute is switched to the default attribute, as follows:

When an Access port is switched to Hybrid, the default VLAN of the port remains unchanged and the VLAN attribute is switched to untagged;

When an Access port is switched to Trunk, the port's default VLAN remains unchanged and the VLAN attribute is switched to untagged;

When the Hybrid port is switched to Access, the default VLAN of the port remains unchanged and the remaining VLANs remove this port;

When a Hybrid port is switched to Trunk, the port's default VLAN remains unchanged, the VLANs remain unchanged, and all but the default VLANs become

tagged attribute;

When a Trunk port is switched to Access, the default VLAN of the port remains unchanged and the remaining VLANs remove this port;

When a Trunk port is switched to Hybrid, the default VLAN of the port remains unchanged and the rest of the VLANs remain unchanged and all become untagged attributes;

- Hybrid ports can allow messages for multiple VLANs to be sent untagged, while Trunk ports only allow messages for the default VLAN to be sent untagged.

8.2.6 Configure the port default VLAN ID

Systems are shipped with a default VLAN 1. The default VLAN is configurable and the configuration operation is shown below:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	interface-list indicates one or more Ethernet ports
Configure the port default VLAN ID	port default vlan *vlan-id*	
Restore factory default VLAN ID	undo port default vlan	After restoration, the default VLAN is 1.

[Example]

! Configure the default VLAN ID of Ethernet port 1 to 100

[GPON-ethernet-0/0/1] port default vlan 100

8.2.7 Configuring Hybrid Port Tag vlan

When a port is set up as a hybrid port, you can set the port to send tagged or untagged messages out by configuring the tag vlan as shown below:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	interface-list indicates one or more Ethernet ports
Configure the port type as Hybrid	port mode hybrid	
Configure the port tagged vlan	port hybrid tagged vlan { all | *vlan-list* }	The vlan-list indicates a one or port vlan, and when all is selected, all vlan is added. The vlan added at this point are set to the tagged attribute.
Configure port untagged vlan	port hybrid untagged vlan { all | *vlan-list* }	

[Example]

! Configure the Hybrid Tag VLAN for Ethernet port 1 to 100

[GPON-ethernet-0/0/1] port hybrid tagged vlan 100

8.2.8 Display VLAN information

After completing the VLAN configuration, execute the display command in any view to view the VLAN information:

manipulate	command	clarification
View information about a specified vlan	display vlan [*vlan-id*]	When vlan-id is specified, the command displays information for the specified vlan. When vlan is not specified, the command displays all vlan information. When the VLAN does not exist, the vlan does not exist message is displayed.

View vlan summary information	display vlan brief	Displays brief information about all vlan.
View port information within a vlan	display vlan interface [ethernet *interface-list*]	When interface-list is not specified, all port information in the vlan is displayed.

[Example]

! Display all VLAN information

[GPON]display vlan

8.3 MAC-based VLAN Configuration

8.3.1 Introduction to MAC-based VLANs

MAC-based VLAN segmentation is another method of VLAN segmentation. It defines VLAN members according to the source MAC address of the message, and sends the specified message after adding it to the Tag of that VLAN. This feature is usually used in conjunction with security (e.g., 802.1X) technologies to achieve secure and flexible access to terminals.

If the mechanism of dividing VLANs based on MAC addresses is used, when the port receives a message, the following method is used to process it:

When the received message is an untagged message, it will use the source MAC of the message as the basis to match the MAC-VLAN table entry. If the MAC address and the keyword in the table entry are exactly the same, the search succeeds and the VLAN ID specified in the table entry is added to the message; if the match fails, the match is performed according to other matching principles. When the received message is a tagged message, the source MAC of the message is also used as the basis to match the MAC-VLAN table entry. If it matches, the VLAN of the message is replaced by the VLAN specified by the MAC-VLAN table entry. If it fails to match, the processing is the same as that of port-based VLAN: if the port allows the VLAN tagged message to pass through, then it forwards the message normally; if it does not allow it, then it discards the message.

8.3.2 MAC-based VLAN Configuration Task List

Configuration tasks	clarification	Detailed Configuration
Create/delete MAC address-based VLAN table entries	compulsory	8.3.3
View MAC address-based VLAN table entries	selectable	8.3.4

8.3.3 Create/delete MAC-based VLAN table entries

The system supports assigning VLAN IDs and 802.1q priorities to messages based on their MAC addresses, and the related configurations are shown below:

manipulate	command	clarification
Go to System View	system-view	
Configure the vlan-mac table and assign the appropriate vlan id and priority to the corresponding mac address according to the configuration table	mac-vlan mac-address mac-address vlan [priority]	
Delete the configured vlan-mac table entry	undo mac-vlan [mac-address *mac-address*]	When mac-address is not specified, all configured vlan-mac table entries are deleted.

[Example]

! Configure the VLAN based on MAC address 00:E1:4B:15:E5:1C to 100

[GPON]mac-vlanmac-address 00:E1:4B:15:E5:1C 100 5

8.3.4 Display MAC-based VLAN table entries

After completing the MAC-based VLAN configuration, execute the display command in any view to view the table entry information:

manipulate	command	clarification
View MAC-based vlan table entries	display mac-vlan [mac-address *mac-address*]	When mac-address is not specified, all configured vlan-mac table entries are displayed.

[Example]

! Display MAC-based VLAN table entries

[GPON] display mac-vlan

8.4 Protocol-based VLAN Configuration

8.4.1 Introduction to protocol-based VLANs

Protocol-based VLAN, also known as protocol VLAN (collectively referred to as protocol VLAN below for ease of description), is another method of VLAN segmentation. By configuring protocol VLAN, the device can analyze the messages received on the port without VLAN Tag, match the messages with the protocol template set by the user according to different encapsulation formats and the values of special fields, and add the corresponding VLAN Tag to the successfully matched messages, so as to realize the function of automatically distributing data belonging to the specified protocols to be transferred to specific VLANs. This feature is mainly used to bind the service types provided in the network with VLANs to facilitate management and maintenance.

The system supports assigning VLAN IDs to messages based on the message protocol field, where the protocol refers to the frame type (categorized as ethernet v2, snap-llc for 802.3, and non-snap-llc) as well as the Ethernet type value (e.g., 0806 for ARP).

8.4.2 Protocol-based VLAN Table Entry Configuration List

Configuration tasks	clarification	Detailed Configuration
Create/delete protocol-based VLANs	compulsory	8.4.3
Viewing Protocol-Based VLAN Configuration	selectable	8.4.5

8.4.3 Create/delete VLANs based on protocol

Creating and deleting protocol-based VLAN configurations consists of two parts:

Configure the protocol address template in system view to specify the frame type and Ethernet type;

Port view references a protocol template and corresponds to a VLAN ID;

Protocol-based VLAN configuration commands, as shown below:

manipulate	command	clarification
Go to System View	system-view	
Configuring Protocol Templates	protocol-vlan profile *index* frame-type *eth-type*	
Delete protocol template configuration	undo protocol-vlan profile [*index*]	

Enter port view	interface ethernet *interface-num*	
Specify the vlan id that needs to be assigned to this port for the previously globally configured protocol-based vlan table entries.	protocol-vlan profile *index* vlan *vlan-id* [priority *priority*]	
Deletes the protocol-based vlan table entry under this port, stopping the assignment of vlan id to the protocol number specified in the table entry	undo protocol-vlan profile [*index*]	When index is not specified, all vlan table entries are deleted.

[Example]

! Configure Ethernet port 1's IP protocol-based VLAN to 100

[GPON]protocol-vlan profile 1 frame-type ethernet2 ether-type 0800

[GPON-ethernet-0/0/1] protocol-vlan profile 1 vlan 100

8.4.4 Display protocol-based VLAN configuration

After completing the protocol-based VLAN configuration, execute the display command in any view to view the table entry information:

manipulate	command	clarification
Display protocol template-based VLAN configuration information	display protocol-vlan profile [*index*]	
Display port-binding-based VLAN template configuration information	display protocol-vlan interface [ethernet *interface-num*]	

[Example]

! Display protocol template configuration information

[GPON] display protocol-vlan profile

8.5 IP subnet-based VLAN configuration

8.5.1 Introduction to VLANs based on IP subnets

VLAN segmentation based on IP subnet is another method of VLAN segmentation. It defines the VLAN members according to the IP subnet address of the message, and the specified message is added to the Tag of the VLAN and then sent.

If the mechanism of dividing VLANs based on IP subnet addresses is used, when the port receives a packet, the following method is used to process it:

When the received message is an untagged message, the source IP address of the message is used as the basis to match the ip-subnet-vlan table entry. If the IP subnet address and the keyword in this table entry are identical, the search succeeds and the VLAN ID specified in the table entry is added to the message; if the match fails, the match is performed according to other matching principles.

When the received message is a tagged message, it also uses the source MAC of the message as the basis to match the ip-subnet-vlan table entry. If it matches, the VLAN of the message is replaced by the VLAN specified by the ip-subnet-vlan table entry. If the match fails, the treatment is the same as that of port-based VLANs: if the port allows the tagged message to pass through, the message will be forwarded normally; if it does not allow it, the message will be discarded.

8.5.2 IP Subnet Based VLAN Configuration Task List

Configuration tasks	clarification	Detailed Configuration
Create/delete VLAN table entries based on IP subnet addresses	compulsory	8.3.3
Configure whether IP subnets take precedence over MAC subnets	selectable	8.3.4
View VLAN table entries based on IP subnet addresses	selectable	8.3.5

8.5.3 Create/delete IP subnet-based VLAN table entries

The system supports assigning VLAN ID and 802.1q priority to messages based on the IP subnet address of the message, and the related configurations are shown below:

manipulate	command	clarification
Go to System View	system-view	
Configure the ip-subnet-vlan table, and assign the appropriate vlan id and priority to the corresponding IP subnet address according to the configuration table	ip-subnet-vlan ipv4 *ip-address* mask *mask* vlan *vlanid* [priority *priority*]	
Delete the configured ip-subnet-vlan table entry	undo ip-subnet-vlan [ipv4 *ip-address* mask *mask*]	When ip-address is not specified, all configured ip-subnet-vlan table entries are deleted.

[Example]

! Configure VLAN based on IP subnet 1.1.1.1/24 to 100

```
[GPON]ip-subnet-vlan ipv4 1.1.1.1 mask 255.255.255.0 vlan 100
```

8.5.4 Configure whether IP subnet VLANs take precedence over MAC-VLAN table entries

The system supports message-based IP subnet address as well as message MAC-based VLAN table entries, and if both are configured at the same time, there is a question of which table entry takes precedence. The system provides configuration commands to determine whether the IP subnet VLAN takes precedence over the MAC-VLAN table entries, and the relevant configurations are shown below:

manipulate	command	clarification
Go to System View	system-view	
Configure ip-subnet-vlan to take precedence over mac-vlan table entries	ip-subnet-vlan precede	
Delete the ip-subnet-vlan takes precedence over mac-vlan table entry	undo ip-subnet-vlan precede	Default MAC-VLAN table entries are preferred over IP subnet VLAN table entries

[Example]

! Configure IP subnet VLAN precedence over MAC-VLAN table entries

```
[GPON]ip-subnet-vlan precede
```

8.5.5 Display IP subnet-based VLAN table entry configuration

After completing the IP subnet-based VLAN configuration, execute the display command in any view to view the table entry information:

manipulate	command	clarification
View IP subnet-based VLAN table entries	display ip-subnet-vlan [ipv4 *ip-address* mask *mask*]	When ip-address is not specified, all configured table entries are displayed.

[Example]

! Display VLAN table entries based on IP subnets

```
[GPON] display ip-subnet-vlan
```

Chapter 9 QinQ Configuration

9.1 QinQ Features

9.1.1 QinQ Function Introduction

1.QinQ Dual Tag Technology

QinQ technology is a simple and flexible Layer 2 VPN tunneling technology, which encapsulates the outer VLAN Tag for the user's private network message at the operator's access side, so that the message carries the two-layer VLAN Tag to traverse the operator's backbone network (public network). In the public network, the message is transmitted only according to the outer VLAN Tag (i.e., the public VLAN Tag), and the user's private VLAN Tag is transmitted as the data portion of the message.

The structure of a message carrying a single-layer VLAN Tag is shown in the following figure:

The structure of a message carrying a dual-layer VLAN Tag is shown in the following figure:

QinQ can mainly solve the following problems:

alleviate the problem of increasingly scarce public network VLAN ID resources;

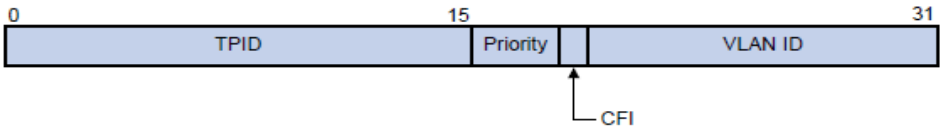
Users can plan their own private VLAN IDs, which will not result in conflicts with public VLAN IDs;

Provides a simpler Layer 2 VPN solution for small metro or enterprise networks;

2. QinQ message TPID value configurable function

TPID (Tag Protocol Identifier) is a field in the VLAN Tag, and the IEEE 802.1Q protocol specifies the value of this field as 0x8100.

The Tag message structure of an Ethernet frame defined by the IEEE 802.1Q protocol is shown below:



This OLT device can identify whether a VLAN Tag is carried in a message based on the TPID value. When the port receives a message, it compares the configured TPID value with the corresponding field in the message, and if they are the same, it means that the message carries a VLAN Tag.

This OLT device uses the protocol-specified TPID value (0x8100) by default, and some vendors set the device-recognizable TPID value to 0x9100 or other values. In order to be compatible with these devices, the device provides a TPID value configuration function for QinQ messages, which allows users to configure the TPID value used by the device when adding the outer Tag, so that the double Tag messages sent to the public network can be recognized by the devices of other vendors; and at the same time, enables the device to recognize the VLAN Tag of the messages on the public network normally.

9.1.2 Introduction to Static QinQ Functions

1. Introduction to the static QinQ function

The QinQ function is categorized into two types: the static QinQ function and the flexible QinQ function.

After the static QinQ function is enabled on a port, when the port receives a message, regardless of whether the message

has a VLAN Tag or not, the switch encapsulates the VLAN Tag of the default VLAN of this port for the message and learns the source MAC address into the MAC address table of the default VLAN. Therefore. when receiving a message:

1) If the original message is a message that already has a VLAN Tag, it will become a message with a double-layer Tag after entering the device;

2) If the original message is a message without a VLAN Tag, it will become a message with the port's default VLAN Tag after entering the device;

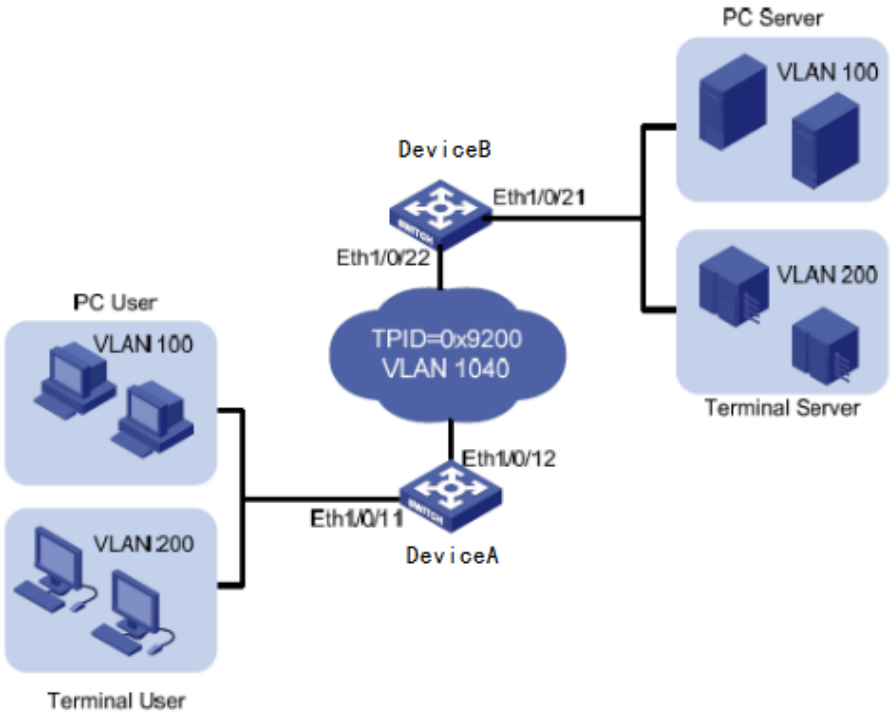
2. static QinQ typical networking applications:

DeviceA and DeviceB, as shown in the figure below, connect the user's workstation to the server over a public network.

1) The user's PC workstations and servers are segmented in private VLAN 100, and the terminal workstations and servers are segmented in private VLAN 200. the operator is now required to utilize VLAN 1040 of the public network to enable connectivity between the user's networks by means of a VPN;

2) The TPID value is 0x9200 for devices from other vendors used in the public network;

3) Configure the VLAN-VPN function of DeviceA and DeviceB so that the user's PC workstations/servers and terminal workstations/servers can be connected via VPN and communicate normally;



9.1.3 Introduction to Flexible QinQ Features

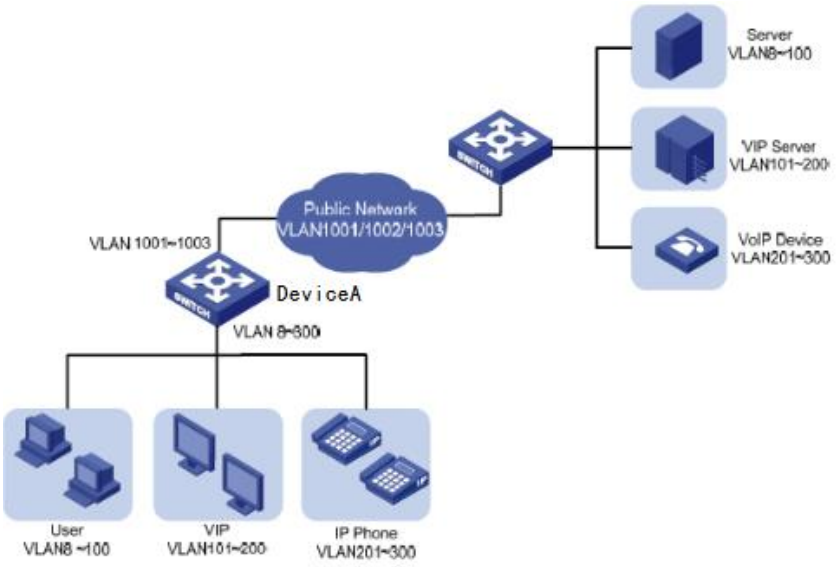
1. Introduction to the Flexible QinQ feature

Flexible QinQ is an enhanced application of the VLAN dual-tag function. With Flexible QinQ, users can configure inner and outer tag mapping rules to encapsulate different outer tags for messages with different inner tags according to the mapping rules.

2. Flexible QinQ Typical Networking Applications

Flexible QinQ function can make the operator's network architecture more flexible, in the port connected to the access layer equipment can be classified according to the VLAN Tag for different end-users, encapsulate different outer Tag for various types of users, and configure QoS policies in the public network according to the outer Tag, and flexibly configure the transmission priority of the data, so that various types of users can obtain the appropriate services.

The following chart is an example.



1) DeviceA is the access device of the operator, and the access users are categorized into general users (VLAN8-100), large customers (VLAN101-200) and IP phone users (VLAN201-300). The data messages of these three types of users are all forwarded to the public network by DeviceA; 2) Flexible QinQ and corresponding inner and outer tag mapping rules are configured on the port where DeviceA connects to the users, and the port will encapsulate the outer tag for the message according to the inner VLAN tag, e.g., encapsulate the VLAN 1002 tag on the outer layer of the data of the IP phone users (inner tag 201-300), and transmit the data to the VLAN 1002 tag. For example, the VLAN Tag of 1002 is encapsulated in the outer layer of the data of IP phone users (inner layer Tag of 201-300), and the data is transmitted to the VoIP device responsible for IP phone service for processing;

3) To ensure the transmission quality of voice messages, you can configure a QoS policy in the public network to adopt the rules of reserving bandwidth and prioritizing the sending of messages for VLAN 1002;

This method can configure forwarding policies for data from different types of users and improve network management flexibility. Moreover, it can save public VLAN resources and keep the isolation between similar users due to different inner VLAN tags, which ensures a certain degree of security.

3. Introduction to the VLAN pass-through feature pass-through

The VLAN passthrough function is generally used in conjunction with the static and flexible QinQ function. When the port is configured with static or flexible QinQ, the device will do double Tag processing on the message. If some VLANs do not need to do double-Tag processing in practical applications, you can configure the VLAN pass-through function of the port, configure the VLANIDs that need to be passed-through as pass-through rules, and when the VLANs carried in the message satisfy the pass-through rules, the message will not be added with the outer Tag, but will be directly passed-through and forwarded. Other VLANs match static or flexible QinQ rules for double Tag processing.

4. Introduction to the VLAN switching function swap

The VLAN Swap switching function means that the device can replace the VLANID of the message with the specified other VLANID in the incoming port according to the VLAN Tag of the message, and then forward the message in the device to realize flexible VLAN switching processing. For messages without VLAN Tag, the device does not perform switching processing and directly adds the port default VLAN to the message. for messages with VLAN Tag but the VLAN value does not match the configured switching rule, the device also does not perform switching processing but matches static or flexible QinQ processing.

5. Introduction to the VLAN switching function translate

The VLAN Translate switching function means that the device can replace the VLANID of the message with the specified other VLANID at the outgoing port according to the VLAN Tag of the message to realize the flexible switching processing of VLANs. The difference between this function and the VLAN Swap function is that the VLAN is swapped to the specified

VLAN on the outgoing port, and the incoming port is processed according to the normal 802.Q VLAN function, and the VLAN forwarding and MAC address learning are processed according to the original VLAN of the telegram, and the telegram is only replaced with the specified VLAN on the outgoing port.

9.2 QinQ Function Configuration

9.2.1 QinQ Configuration Task List

The list of configuration tasks related to the QinQ function is as follows.

Configuration tasks	clarification	Detailed Configuration
Turn on/off the port QinQ function	compulsory	9.2.2
Configure the port internal/external TPID	selectable	9.2.3
Configuring Port Flexible QinQ Inser Rules	compulsory	9.2.4
Configuring Port Flexible QinQ Pass-through Rules	selectable	9.2.5
Configuring Port Flexible QinQ Swap Rules	selectable	9.2.6
Configuring Global VLAN-Translate Rules	selectable	9.2.7
Turn on/off the port VLAN-Translate function	selectable	9.2.8
Displaying QinQ Configuration Information	selectable	9.2.9

9.2.2 Turn on/off the port QinQ function

The QinQ function switch is controlled based on the port, please turn on/off the port QinQ function in port mode.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	interface-list indicates one or more Ethernet ports
Turn on the QinQ function	qinq	
Disable the QinQ function	undo qinq	The device disables qinq by default

[Example]

! Enable the QinQ function on Ethernet port 1

[GPON-ethernet-0/0/1]qinq

9.2.3 Configure the port internal/external TPID

The device supports the function of configuring TPID for messages, including configuring inner-tpid and outer-tpid.

Inner-tpid is mainly used to determine whether the message has a VLAN Tag or not. when the message enters the device port, if the port has qinq enabled and inner-tpid configured, the device will judge whether the current message has a VLAN Tag based on inner-tpid, and if the VLAN Tpid of the message is the same as that of the port configuration, the device considers that the message has a VLAN Tag and then processes it based on the value in the VLAN Tag. If the VLAN Tpid of the message is the same as the inner-tpid configured by the port, the device considers that the message has a VLAN Tag and processes it according to the value in the VLAN Tag. If the VLAN Tpid of the message is different from the inner-tpid of the port configuration, the device considers that the message does not have a VLAN Tag, and adds a layer of VLANs directly according to the port PVID.

The main function of Outer-tpid is to modify the VLAN TPID of the message to the formulated TPID value when the message goes out the outgoing port.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	
Configuring the Internal TPID	qinq inner-tpid *tpid*	The tpid is configured in the range of 1-FFFF in hexadecimal
Delete internal TPID	undo qinq inner-tpid	
Configuring an External TPID	qinq outer-tpid *tpid*	
Delete external TPID	undo qinq outer-tpid	

[Example]

! Configure the internal TPID of Ethernet port 1 to 0x9100

[GPON-ethernet-0/0/24]qinq inner-tpid 9100

! Configure the external TPID of Ethernet port 2 to 0x9200

[GPON-ethernet-0/0/24]qinq outer-tpid 9200

9.2.4 Configuring Port Flexible QinQ Insert Rules

After a port is configured with a flexible QinQ insert rule, the device will add a layer of the outer VLAN specified by the insert rule to the message if the message carries a VLAN that satisfies the insert rule.

The setup rule of Flexible QinQ insert is to set up a group of consecutive VLANs and configure them in the way of start VLAN plus end VLAN. All VLAN Tag messages between the start VLAN and end VLAN will be forwarded in the way of double-layer VLAN Tag header with the destination VLAN if they are not being passed through. At the same time, users can also configure the 802.1P priority of the specified outer VLAN.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	
Configuring insert rules	flexible-vlan insert startvlanid endvlanid targetvlanid priority	Startvlanid, endvlanid, and targetvlanid are all VLAN values configured in the range of 1-4094, where endvlanid is greater than startvlanid. Priority is the 802.1P priority, configured in the range of 0-7
Remove insert rules	undo flexible-vlan insert { *startvlanid endvlanid* | all }	When all is selected, all insert rules are deleted.

[Example]

! Configure Ethernet port 1 with a flexible QinQ insertion rule that inserts messages from 100 to 200 into the outer 1000 VLAN and configure the 802.1P priority to 5

[GPON-ethernet-0/0/1] flexible-vlan insert 100 200 1000 5

9.2.5 Configuring Port Flexible QinQ Pass-through Rules

After a port is configured with the Flexible QinQ pass-through rule, if the VLANs of the message satisfy the pass-through

rule, the device will forward the message directly through the pass-through rule and will not add the outer VLANs to the message.The setup rule of the Flexible QinQ pass-through rule is as follows: set up a group of consecutive VLANs and configure them in the way of starting VLAN Flexible QinQ pass-through rules are as follows: Set a set of consecutive VLANs and configure them in the form of a start VLAN plus an end VLAN, and all VLAN Tag messages between the start VLAN and the end VLAN will be passed-through.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	
Configure pass-through rules	flexible-vlan pass-through *startvlanid endvlanid*	Startvlanid, endvlanid are both VLAN values configured in the range 1-4094, where endvlanid is greater than startvlanid.
Remove pass-through rules	undo flexible-vlan pass-through { *startvlanid endvlanid* | all }	When all is selected, all pass-through rules are deleted.

[Example]

! Configure a pass-through rule for Ethernet port 1 to passthrough packets from vlan 300 to 400

```
[GPON-ethernet-0/0/1] flexible-vlan pass-through 300 400
```

9.2.6 Configuring Port Flexible QinQ Swap Rules

After a port is configured with a Flexible QinQ Swap rule, if the message carries a VLAN that satisfies the swap rule, the device converts the VLAN ID of this message to the VLAN formulated by the swap rule, and then forwards it.

The setup rule for Flexible QinQ Swap is to set up a group of consecutive VLANs and configure them in the manner of start VLAN plus end VLAN. all VLAN Tag messages between the start VLAN and the end VLAN will be replaced with the VLAN specified by the swap rule. and at the same time the user can configure the 802.1P priority of the specified replacement VLAN.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface ethernet *interface-list*	
Configuring swap rules	flexible-vlan swap startvlanid endvlanid targetvlanid priority	Startvlanid, endvlanid, and targetvlanid are all VLAN values configured in the range of 1-4094, where endvlanid is greater than startvlanid. Priority is the 802.1P priority, configured in the range of 0-7
Remove swap rules	undo flexible-vlan swap { *startvlanid endvlanid* | all }	When all is selected, all swap rules are deleted.

[Example]

! Configure the swap rule for Ethernet port 1 with 500 to 600 messages replaced with VLAN 3000 and configure 802.1P priority 7

```
[GPON-ethernet-0/0/1] flexible-vlan swap 500 600 3000 7
```

9.2.7 Displaying QinQ Configuration Information

QinQ-related configuration information can be viewed under any attempt.

manipulate	command	clarification

Viewing QinQ Configuration Information	display flexible-vlan interface [ethernet *interface-list*]	When no port number is entered, the QinQ configuration information for all ports is displayed
View the port's VLAN-Translate feature configuration switches	display vlan-translate interface [ethernet *interface-list*]	
View global VLAN-Translate rule configuration	display vlan-translate-table egress	

[Example]

! View the QinQ configuration information for all ports

[GPON]display flexible-vlan interface

Chapter 10 MAC address management

10.1 Introduction to MAC Address Table Management

The system maintains a table of MAC addresses for forwarding Layer 2 messages. The entries in this table contain the device's MAC address, VLAN ID, and the port number on which the message entered the device. When a message enters the device, the device first looks up the message in the MAC address table based on the destination MAC and the VLAN ID information of the message, and sends the message out from the port specified in the MAC address table entry if it is found; otherwise, it broadcasts the message in this VLAN.

The system has the function of MAC address learning. If the source MAC address of a received message does not exist in the address table, the system adds the source MAC address, VLAN ID, and port number of the port that receives this message to the MAC address table as a new table entry.

The system supports manual configuration of MAC address table entries. The administrator can configure the MAC address table according to the actual network conditions, and the added or modified table entries can be static, permanent, black hole, and dynamic table entries.

The system supports the function of MAC address aging. A device does not send any messages for a certain period of time. the system removes the MAC address table entries associated with this device. the MAC address aging takes effect only on the learned or user-configured dynamic MAC address table entries.

10.2 MAC address table management configuration

10.2.1 MAC Address Table Management Configuration Task List

The list of MAC address table management configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Setting the MAC address aging time	selectable	10.2.2
Display MAC address aging time	selectable	10.2.3
Add/delete MAC address table entries	selectable	10.2.4
Display MAC address table entries	selectable	10.2.5
Enable/disable MAC address learning switch	selectable	10.2.6
Display MAC address learning switch	selectable	10.2.7
Configure the number of MAC addresses allowed to be learned for a port and VLAN	selectable	10.2.8
Display the number of MAC addresses allowed to be learned	selectable	10.2.9

10.2.2 Setting the MAC address aging time

The system supports learning MAC address table entries, and the learned MAC address table entries can set the aging time, after the aging time, if the device has not received the messages sent by this MAC, the MAC address will be automatically aged, and the related configurations are as follows:

manipulate	command	clarification
Go to System View	system-view	
Configure the MAC address aging time	mac-address-table age-time { *agetime* | disable }	A setting of disable indicates that the MAC never ages. The aging time supports 10-1000000S, and the default aging time is 300S.

Restore MAC address aging time	undo mac-address-table age-time	
Display MAC address aging time	display mac-address-table age-time	MAC address aging time can be viewed in any view

[Example]

! Set MAC address table aging time to one hour

[GPON]mac-address-tableage-time 3600

! Restore MAC address table aging time to the default time of 300 seconds

[GPON]undo mac-address-tableage-time

10.2.3 Display MAC address aging time

You can display the MAC address table aging time in any view.

manipulate	command	clarification
Display MAC address aging time	display mac-address-table age-time	

[Example]

! Display MAC address table aging time

[GPON]display mac-address-tableage-time

10.2.4 Add/delete MAC address table entries

The system supports manual configuration of MAC address table entries, including configuration of dynamic, static, permanent, and blackhole MAC address table entries.MAC address attributes can be categorized as dynamic, static, permanent, and blackhole MAC. Dynamic MAC address means that it can be aged, static MAC address means that it will not be aged but will be lost after system reboot, and permanent MAC address means that it will not be aged and this MAC address still exists after system reboot. Black hole MAC indicates that when the source or destination address of a message is a black hole MAC address, this message is discarded for processing. The related configurations are as follows:

manipulate	command	clarification
Go to System View	system-view	
Configure MAC address table entries	mac-address-table { static | permanent | dynamic } *mac-address* interface ethernet *interface-num* vlan *vlan-id*	
Configuring the Black Hole MAC Address	mac-address-table blackhole *mac-address* vlan *vlan-id*	
Delete MAC address table entries based on MAC+VLAN+Port	undo mac-address-table [dynamic | permanent | static] *mac-address* interface ethernet *interface-num* vlan *vlan-id*	
Delete MAC address table entries based on MAC+VLAN	undo mac-address-table [blackhole | dynamic | permanent | static] *mac-address* vlan *vlan-id*	
Delete MAC address table entries based on Port	undo mac-address-table [static | permanent | dynamic] interface ethernet *interface-num*	
Delete MAC address table entries based on VLANs	undo mac-address-table [blackhole | dynamic | permanent | static] vlan *vlan-id*	
Delete all MAC address table entries	undo mac-address-table	

[Example]

! Add a static MAC address with MAC address 00:E1:4B:15:E5:1C

[GPON]mac-address-table static 00:E1:4B:15:E5:1C interface ethernet 0/0/1 vlan 1

! Prohibit packets with source or destination address 00:E1:4B:15:E5:1C and VLAN 100 from passing through the system

[GPON]mac-address-table blackhole 00:E1:4B:15:E5:1C vlan 100

! Delete all MAC address table entries

[GPON]undo mac-address-table

 Attention:

When link aggregation exists in the system, the MAC address table associated with the link aggregation port is displayed as the corresponding aggregation group number. When link aggregation exists, adding or deleting MAC addresses for the aggregation ports will cause confusion, so it is recommended that you do not use them at the same time.

10.2.5 Display MAC address table entries

The MAC address table entries can be displayed in any view mode.

manipulate	command	clarification
Display all MAC address table entries	display mac-address-table	
Display MAC address table entries based on CPU port	display mac-address-table cpu	Display the MAC address table entry corresponding to the CPU port
Display MAC address table entries based on MAC	display mac-address-table *mac-address* [vlan *vlan-id*]	
Display MAC address table entries based on MAC address type	display mac-address-table { static | dynamic | permanent | blackhole } [vlan *vlan-id*]	
Display MAC address table entries based on port	display mac-address-table { static | dynamic | permanent | blackhole } interface ethernet *interface-num* [vlan *vlan-id*]	
Display MAC address table entries based on VLANs	display mac-address-table vlan *vlan-id*	

[Example]

! Display all MAC address table entries

[GPON] display mac-address-table

10.2.6 Enable/disable MAC address learning switch

The system supports configuring the MAC address learning switch function. When the MAC address learning function is turned off, the port will no longer dynamically learn the MAC address.

The system supports configuring the MAC address learning switch in global and port views. system view is to match all ports with the same configuration. Port view configures the MAC address learning switch for individual ports. When MAC address learning is disabled on a port, the port no longer dynamically learns MAC addresses. By default, MAC address

learning is turned on by default for all ports, and the related configurations are as follows:

manipulate	command	clarification
Go to System View	system-view	
Turn on MAC address learning globally	mac-address-table learning	
Disable the MAC address learning function globally	undo mac-address-table learning	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Turn on port MAC address learning	mac-address-table learning	
Disable port MAC address learning	undo mac-address-table learning	

[Example]

! Disable MAC address learning on Ethernet port 7

[GPON-ethernet-0/0/7]undo mac-address-table learning

10.2.7 Display MAC address learning switch

You can display the MAC address learning switch function configuration in any view mode.

manipulate	command	clarification
Display MAC address aging time	display mac-address learning [interface ethernet [*interface-num*]]	Displays MAC address learning switches for all ports when no port number is specified

[Example]

! Display the MAC address learning switch function for Ethernet port 7

[GPON-ethernet-0/0/7]display mac-address-table learning interface ethernet 0/0/7

10.2.8 Configure the number of MAC addresses allowed to be learned for a port and VLAN

The system supports the function of configuring the number of MAC addresses allowed to be learned based on ports and VLANs. By default, the number of MAC addresses that can be learned by all ports and VLANs is 64K. After reconfiguring the limit of the number of MAC addresses for a port or a VLAN, all the dynamic MAC addresses in the port or the VLAN before the configuration will be deleted automatically, and thereafter the number of dynamic MAC addresses learned by the port or the VLAN should be less than or equal to the limit, and any message that exceeds the limit will be discarded and not forwarded. If the number of MAC addresses exceeds the limit, the device will discard and not forward the message. When the number of MAC addresses limit is configured under both the port and VLAN, the MAC address learning limit is based on the smallest value between the two.

manipulate	command	clarification
Go to System View	system-view	
Entering VLAN mode	vlan vlan-id	
Configure a limit on the number of MAC addresses	mac-address-table max-mac-count *max-mac-count*	The number of MAC addresses is limited to a range of 1-65536
Remove the limit on the number of MAC addresses	undo mac-address-table max-mac-count	
Enter port view	interface { { ethernet interface-num } | interface-name }	

Configure a limit on the number of MAC addresses	mac-address-table max-mac-count *max-mac-count*	The number of MAC addresses is limited to a range of 1-65536
Remove the limit on the number of MAC addresses	undo mac-address-table max-mac-count	

[Example]

! Configure the maximum number of MAC addresses to be learned for Ethernet port 7 to 5

[GPON-ethernet-0/0/7]mac-address-table max-mac-count 5

! Configure the maximum number of MAC addresses to be learned for VLAN 100 to 100

[GPON-vlan-100]mac-address-table max-mac-count 100

10.2.9 Display the number of MAC addresses allowed to be learned

You can display the MAC address allow learning number configuration in any view mode.

manipulate	command	clarification
Display the number of MAC addresses allowed to be learned	display mac-address max-mac-count { interface ethernet [*interface-num*] | vlan *vlan-id* }	

[Example]

! Displays the number of MAC addresses allowed to be learned for Ethernet port 7

[GPON]display mac-address-table max-mac-count interface ethernet 0/0/7

Chapter 11 STP Configuration

11.1 Introduction to the STP protocol

STP (Spanning Tree Protocl, Spanning Tree Protocol) is part of the IEEE 802.1D bridge protocol. The standard implementation of STP eliminates network broadcast storms caused by looped connections to the network, which can be brought about by errors or accidents, and also provides the possibility of providing backup connections to the network.
The IEEE 802.1D standard STP protocol provides a dynamic redundant switching mechanism for the network and is responsible for preventing circular connections in a bridged network. It determines which port of the bridge is able to send packets. After the Spanning Tree algorithm is implemented on the devices in the LAN, they will form a spanning tree dynamic topology, which makes it possible for no loops to exist between any two workstations in the LAN, in order to prevent the resulting LAN broadcast storms, and the Spanning Tree algorithm is also responsible for monitoring the changes in the physical topology, and is able to create a new Spanning Tree after a change in the topology. For example, when a device breaks down or a data channel breaks, it can provide a certain degree of fault tolerance and reconfigure the topology of the spanning tree.

11.2 STP Function Configuration

11.2.1 STP Function Configuration Task List

The various configuration tasks take effect only after STP is started. Before starting STP, you can configure the relevant parameters of the device or the Ethernet port. After STP is shut down, these configuration parameters are still retained and will take effect when STP is restarted.
The list of major STP configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable device STP function	compulsory	11.2.2
Enable/disable port STP function	selectable	11.2.3
Configure the device's spanning tree protocol mode	selectable	11.2.4
Configure the device STP priority	selectable	11.2.5
Configuring the Device Forward Delay Feature	selectable	11.2.6
Configure the device hello-time feature	selectable	11.2.7
Configuring the Device Max Age Feature	selectable	11.2.8
Configure port-specific path overhead	selectable	11.2.9
Configuring STP Priority for a Specific Port	selectable	11.2.10
Configure specific ports to force the sending of RSTP messages	selectable	11.2.11
Configure the link type for a specific port	selectable	11.2.12
Configure the border port state for a specific port	selectable	11.2.13
Configure the rate limit for sending BPDUs on a specific port	selectable	11.2.14
Display information about STP state machine configuration parameters	selectable	11.2.15

11.2.2 Enable/disable device STP function

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Enable device STP function	stp	
Disable the device STP function	undo stp	

[Example]

! Enable the STP protocol for the device

[GPON]stp

11.2.3 Enable/disable port STP function

The system supports to enable/disable the STP function of the specified port, and after the port is closed, the port will not participate in the STP protocol calculation.

Please make the following configurations in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Enable device STP function	stp	
Disable the device STP function	undo stp	

[Example]

! Disable STP on Ethernet port 1

[GPON-ethernet-0/0/1]undo stp

11.2.4 Configure the device's spanning tree protocol mode

The spanning tree protocols supported by the system include STP, RSTP, and MSTP, which can be configured in system view in spanning tree mode.

manipulate	command	clarification
Go to System View	system-view	
Configuring Spanning Tree Protocol Mode	stp mode { stp | rstp | mstp }	
Restore default spanning tree protocol mode	undo stp mode	The default spanning tree protocol mode is RSTP

[Example]

! Configure the device to run the STP protocol

[GPON]stp mode stp

11.2.5 Configure the device STP priority

Set the STP priority of the device; the lower the priority value, the more likely the device will be the root bridge in the network.

manipulate	command	clarification
Go to System View	system-view	
Configure the device STP priority	stp priority bridge-priority	Spanning tree priority configuration ranges from 0-61440, with a default value of 32768
Restore the default device STP priority	undo stp priority	

[Example]

! Set the device STP priority to 4096

[GPON]stp priority 4096

Attention:

- If the same value is used for the priority of all bridges in the network, the one with the smallest MAC address will be selected as the root.
- Configuring the priority of a bridge with the STP protocol on causes spanning tree recalculation.
- The value range of the priority is 0 to 61440, and the value must be an integer multiple of 4096.

11.2.6 Configuring the Device Forward Delay Feature

The system supports setting the time interval for port state switching when the device is selected as the root bridge. Its value is related to the network diameter of the switching network, the larger the network diameter, the longer it takes.

manipulate	command	clarification
Go to System View	system-view	
Configure the device Forward Delay time	stp forward-time *seconds*	Forward Delay is configured in the range of 4-30 seconds, with a default value of 15 seconds
Restore the default device Forward Delay time	undo stp forward-time	

[Example]

! Set Forward Delay to 20 seconds

[GPON]stp forward-time 20

Attention:

If the Forward Delay is configured too small, temporary redundant paths may be introduced, and if the Forward Delay is configured too large, the network may not be able to regain connectivity for a longer period of time.The value of the Forward Delay ranges from 4 to 30 seconds, and the default value of 15 seconds is recommended.The duration of the Forward Delay must be greater than or equal to Hello Time + 2.

11.2.7 Configuring the Device Hello Time Feature

The system supports configuring the time interval Hello Time for the device to send STP messages. The appropriate hello time value can ensure that the bridge can discover link failures in the network in time without occupying too much network resources.

manipulate	command	clarification
Go to System View	system-view	
Configure the device Hello Time time	stp hello-time *seconds*	Hello Time is configured in the range of 1-10 seconds, with a default value of 2 seconds
Restore the default device Hello Time time	undo stp hello-time	

[Example]

! Set STP Hello Time to 5 seconds

[GPON]stp hello-time 5

 Attention:

A value of Hello Time that is too large can cause the bridge to think that the link has failed and start recalculating the spanning tree because of packet loss on the link. A value of Hello Time that is too short can cause the bridge to send frequent configuration messages, increasing the burden on the network and CPU.The value of Hello Time ranges from 1 to 10 seconds, and the default value of 2 seconds is recommended.Hello Time must be less than or equal to Forward Delay - 2.The Forward Delay time must be be greater than or equal to Hello Time + 2.

11.2.8 Configuring the Device Max Age Feature

Device Max Age is a parameter used to determine whether a configuration message is "outdated", which can be configured by the user according to the actual network conditions.

manipulate	command	clarification
Go to System View	system-view	
Configure the device Max Age time	stp max-age *seconds*	Max Age is configured in the range of 6-40 seconds, with a default value of 20 seconds.
Restore default device Max Age time	undo stp max-age	

[Example]

! Set Max Age to 10 seconds

[GPON]stp max-age 10

 Attention:

Max Age is used to set the maximum time interval for STP protocol message aging, and if the timeout period is exceeded, the message is directly discarded. If this value is too small, the spanning tree calculation will be more frequent, and it is

possible to mistake network congestion for link failure; if this value is too large, it is not conducive to the timely detection of link failures.The range of values for Max Age is from 6 to 40 seconds.The value of Max Age time is related to the network diameter of the switching network. It is recommended that the default value of 20 seconds be used.The Max Age time must be greater than or equal to 2*(Hello Time + 1) and less than or equal to 2*(Forward Delay- 1).

11.2.9 Configure port-specific path overhead

Configure the spanning tree path overhead of ports participating in STP calculations, and select the path with the smallest path overhead as the valid path. The path overhead of a port is related to the link rate of that port, and the larger the link rate, the smaller you should configure this parameter. the STP protocol can automatically detect the link rate of the current port and convert it to the corresponding path overhead.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet *interface-num* } | interface-name }	
Configure the port's path overhead	stp cost *cost*	The cost configuration range is 1-200000000, and the default value is 200000
Path overhead for restoring default ports	undo stp cost	

[Example]

! Set the path spend for Ethernet port 1 to 20000

[GPON-ethernet-0/0/1]stp cost 20000

 Attention:

Configuring the path overhead of an Ethernet port causes spanning tree recalculation. The range of values for the port path overhead is 1 to 200000000. it is recommended that the default value of 200000 be used to allow the STP protocol to calculate the path overhead for the current port by itself. By default. the path overhead is determined based on the speed of the particular port at the time.

The default value of the port path overhead is based on the port speed; the default value is 2000000 for a port speed of 10M, 200000 for 100M, and 20000 for 1000M.

11.2.10 Configuring STP Priority for a Specific Port

The system supports configuring the STP of a port. a lower priority value means a higher priority, and the port is more likely to be the root port. If all the ports of the device use the same priority parameter value, the port's priority level depends on the index number of the port. the lower the index number, the higher the priority.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the STP priority of the port	stp port-priority *port-priority*	The port STP priority configuration range is 0-240, the value must be an integer multiple of 16, and the default value is 128.
Restore the STP priority of the default port	undo stp port-priority	

[Example]

! Set the spanning tree priority of Ethernet port 1 to 112

[GPON-ethernet-0/0/1]stp port-priority 112

 Attention:

A smaller priority value indicates a higher priority, and the easier it is for the port to become the root port. Changing the priority of an Ethernet port causes a spanning tree recalculation. The value range of port spanning tree priority is 0 to 240, and the value must be an integer multiple of 16. By default, the port spanning tree priority is 128.

11.2.11 Configure specific ports to force the sending of RSTP messages

This function is mainly used to check the presence of legacy bridges running the STP protocol in the network.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configure the port to force RSTP messages	stp mcheck	
Close the port to force RSTP messages	undo stp mcheck	

[Example]

! Set Ethernet port 1 to force rstp packets to be sent

[GPON-ethernet-0/0/1]stp mcheck

11.2.12 Configure the link type for a specific port

In RSTP, the port's fast entry into the forwarding state requires that the port must be a point-to-point link and not a shared media link. you can manually specify the link type of the port or the bridge can determine the current link type of the port.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the port as a point-to-point link	stp point-to-point forcetrue	
Configure the port as a non-point-to-point link	stp point-to-point forcefalse	
Configure to automatically detect if a port is a point-to-point link	stp point-to-point auto	

[Example]

! Setting Ethernet port 1 as a point-to-point link

[GPON-ethernet-0/0/1]stp point-to-point forcetrue

11.2.13 Configure the border port state for a specific port

Border ports are ports that are connected to the host. these ports can enter the forwarding state for a short time after linkup, but once these ports receive spanning tree packets they automatically switch to non-border ports.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the port as a border port	stp portfast	
Configure the port as a non-border port	undo stp portfast	

[Example]

! Setting Ethernet port 1 as a border port

[GPON-ethernet-0/0/1]stp portfast

11.2.14 Configure the rate limit for sending BPDUs on a specific port

Bandwidth consumption by the Spanning Tree Protocol can be suppressed by setting a rate limit for BPDU messages sent by the port. the rate is measured in terms of the number of bpdu's sent during each hello time.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the rate limit for BPDU messages sent by the port	stp transit-limit *limit*	The limit configuration range is 1-255, and the default value is 3.
Restore the port's default rate limit for sending BPDU messages	undo stp transit-limit	

[Example]

! Set Ethernet port 1 to send a maximum of 2 bpdu messages per hello time time

[GPON-ethernet-0/0/1]stp transit-limit 2

11.2.15 Display STP status and configuration parameter information

STP status information can be displayed in any view mode, and the contents of STP status information include: STP status, root bridge ID, follow port ID, and various configuration parameter information of STP.

manipulate	command	clarification
Display STP status and configuration parameter information	display stp interface [brief | ethernet *interface-num*]	When no port is specified, all port STP status information is displayed. Select the brief parameter to display all port STP status brief information.

[Example]

! Display device STP configuration status

[GPON]display stp interface ethernet 0/0/1

Chapter 12 MSTP Configuration

12.1 Introduction to MSTP Protocol

Multiple spanning tree (IEEE802.1S, Multiple Spanning Tree) is an upgrade to SST (Single Spanning Tree, IEEE8021.D/8021,W). Single Spanning Tree can realize link redundancy and loop elimination, but because all VLANs share a tree, it often results in a waste of effective bandwidth, leading to overload on some links while others are always in a backup state. while some other links are always in a backup state. Multiple Spanning Tree compensates for these shortcomings by mapping different VLANs to different spanning tree instances, which can achieve load balancing while taking into account all the functions of SST, i.e., different spanning tree instances can form different topologies, and the data of different VLANs may be selected for different transmission channels depending on the spanning tree instances in which the VLANs are located.

12.2 MSTP Feature Configuration

12.2.1 MSTP Feature Configuration Task List

Each parameter of the MSTP configuration takes effect only when the spanning tree is turned on and the spanning tree protocol mode is MSTP. these parameter configurations remain when MSTP is turned off and these parameters take effect the next time MSTP is turned on. the list of the MSTP configurations is as follows.

Configuration tasks	clarification	Detailed Configuration
Configure the device's spanning tree protocol mode to MSTP	compulsory	12.2.2
Configuring MSTP Timer Parameter Values	selectable	12.2.3
Configure the configuration identifier for MSTP	selectable	12.2.4
Configuring MSTP Bridge Priorities	selectable	12.2.5
Configure the border port state of an MSTP port	selectable	12.2.6
Configure the link type of the MSTP port	selectable	12.2.7
Configure MSTP ports for path spending	selectable	12.2.8
Configuring MSTP Port Priority	selectable	12.2.9
Display MSTP configuration information	selectable	12.2.10

12.2.2 Configure the device's spanning tree mode to MSTP

You need to enable the STP function globally and then configure MSTP in spanning tree mode for the MSTP function to take effect.

manipulate	command	clarification
Go to System View	system-view	
Enable STP function globally	stp	
Configuring Spanning Tree Protocol Mode	stp mode mstp	

[Example]

! Enable the STP function and configure the spanning tree mode to MSTP

```
[GPON]stp
[GPON]stp mode mstp
```

12.2.3 Configuring MSTP Timer Parameter Values

MSTP timer parameters include: forward delay, hello time, max age, and max hops.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Forward Delay Time for MSTP	stp mst forward-time *seconds*	Forward Delay is configured in the range of 4-30 seconds, with a default value of 15 seconds
Restore the Forward Delay time for the default MSTP	undo stp mst forward-time	
Configuring MSTP for hello time	stp mst hello-time *seconds*	Hello time is configured in the range of 1-10 seconds, and the default value is 2 seconds.
Restore the default MSTP hello time	undo stp mst hello-time	
Configure the MSTP max age	stp mst max-age *seconds*	Max age is configured in the range of 6-40 seconds, with a default value of 20 seconds.
Restore the default MSTP max age	undo stp mst max-age	
Configure max hops for MSTP	stp mst max-hops *hops*	Max hops configuration range is 1-255 hops, default value is 20 hops
Restore default MSTP max hops	undo stp mst max-hops	

[Example]

! Configure the maximum number of hops for messages on the bridge to 10

```
[GPON]stp mst max-hops 10
```

12.2.4 Configure the configuration identifier for MSTP

MSTP configuration identifiers include: the MSTP configuration name, the MSTP correction level, and the mapping relationship between MSTP instances and VLANs. MSTP treats bridges that have the same configuration identifier and are interconnected with each other logically as a virtual bridge.

manipulate	command	clarification
Go to System View	system-view	
Configure the name of the configuration identifier for MSTP	stp mst name *name*	
Delete the name of the configuration identifier for MSTP	undo stp mst name	
Configure the correction level of the configuration identifier for MSTP	stp mst revision *revision-level*	
Restore the correction level of the configuration identifier of the default MSTP	undo stp mst revision	
Configure the mapping of MSTP instances and VLANs for MSTP configuration identifiers	stp mst instance *instance-num* vlan *vlan-list*	Instance instance configuration ranges from 0-15
Deleting VLAN instances for MSTP	undo stp mst instance *instance-num* vlan *vlan-list*	

[Example]

! Configure the name of the MSTP configuration identifier to be test

[GPON]stp mst name test

! Configure the correction level of the MSTP configuration identifier to 10

[GPON]stp mst revision 10

! Configure VLANs 2~7 to be mapped to spanning tree instance 5

[GPON]stp mst instance 5 vlan 2-7

12.2.5 Configuring MSTP Bridge Priorities

In MSTP, the bridge priority is a parameter based on each spanning tree instance. The bridge priority, together with the port priority and the port path spend, determines the topology of each spanning tree instance, and together they form the basis for achieving link load balancing.

manipulate	command	clarification
Go to System View	system-view	
Configuring MSTP Bridge Priorities	stp mst instance *instance-num* priority *priority*	The bridge priority configuration range is 0-61440, and the default value is 32768
Restore the default MSTP bridge priority	undo stp mst instance *instance-num* priority *priority*	

[Example]

! Configure the bridge to have a priority of 4096 in Example 4

[GPON]stp mst instance 4 priority 4096

12.2.6 Configure the border port state of an MSTP port

As with SST, a port with the boundary port attribute enters the forwarding state immediately after linking up if it does not receive a spanning tree message after two packet-sending cycles.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the port as a border port	stp mst portfast	
Configure the port as a non-border port	undo stp mst portfast	

[Example]

! Configure Ethernet port 1 as a border port

[GPON-ethernet-0/0/1]stp mst portfast

12.2.7 Configure the link type of the MSTP port

There are two types of link types for ports: shared media link types (links through hubs, etc.) and point-to-point link types. The link type is mainly used in the port state fast transition of the recommendation-consent mechanism, only the link type for the point-to-point port to allow fast transition of the port state, the link type can be specified manually or by the spanning tree protocol automatically detects.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the link type of the MSTP port	stp mst link-type point-to-point { forcetrue | forcefalse | auto }	

[Example]

! Configure the link type of Ethernet port 2 to be a forced non-point-to-point

[GPON-ethernet-0/0/2]stp mst link-type point-to-point forcefalse

12.2.8 Configure MSTP ports for path spending

The path spend of a port is categorized into internal spend, which is a configuration parameter based on each MSTP instance and is used to determine the topology of the different instances within each MSTP region, and external spend, which is an instance-independent parameter and is used to determine the topology of the CSTs comprising each region.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the path spend for MSTP ports	stp mst instance *instance-num* cost *cost*	Cost configuration range is 1-200000000, the default value is 200000
Path spend to restore the default MSTP port	undo stp mst instance *instance-num* cost	
Configuring external path spend for MSTP ports	stp mst external cost *cost*	External Cost configuration range is 1-200000000, default value is 200000
Restore external path spend for default MSTP ports	undo stp mst external cost	

[Example]

! Configure Ethernet port 2's path spend inside instance 1 to 10

[GPON-ethernet-0/0/2]stp mst instance 1 cost 10

! Configure the external path spend for Ethernet port 2 to 10

[GPON-ethernet-0/0/2]stp mst external cost 10

12.2.9 Configuring MSTP Port Priority

Port prioritization in MSTP is based on parameters for each spanning tree instance.

manipulate	command	clarification
Go to System View	system-view	

Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring MSTP Port Priority	stp mst instance *instance-num* port-priority *priority*	The port priority configuration range is 0-240, the value must be an integer multiple of 16, and the default value is 128.
Restore the default MSTP port priority	undo stp mst instance *instance-num* port-priority	

[Example]

! Configure Ethernet port 2 to have priority 16 in instance 1

[GPON-ethernet-0/0/2]stp mst instance 1 port-priority 16

12.2.10 Display MSTP configuration information

The basic information of MSTP consists of two parts, one is the configuration identifier information of MSTP (including configuration name, correction level, and the mapping relationship between vlan and MSTP instance), and the other is the configuration information of spanning tree instance and port.

manipulate	command	clarification
Displaying MSTP Configuration Marker Information	display stp mst *config-id*	
Display port information for MSTP instances	display stp mst instance *instance-num* interface ethernet [*interface-list*]	Display MSTP information for multiple ports at once

[Example]

! Display information about MSTP configuration identifiers

[GPON]display stp mst config-id

! Display information about Ethernet port 2 within instance 1

[GPON]display stp mst instance 1 interfaceethernet 0/0/2

Chapter 13 Remote Loop Detection Function Configuration

13.1 Introduction to Remote Loop Detection Function

When a device is applied in a multilayer cascade, if the device in the middle layer turns off spanning tree, the BPDU message sent by the upper layer device may be terminated by the middle layer device, so that when a loop occurs in the network below the middle layer, the upper layer device will not be able to detect the occurrence of the loop, and the far-end loop detection function is a complementary treatment for this situation.

After enabling the remote loop detection function, the device will send out a remote loop detection message, which is encapsulated and sent in the form of a broadcast message. If this broadcast message is sent from a port of the device and then received on this port or other ports of the device, it indicates that there is a loop in the network under the device, and the device will process the loop port in shutdown or set it to the discovering state.

13.2 Remote Loop Detection Function Configuration

13.2.1 Remote Loop Detection Function Configuration Task List

The remote loop detection function configuration list is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable remote loop detection	compulsory	13.2.2
Configure the remote loop detection processing policy	selectable	13.2.3
Configuring the Remote Loop Detection Message Transmission Interval	selectable	13.2.4
Configuring Remote Loop Detection Port Recovery Time	selectable	13.2.5
Display remote loop detection status information	selectable	13.2.6

13.2.2 Enable/disable remote loop monitoring

The system supports globally turning on the far-end loop detection function, which means turning on the far-end loop detection function for all ports. You can also specify to turn on the far-end loop detection function of a certain port, and the related configurations are as follows:

manipulate	command	clarification
Go to System View	system-view	
Enable remote loop detection	stp remote-loop-detect interface [ethernet [*interface-list*]]	When no port is specified, it means that the remote loop detection function is turned on for all ports.
Disable Remote Loop Detection	undo stp remote-loop-detect interface [ethernet [*interface-list*]]	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable remote loop detection for specified ports	stp remote-loop-detect	
Disable remote loop detection for specified ports	undo stp remote-loop-detect	

[Example]

! Enable remote loop detection on Ethernet port 1 in system view

```
[GPON]stp remote-loop-detect interface ethernet 0/0/1
```

! Disable far-end loop detection on Ethernet port 1 in port view

[GPON-ethernet-0/0/1]undo stp remote-loop-detect

13.2.3 Configure the remote loop detection processing policy

After the system detects the existence of a far-end loop, it supports the policy processing of the loop port, and the processing policy includes shutting down the loop port, or putting the loop port into the discarding state and not forwarding service data.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Remote Loop Detection Handling Policy	stp remote-loop-detect action { shutdown | discarding }	The default processing strategy is discarding

[Example]

! Configure the remote loop detection handling policy to shutdown

[GPON]stp remote-loop-detect action shutdown

13.2.4 Configuring the Remote Loop Detection Message Transmission Interval

The system supports configuring the sending interval of remote loop detection messages, and the related configurations are as follows:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Remote Loop Detection Message Transmission Interval	stp remote-loop-detect interval-time *interval-time*	Configure the sending interval from 5 to 300 seconds, with a default value of 5 seconds.

[Example]

! Configure the remote loop detection message sending interval to 10 seconds

[GPON]stp remote-loop-detect interval-time 10

13.2.5 Configuring Remote Loop Detection Port Recovery Time

The system supports configuring the remote loop detection port recovery time, after the recovery time is up, the port will reopen and resend messages for loop detection, the relevant configurations are as follows:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Remote Loop Detection Message Transmission Interval	stp remote-loop-detect recover-time *recover-time*	The recovery time configuration ranges from 0, 10-600 seconds. Where 0 means never recover, the default value is 20 seconds

[Example]

! Configure the remote loop detection port recovery time to 30 seconds

[GPON]stp remote-loop-detect recover-time 30

13.2.6 Display remote loop detection status information

The remote loop detection status information includes: function configuration status, detection status, processing policy

configuration information, and configuration of message sending interval and port recovery time. You can view the remote loop detection status information in any view mode.

manipulate	command	clarification
Display remote loop detection status information	display stp remote-loop-detect interface [ethernet [*interface-list*]]	When no port is specified, it means to display all port information

[Example]

! Displays remote loop detection status information for all ports

[GPON]display stp remote-loop-detect interface

Chapter 14 ACL Configuration

14.1 ACL Introduction

14.1.1 ACL Overview

ACL (Access Control List), mainly used to realize the identification and control of network data. In order to filter packets, network devices need to configure a series of packet matching rules to identify the objects to be filtered. After identifying a specific object, the packet is allowed or prohibited to pass according to a predefined policy.

ACLs classify packets according to a series of matching conditions, which include the source MAC address, destination MAC address, source IP address, destination IP address, L4 port number, VLAN, 802.1P priority, DSCP priority, and so on. The device detects the packet according to the conditions specified in the ACL, and then decides whether to forward or discard the packet through the set rules.

The packet matching rules defined by ACLs can also be referenced by other actions that need to classify flows, such as flow mirroring, flow statistics, message redirection, flow rate limiting, message copy CPU, and flow priority marking in the definition of flow classification rules in QoS.

14.1.2 ACL Classification

Access control lists are divided into the following categories:

An access control list (ACL) is a control list of instructions applied to a device that are used to tell the device which packets can be received and which packets need to be rejected. It is composed of a series of judgment statements. After activating a control list, the device will check every packet entering the device according to the judgment conditions given in this access control list, and the packets that meet the conditions will be allowed and discarded according to the access control list.

In the system, access control lists are divided into the following categories:

- Standard access control lists based on numeric identifiers
- Standard access control lists based on name identification
- Extended access control lists based on numeric identifiers
- Extended access control lists based on name identification
- Layer 2 access control lists based on numeric identifiers
- Layer 2 access control lists based on name identification

A limit on the number of access control lists:

Standard access control lists based on numeric identifiers	1-99	99
Extended access control lists based on numeric identifiers	100-199	100
Layer 2 access control lists based on numeric identifiers	200-299	100
Standard access control lists based on name identification	--	1000
Extended access control lists based on name identification	--	1000
Layer 2 access control lists based on name identification	--	1000
Number of subrules that can be configured for an ACL	0-127	128
time period	--	128
An absolute time period that can be configured for a time period	--	12
Periodic time periods that can be configured for a time period	--	32

14.2 ACL Configuration

14.2.1 ACL Configuration Task List

The list of ACL configuration considerations is as follows.

Configuration tasks	clarification	Detailed Configuration
ACL Match Order Configuration	selectable	14.2.2
Configure the time period	selectable	14.2.3
Configuring Standard ACLs	compulsory	14.2.4
Configuring Extended ACLs	compulsory	14.2.5
Configuring Layer 2 ACLs	compulsory	14.2.6
Activate ACL	compulsory	14.2.7
ACL monitoring and maintenance	selectable	14.2.8

It is recommended to configure the time period first, then define the access control list in which the defined time period will be referenced, and finally activate the access control list to make it effective.

14.2.2 ACL Match Order Configuration

An ACL can be composed of multiple "permit | deny" statements, and each statement matches different packet ranges, there is a match order problem when matching a packet with an access control rule. You can use the following command to set the match order of access control rules:

manipulate	command	clarification
Go to System View	system-view	
Configuring ACL Matching Order	acl *{acl-number* | acl-name} match-order { config | auto }	

acl-number: access control list serial number, a number between 1 and 299.

acl-name: access control list name.

config: Specifies the order in which the rules are to be matched according to the user's configuration.

auto: Specifies that the system automatically sorts the rules when they are matched (in "depth-first" order).

By default the matching order is sorted by user's configuration, i.e. "config". Once a user specifies the matching order of an access control rule, the order cannot be changed unless the rule is deleted and the matching order is specified again.

The "depth-first" principle used by auto: the statement that specifies the smallest range of packets is placed last. This can be accomplished by comparing the wildcards of the addresses; the smaller the wildcard, the smaller the range of the specified host. For example, 192.168.2.1 0 specifies a host: 192.168.2.1, while 192.168.2.1 0.0.0.255 specifies a network segment:

192.168.3.1 ～ 192.168.3.255, obviously the former comes last in the access control rules. The specific criteria are:

For standard access control rule statements, the source address wildcards are compared directly, and those with the same wildcard are in the configured order;

For Layer 2 access control rules, the rule configured with "any" comes first, and the others are in the order of configuration;

For extended access control rules, first compare the source address wildcard, then compare the destination address wildcard if it is the same, and then compare the range of the port number if it is still the same, and the one with a smaller range will be at the back, and if the range of the port number is also the same, then it will be in the configured order.

For user-defined access control rules, the mask lengths are compared, the longer masks are placed at the end, and the masks are the same in the configured order.

[Example]

! Configure numeric identity-based ACLs and configure the ACL match order to auto

[GPON] acl 2 match-order auto

! Configure an ACL based on name identification and configure the ACL match order to auto

[GPON] acl standard test match-order auto

14.2.3 Time Period Configuration

manipulate	command	clarification
Go to System View	system-view	
Go to the time period view	time-range time-range-name	This command automatically creates a time period when no time period configuration has been created.
Delete time period	undo time-range *time-range-name*	
Configuring Absolute Time Period Entries	absolute [start start-time date] [end end-time date]	
Deletion of Absolute Time Period Entries	undo absolute [start *start-time date*] [end *end-time date*]	
Configuring cycle time period parameters	periodic days-of-the-week hh:mm:ss to [day-of-the-week] hh:mm:ss	
Delete cycle time period parameter	undo periodic days-of-the-week hh:mm:ss to [days-of-the-week] hh:mm:ss	

Configuring time periods is divided into two forms: configuring absolute time ranges and configuring periodic time ranges. Configure the absolute time range to use time in the form of year, month, day, hour, and minute, and configure the periodic time range to use time in the form of day of week, time of day, and minute of week.

Configure the absolute time: if you do not configure the start time, it means that there is no limit on the start time, only the end time is of interest. If no end time is configured, the end time is the maximum time the system can indicate. The end time must be greater than the start time. The absolute time range determines a large effective time and also limits the time range for the cycle time range in which it takes effect. There are 12 absolute time ranges that can be configured.

Create cycle time:

Cycle time ranges have an effective period of one week. A maximum of 32 cycle time ranges can be configured.

[Example]

! Configure the absolute time period, taking the value from 04:00 October 1, 2014 to 04:00 October 2, 2014

[GPON]time-range test

[GPON-timerange-test] absolute start 04:00:00 2014/10/01 end 04:00:00 2014/10/02

14.2.4 Configuring Standard ACLs

Standard ACLs set up matching rules based on the source IP address of the message and analyze the original IP address of the packet accordingly.

If the standard ACL is identified by a number, then the ACL serial number takes a value in the range of 1-99, and a maximum of 99 standard ACLs identified by numbers can be created.If the standard ACL is identified by a name, then a maximum of 1000 can be defined. You can also define up to 128 subrules per ACL. If you want to configure a rule with a time period parameter, you need to define the corresponding time period first.

Configure standard ACLs based on numeric identifiers:

manipulate	command	clarification
Go to System View	system-view	
Configure standard ACLs based on numeric identifiers	acl *acl-number* { deny | permit } { *source-addr source-wildcard* | any } [fragments] [time-range *time-range-name*]	If you need to quote the time period configuration, you need to configure the time period first
Define the ACL match order	acl *acl-number* match-order { config | auto }	This item can be left out if the default auto match order is used.
Deleting ACLs	undo acl { all | { *acl-number* | name *acl-name* } [*subitem*] }	

Configure standard ACLs based on name identification:

manipulate	command	clarification
Go to System View	system-view	
Enter standard ACL view based on name identification	acl standard *acl-name* [match-order { config | auto }]	If no ACL of this name has been created, the system automatically creates an ACL of this name.
Configuring ACL Rules	{ permit | deny } { *source-addr source-wildcard* | any } [fragments] [time-range *time-range-name*]	
Deleting ACLs	undo acl { all | { *acl-number* | name *acl-name* } [subitem] }	

[Example]

! Configure a standard ACL based on numeric identifiers to prohibit messages with source IP address 192.168.1.100 from passing through the

[GPON] acl 2 deny 192.168.1.100 0

! Configure a standard ACL based on name identification to allow messages with source IP address 192.168.2.100 to pass through the

[GPON] acl standard teststandard

[GPON-std-nacl-teststandard] permit192.168.2.100 0

Description:

- Defining an ACL based on name identification requires access to a specialized view, which can be exited with the command quit.
- When defining ACL rules, you can use the {permit|deny} command multiple times to define multiple rules for the same ACL.
- Once you specify the matching order of an ACL, you cannot change the order, and if you need to change it, you need to delete the ACL first and then re-create it. By default, the ACL matching order is configured by the user (config).

14.2.5 Configuring Extended ACLs

Extended ACL can set up matching rules based on message source IP address, destination IP address, TCP or UDP source port number, TCP or UDP destination port number, message IP priority, ToS priority, DSCP priority, etc., and analyze and process packet IP header related parameters accordingly.

If the extended ACL is identified by a number, then the ACL serial number takes a value in the range of 100-199, and a maximum of 99 extended ACLs identified by numbers can be created.If the extended ACL is identified by a name, then a maximum of 1000 can be defined. You can also define up to 128 subrules per ACL. If you want to configure a rule with a time period parameter, you need to define the corresponding time period first.

Configure extended ACLs based on numeric identifiers:

manipulate	command	clarification
Go to System View	system-view	
Configure extended ACLs based on numeric identifiers	acl acl-number { permit | deny } [protocol] [established] { source-addr source-wildcard | any } [port [portmask]] { dest-addr dest-wildcard | any } [port [portmask]] [icmp-type [icmp-code]] [fragments] { [precedence precedence] [tos tos] | [dscp dscp] } [time-range time-range-name]	If you need to quote the time period configuration, you need to configure the time period first
Define the ACL match order	acl *acl-number* match-order { config | auto }	This item can be left out if the default auto match order is used.
Deleting ACLs	undo acl { all | { *acl-number* | name *acl-name* } [*subitem*] }	

Configure extended ACLs based on name identification:

manipulate	command	clarification
Go to System View	system-view	
Enter name identity-based extended ACL view	acl *extendedacl-name* [match-order { config | auto }]	If no ACL of this name has been created, the system automatically creates an ACL of this name.
Configuring ACL Rules	{ permit | deny } [*protocol*] [established] { *source-addr source-wildcard* | any } [*port* [*portmask*]] { *dest-addr dest-wildcard* | any } [*port* [*portmask*]] [*icmp-type* [*icmp-code*]] { [precedence *precedence*] [tos *tos*] | [dscp *dscp*] } [fragments] [time-range *time-range-name*]	
Deleting ACLs	undo acl { all | { *acl-number* | name *acl-name* } [*subitem*] }	

[Example]

! Configure an extended ACL based on numeric identifiers to prohibit messages with source IP address 192.168.1.100 and destination IP address 192.168.2.100 from passing through the

```
[GPON] acl 100 deny 192.168.1.100 0 192.168.2.100 0
```

! Configure extended ACLs based on name identifiers to allow TCP packets with source IP address 192.168.1.100, source port number 1111, destination IP 192.168.2.100, and destination port number 21 to pass through the

```
[GPON] acl extended testextended
[GPON-ext-nacl-testextended] permit tcp 192.168.1.100 0 1111 192.168.2.100 0 21
```

Description:

The port parameter in the above configuration commands refers to the TCP or UDP port number used by various high-level applications. For some common port numbers, you can replace the actual number with the corresponding mnemonic, for example, you can use "ftp" to replace port 21.

14.2.6 Configuring Layer 2 ACLs

Layer 2 ACLs can set matching rules based on Layer 2 information such as message source MAC address, destination MAC address, VLAN, VLAN priority, Layer 2 protocol type, message Layer 2 receive port, message Layer 2 forwarding port, and other Layer 2 information, and analyze and process packet Layer 2 related parameters accordingly. If a Layer 2 ACL is identified by a number, then the ACL serial number ranges from 200 to 299, and up to 99 Layer 2 ACLs identified by numbers can be created. if a Layer 2 ACL is identified by a name, then up to 1000 ACLs can be defined. Also a maximum of 128 subrules can be defined for each ACL. If you want to configure a rule with a time period parameter, you need to define the corresponding time period first.

Configure Layer 2 ACLs based on numeric identifiers:

manipulate	command	clarification
Go to System View	system-view	
Configure Layer 2 ACLs based on numeric identifiers	acl acl-number { permit | deny } [protocol] [cos vlan-pri] ingress { { { [source-start-vlan-id source-end-vlan-id] [inner-vid source-inner-vlan-id] [source-mac-addr source-mac-wildcard] [interface ethernet interface-num] } | any } egress { dest-mac-addr dest-mac-wildcard] | any } [time-range time-range-name]	If you need to quote the time period configuration, you need to configure the time period first
Define the ACL match order	acl *acl-number* match-order { config | auto }	This item can be left out if the default auto match order is used.
Deleting ACLs	undo acl { all | { *acl-number* | name *acl-name* } [*subitem*] }	

Configure a Layer 2 ACL based on name identification:

manipulate	command	clarification
Go to System View	system-view	
Enter name identity-based Layer 2 ACL view	acl link *acl-name* [match-order { config | auto }]	If no ACL of this name has been created, the system automatically creates an ACL of this name.
Configuring ACL Rules	{ permit | deny } [protocol] [cos vlan-pri] ingress { { [source-start-vlan-id source-end-vlan-id] [inner-vid source-inner-vlan-id] [source-mac- addr source-mac-wildcard] [interface ethernet interface-num] } | any } egress { dest-mac-addr dest-mac-wildcard] | any } [time-range time-range- name]	

Deleting ACLs	undo acl { all | { *acl-number* | name *acl-name* } [*subitem*] }	

[Example]

! Configure a Layer 2 ACL based on numeric identifiers to prohibit messages with source MAC address 00:E1:4B:15:E5:1C, VLAN ID 100, and destination MAC address 00:1B:2D:68:76:3E from passing through the

[GPON]acl 200 deny 100 ingress 00:E1:4B:15:E5:1C 0 egress 00:1B:2D:68:76:3E 0

! Configure a name identity-based Layer 2 ACL to allow messages with source MAC address 00:E1:4B:15:E5:1C, VLAN ID 200, VLAN priority 5, and destination MAC 00:1B:2D:68:76:3E to pass through the

[GPON] acl link testlink

[GPON-link-nacl-testlink] permit 200 cos 5 ingress 00:E1:4B:15:E5:1C 0 egress 00:1B:2D:68:76:3E 0

14.2.7 Activate Access Control Lists

After an ACL is defined, it must be activated for it to take effect, and the activation configuration is as follows:

manipulate	command	clarification
Go to System View	system-view	
Activate ACL	access-group { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	
De-activate ACL	undo access-group { all | { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] } }	

Description:

The system supports the simultaneous combination of Layer 2 and Layer 3 ACLs, but the actions of the combined items are required to be the same, and cannot be activated if the actions are conflicting (one is permit and the other is deny). The device uses parallel combination to activate Layer 2 and Layer 3 access control lists, that is, subitem 1 of Layer 2 ACL is combined with subitem 1 of Layer 3 ACL, subitem 2 of Layer 2 ACL is combined with subitem 2 of Layer 3 ACL, and so on. If the number of subitems of two groups of ACLs is not equal, the extra subitems need to be activated separately.

14.2.8 ACL monitoring and maintenance

You can view the relevant configuration and activation status information of ACLs at any attempt:

manipulate	command	clarification
Show time period status	display time-range [all | statistic | name *time-range-name*]	
Display detailed configuration information for ACLs	display acl config { all | *acl-number* | name *acl-name* }	
Display ACL statistics	display acl config statistic	
Displays information about the downstream application of ACLs	display acl runtime { all | *acl-number* | name *acl-name* }	
Displays statistics on the downstream applications of ACLs	display acl runtime statistic	

Chapter 15 QoS Configuration

15.1 Introduction to QoS

In traditional packet networks, all messages are treated equivalently without distinction, and each network device uses a first-in-first-out (FIFO) policy for all messages, which does its best effort (Best-Effort) to deliver the message to the destination, but does not provide any commitment or guarantee for the transmission performance of the message delivery in terms of latency, delay jitter, and so on.

With the high-speed development of computer networks, people's requirements for networks are getting higher and higher. Because of the bandwidth, delay, jitter-sensitive voice, image, important data increasingly transmitted on the network, on the one hand, making the online business resources greatly enriched, on the other hand, due to frequent network congestion, people on the network transmission of quality of service (Quality of Service, referred to as QoS) puts forward a higher demand. Ethernet is the most widely used network technology today. Currently, Ethernet has not only become the dominant technology in a variety of independent LANs, but many Ethernet LANs have also become part of the Internet network. With the continuous development of Ethernet technology, Ethernet access will become one of the main access methods for the general Internet users. Therefore, in order to realize end-to-end network-wide QoS solution, it is inevitable to consider the problem of QoS service guarantee on Ethernet. This requires Ethernet switching equipment to apply Ethernet QoS technology to provide different levels of QoS assurance for different types of service flows, especially to support those service flows with higher requirements for delay and jitter.

1. Streams

A flow is a service flow (traffic), which refers to all messages that pass through the device.

2. Stream classification

Traffic classification refers to the use of certain rules to identify messages that meet certain characteristics. Classification rule refers to the filtering rules configured by the configuration administrator according to the management requirements. It can be very simple, such as identifying the traffic with different priority characteristics based on the ToS field in the IP message header; it can also be very complex, such as the integrated link layer (Layer 2), network layer (Layer 3), and transport layer (Layer 4) information, such as MAC address, IP protocol, source address, destination address, or application port number. It can also be very complex, such as combining link layer (Layer 2), network layer (Layer 3), and transport layer (Layer 4) information, such as MAC address, IP protocol, source address, destination address, or port number of an application program, to classify messages, i.e., a complex flow classification rule. The general classification basis is limited to the header information of the encapsulated message, and it is rare to use the content of the message as a criterion for classification.

3. Access Control Lists (ACLs)

The purpose of stream classification is to provide services differentially, and it must be associated with some kind of flow control and resource allocation action in order to be meaningful. The ability to associate flow rules with flow actions, such as packet filtering, bandwidth management, mirroring, and flow statistics, can be achieved by utilizing Access Control Lists (ACLs). The specific flow control actions to be taken are related to the stage in which they are taken and the current load condition of the network. For example, when the message enters the network based on the average rate of commitment to regulate the message, flow out of the node before the queue scheduling management.

4. Packet filtering

Packet filtering is the process of performing filtering operations on business flows, such as a drop operation (deny), whereby a business flow that matches a flow classification rule is dropped and all other traffic is allowed to pass. Since the system uses complex flow classification rules, this allows filtering of all kinds of information for the Layer 2 messages of a business flow, discarding useless, unreliable, and questionable business flows, thus enhancing the security of the network.

To realize packet filtering, there are two key aspects:

The first step: is to categorize the flow of traffic entering the port according to established rules;

Step 2: Filter the distinguished streams - drop the operation (deny). deny is the default access control operation.

5. Flow regulation

In order to make limited network resources work better for users, QoS can regulate the service flow of a particular user on an input port to adapt to the portion of network resources allocated to it.

6. Outlet bandwidth limitation

The egress bandwidth limit is based on the rate limitation of the port and limits the total rate of the port's output messages.

7. Entrance bandwidth limitation

Ingress bandwidth limiting is based on port rate limiting, which limits the total rate of incoming messages to a port.

8. Redirection

Users can reassign the forwarding port of the message based on the needs of their own QoS policy.

9. Priority marking

The service of priority marking can be provided for specific messages. The markings include TOS, DSCP, 802.1p, etc. These priority markings are applicable to different QoS models and are defined in different models.

10. Select port output queue for messages

The corresponding output queue can be selected for a specific message.

11. Queue scheduling

When the network is congested, the problem of multiple messages competing for resources at the same time must be solved, and queue scheduling is usually used to solve it. Here we introduce four distinctive queue scheduling algorithms, Strict-Priority Queue (PQ) scheduling, Weighted Round Robin (WRR) scheduling and WRR algorithm with maximum delay and Strict-Priority + Weighted Round Robin scheduling.

(1) PQ

PQ (Priority Queueing) queue scheduling, is designed for business-critical applications. An important characteristic of business-critical services is that they require priority of service when congestion occurs in order to reduce the response latency. Priority Queueing divides all messages into a maximum of eight categories, (in order of 7, 6, 5, 4, 3, 2, 1, 0 queue), their priority decreases in turn.

In queue scheduling, PQ sends packets in the higher priority queue strictly in the order of priority from high to low, and when the higher priority queue is empty, then sends packets in the lower priority queue. In this way, putting the packets of critical services into the higher priority queue and putting the packets of non-critical services (such as E-Mail) into the lower priority queue ensures that the packets of critical services are prioritized for transmission, and the packets of non-critical services are transmitted in the idle gaps of processing the critical service data.

The disadvantage of PQ is that when congestion occurs, if there are packets in the higher priority queue for a long period of time, the messages in the lower priority queue will "starve to death" due to lack of service.

(2) WRR

WRR queue scheduling divides each port into four or eight output queues (the device supports eight hardware queues, in order of 7, 6, 5, 4, 3, 2, 1, 0, their priority decreases in turn), and scheduling rotates among the queues to ensure that each queue receives a certain amount of service time, and the WRR can configure a weighted value for each queue (w7, w6, w5, w4, w3, w2, w1, w0, in turn), and the weighted value indicates the proportion of resources obtained. w7, w6, w5, w4, w3, w2, w1, w0) for each queue, and the weighted value indicates the weight of the access to resources. For example, for a 1000M port, configure its WRR queue scheduling algorithm with a weighted value of 8, 7, 6, 5, 4, 3, 2, and 1 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0 in turn), which ensures that the lowest-priority queue will get at least 27 Mbit/s (1000M * 1/(1+2+3+4+5+6+7)) of bandwidth to avoid the problem of low-priority queues when using PQ scheduling. This ensures that the lowest priority queue gets at least 27 Mbit/s (1000M * 1/(1+2+3+6+7)) bandwidth and avoids the disadvantage that messages in the low priority queue may not be served for a long period of time when PQ is used.

Another advantage of WRR queuing is that, although the scheduling of multiple queues is round-robin, but for each queue is not a fixed allocation of service time slice - if a queue is empty, then immediately switched to the next queue scheduling,

so that bandwidth resources can be fully utilized.

(3) WRR Algorithm with Maximum Delay

A special feature of WRR queue scheduling with maximum delay compared to normal WRR is that the maximum time from entry to exit of a message in the highest priority queue is guaranteed not to exceed the set maximum delay.

(4) Strict Priority + Weighted Round Robin Scheduling

Strict priority scheduling algorithm is used for the highest priority queue and WRR algorithm is used for the other queues

12. Mapping between hardware priority queues and 802.1p protocol priorities

The system maps between the 802.1p protocol priority of the message and the hardware queue priority. For each message that enters the device, the system maps to a specific hardware queue priority based on the 802.1p protocol priority in the message.

13. Mapping of DSCP to hardware priority queues

The system maps between the dscp protocol priority of the message and the hardware queue priority. For each message that enters the device, the system maps to a specific hardware queue priority based on the dscp protocol priority in the message.

14. Stream mirroring

Flow mirroring, which is the ability to copy specified packets to a monitor port for network inspection and troubleshooting.

15. Flow-based traffic statistics

Stream-based traffic statistics for statistical analysis of messages of interest to users.

16. Copying of messages to CPU

Users can copy the specified messages to the CPU based on the needs of their own QoS policies.

The system accomplishes QoS functions by referencing access control lists, and the QoS functions it implements include traffic supervision, egress bandwidth limiting, ingress bandwidth limiting, message redirection, priority marking, queue scheduling, flow mirroring, traffic statistics, message copy to CPU, message rewrite vlan, message insertion into vlan, and so on.

15.2 QoS Configuration

15.2.1 QoS Configuration Task List

QoS configuration includes the following tasks:

Configuration tasks	clarification	Detailed Configuration
Configuring Traffic Supervision	selectable	15.2.2
Configuration of two-speed three-color marking	selectable	15.2.3
Configuring Priority Marking	selectable	15.2.4
Configuring Flow Mirroring	selectable	15.2.5
Configuring Traffic Statistics	selectable	15.2.6
Configuring Message Redirection	selectable	15.2.7
Configure message copy to CPU	selectable	15.2.8
Configuring Queue Scheduling	selectable	15.2.9
Configure the mapping of hardware priority queues to 802.1p protocol priorities	selectable	15.2.10
Configure the mapping of DSCP to hardware priority queues	selectable	15.2.11
Configuring Egress Bandwidth Limiting	selectable	15.2.11
Configuring Ingress Bandwidth Limiting	selectable	15.2.12
QOS Monitoring and Maintenance	selectable	15.2.13

The corresponding access control lists should be defined first, and then the above QoS configuration should be performed.

15.2.2 Configuring Traffic Supervision

Traffic supervision is based on flow rate limiting, which monitors the rate of a particular flow entering the device and takes action to discard out-of-specification messages or modify the priority of a message if the flow exceeds a set threshold.

manipulate	command	clarification
Go to System View	system-view	
Configuring Flow-Based Rate Limiting	rate-limit input { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] } { *target-rate* [exceed-action { drop | set-dscp-value *value* }] | two-rate-policer cir *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-value* | transmit } } violate-action { copy-to-cpu | drop | set_dscp_value *dscp -value* | transmit } }	The rate limit range is 64-1048512 Kbps. the default action is drop
Eliminate flow-based rate limiting configuration	undo rate-limit input { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	

Be sure to configure the appropriate ACLs before configuring traffic supervision.

Users can choose between normal rate-limiting regulation (discarding messages that exceed a set rate) and two rate three color marker regulation (two rate three color marker, see RFC2698).

[Example]

! Limit message rate to 2048Kbps for source IP address 192.168.1.100

[GPON]acl 2 permit 192.168.1.100 0

[GPON] rate-limit input ip-group 2 2048

15.2.3 Configuration of two-speed three-color marking

The two-speed, three-color marking feature, defined in RFC 2698, marks messages green, yellow, and red by measuring the IP message stream and evaluating it against four traffic parameters: the CIR, the CBS, the Peak Information Rate (PIR), and the Peak Burst Size (PBS). If the message exceeds the PIR mark it as red, otherwise see if it exceeds the CIR mark it as red or green. Users can set different actions for different colors to transmit, mark or discard messages according to application needs.

manipulate	command	clarification
Go to System View	system-view	
Configuration of two-speed three-color mode	two-rate-policer mode { color-aware | color-blind }	Defaults to blind mode
Restore Default Mode	undo two-rate-policer mode	
Configure color marking of different DSCP messages	two-rate-policer set-pre-color *dscp-value* { green | red | yellow }	
Deleting the DSCP Color Marker Configuration	undo two-rate-policer set-pre-color *dscp-value*	
Configure a two-speed, three-color application policy (processing actions for three different colored messages)	rate-limit input { [ip-group { *num* | *name* } [subitem *subitem*]] [link-group { *num* | *name* } [subitem *subitem*]] } two-rate-policer cir *cir-value* cbs *cbs- value* pir *pir-value* pbs *pbs-value* conform-action { copy-to-cpu | drop |	

	set_dscp_value *dscp_value* | transmit } exceed-action { copy-to-cpu | drop | set_dscp_ value *dscp_value* | transmit } violate-action { copy-to-cpu | drop | set_dscp_value *dscp_value* | transmit }	
Delete the dual-speed, three-color application policy configuration	undo rate-limit input { [ip-group { *num* | *name* } [subitem *subitem*]] [link-group { *num* | *name* } [subitem *subitem*]] }	

Note: The color-blind mode corresponds to the color- aware mode, and the system default is color-blind mode, the differences are as follows:

In color-blind mode, incoming messages are considered colorless, and the color of the message is determined only based on the current rate reaching the set peak value; whereas in color-aware mode, the color of the message is determined not only based on the rate, but also based on the color of the message's parameter matches for marking scheduling.

[Example]

! Configure the dual-speed tri-color mode as color-aware, set dscp20 to yellow and dscp60 to red, and set the corresponding processing action

[GPON] two-rate-policer mode color-aware

[GPON] two-rate-policer set-pre-color 20 yellow

[GPON] two-rate-policer set-pre-color 60 red

[GPON] rate-limit input ip-group 1 subitem 0 two-rate-policer cir 64 cbs 4 pir 10240 pbs 4 conform-action copy-to-cpu exceed-action set_dscp_value 63 violate-action drop

15.2.4 Configuring Priority Marking

Priority tagging configuration is the policy of re-tagging the priority of messages that match an access control list. the tagged priority can be filled in the field reflecting the priority in the header of the message or sent to the specified hardware output queue of the port.

The following commands can be used for priority tagging configuration.

manipulate	command	clarification
Go to System View	system-view	
Configuring Priority Marking	traffic-priority { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] } { [dscp *dscp-value*] [cos *cos-value*] [local-precedence *pre-value*] [precedence *pre-value*] }	
Cancel Priority Marker Configuration	undo traffic-priority { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	

The system supports to prioritize the message with IP priority (the value specified by the precedence in the traffic-priority command), DSCP (the value specified by the dscp in the traffic-priority command), and 802.1p priority (i.e., the cos value in the traffic-priority command). Users can assign different priorities to the messages according to the actual QoS policy requirements. The device puts the message into the corresponding port output queue according to the 802.1p priority of the message, and also supports to put the message into the corresponding port output queue directly according to the local priority (the value specified by the local-precedence in the command) specified in the traffic-priority command. If both 802.1p priority and local-priority are specified, the device will prioritize the 802.1p priority to put the message into the corresponding port output queue.

[Example]

! Configure the message with source IP address 192.168.1.100 to hit 802.1P priority 5, DSCP priority 33

[GPON]acl 2 permit 192.168.1.100 0

[GPON] traffic-priority ip-group 2 cos 5 dscp 33

15.2.5 Configuring Flow Mirroring

Flow mirroring is the process of copying the service flows that match the access control list rules to the specified monitor port for message analysis and monitoring. You can use the following commands to configure flow mirroring.

manipulate	command	clarification
Go to System View	system-view	
Configuring Flow Mirroring	mirrored-to { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] } [interface ethernet *interface-num*]	
Deleting a Flow Mirror Configuration	undo mirrored-to { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	

[Example]

! Configure the message with source IP address 192.168.1.100 to mirror to Ethernet port 7

[GPON]acl 2 permit 192.168.1.100 0

[GPON] mirrored-to ip-group 2 interface ethernet 0/0/7

15.2.6 Configuring Traffic Statistics

Traffic statistics refers to the number of messages that will be matched ACL messages for monitoring the number of packets for a specified service flow.

You can use the following command for traffic statistics configuration.

manipulate	command	clarification
Go to System View	system-view	
Configuring Traffic Statistics	traffic-statistic { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	
Zeroing of statistical information	clear traffic-statistic { all | { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	
Deleting a Traffic Statistics Configuration	undo traffic-statistic { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	
Displaying traffic statistics	display qos-info traffic-statistic	

If you reconfigure the traffic statistics, the corresponding traffic statistics are cleared.

[Example]

! Statistics for messages with source IP address 192.168.1.100

[GPON]acl 2 permit 192.168.1.100 0

[GPON] traffic-statistic ip-group 2

15.2.7 Configuring Message Redirection

Message redirection refers to the redirection of messages matching an ACL to a CPU or a port. after message redirection, messages are no longer forwarded to other ports and are only forwarded to the redirected destination port.

You can use the following command for message redirection configuration.

manipulate	command	clarification
Go to System View	system-view	
Configuring Message Redirection	traffic-redirect { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] } { cpu | interface ethernet *interface-num* }	
Delete Message Redirection Configuration	undo traffic-redirect { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	

[Example]

! Redirects messages with source IP address 192.168.1.100 to Ethernet port 7

[GPON]acl 2 permit 192.168.1.100 0

[GPON] traffic-redirect ip-group 2 interface ethernet 0/0/7

Attention:

- When a message is redirected to a CPU, it will not be forwarded normally. When a message is redirected to a port, the message will not be forwarded to other ports, but only to the configured redirected port.
- The redirection configuration is valid only for rules with the action of permit in the ACL. The redirection feature is generally used for certain protocol messages that require CPU processing, or messages that require the CPU to find routes for them.

15.2.8 Configuration message copy to CPU

Message copy to CPU means to take the message that matches the ACL and make a copy of it to the CPU.

You can use the following commands to configure the message copy to CPU function.

manipulate	command	clarification
Go to System View	system-view	
Configuration message copy to CPU	traffic-copy-to-cpu{ [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	
Delete message copy to CPU configuration	undo traffic-copy-to-cpu { [ip-group { *acl-number* | *acl-name* } [subitem *subitem*]] [link-group { *acl-number* | *acl-name* } [subitem *subitem*]] }	

The message copy to CPU configuration is valid only for rules with the action of PERMIT in the access list.

[Example]

! Copy the message with source IP address 192.168.1.100 to CPU

[GPON]acl 2 permit 192.168.1.100 0

[GPON] traffic-copy-to-cpu ip-group 2

15.2.9 Configuring Queue Scheduling

When the network is congested, the problem of multiple messages competing for resources at the same time must be solved, and queue scheduling is usually used to solve the problem. The system supports configuring queue scheduling mode based on group mode, different ports can refer to different groups and use different scheduling methods. For the queue scheduling algorithm, please refer to the introduction of queue scheduling in Section 15.1.

The system supports three queue scheduling modes: strict priority scheduling, weighted round robin scheduling, and strict priority + weighted round robin scheduling. By default, the device adopts the strict priority scheduling mode. Please configure the queue scheduling algorithm in global mode.

The port references a different queue scheduling group. do the following configuration in port view.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Queue Scheduling Algorithm	queue-scheduler group-id { strict-priority | wrr queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6- weight queue7-weight | sp-wrr queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight }	The system supports 4 group configurations, and the algorithm defaults to SP scheduling
Restore the default queue scheduling algorithm	undo queue-scheduler { *group-id* }	When the group parameter is not entered, it means that all groups are restored to the default SP scheduling algorithm
Enter port view	interface { { ethernet *interface-num* } | interface-name }	
Port Reference Queue Scheduling Algorithm	queue-scheduler *group-id*	The port references the queue scheduling algorithm corresponding to group 1 by default

[Example]

! Configure group1 for WRR scheduling with weights 1:2:3:4:5:6:7:8

Configure group2 for WRR scheduling with weights of 2:2:3:3:4:4:5:5

```
[GPON]queue-scheduler 1 wrr 1 2 3 4 5 6 7 8
[GPON]queue-scheduler 2 wrr 2 2 3 34455
```

! Configure Ethernet port 1 to reference the queue scheduling algorithm corresponding to group1

Configure Ethernet port 2 to reference the queue scheduling algorithm corresponding to group2

```
[GPON-ethernet-0/0/1] queue-scheduler 1
[GPON-ethernet-0/0/2] queue-scheduler 2
```

15.2.10 Configure the mapping of hardware priority queues to 802.1P protocol priorities

The system supports 8 hardware priority queues from 0 to 7, with 7 having the highest priority. The system prioritizes sending packets in the chip queue with high priority. The system supports configuring 802.1P priority mapping relationship based on group mode. Different ports can refer to different groups and use different 802.1P priority mapping relationships. By default, the mapping of 802.1P priorities to hardware queues is as follows:

802.1p: 0 1 2 3 4 5 6 7

Hardware queue priority: 0 1 2 3 4 5 6 7

The following command can be used to set the mapping relationship between the system's eight hardware priority queues and the eight priorities defined in the 802.1P protocol, i.e., the cos-amp mapping relationship, to deliver the specified 802.1P priority packets to the specified hardware queues.

manipulate	command	instructions
Go to System View	system-view	
Configure the cos-map mapping relationship	queue-scheduler cos-map group-id queue-number packed-priority	The system supports 4 cos-map group configurations
Enter port view	interface { { ethernet interface-num } | interface-name }	
Port reference cos-map mapping	queue-scheduler cos-map *group-id*	The port references the cos-map mapping relationship corresponding to group 1 by default

[Example]

! Configure cos-map for group 1 to map 802.P priority 5 messages to hardware priority queue 7

[GPON]queue-scheduler cos-map 1 7 5

! Ethernet port 7 references 802.1p protocol priority 5 mapped to hardware priority queue 7

[GPON-ethernet-0/0/7] queue-scheduler cos-map 1

15.2.11 Configure the mapping of DSCP to hardware priority queues

DSCP is the high 6 bits in the ToS field of a Layer 3 message, with values ranging from 0-63. By default, this mapping relationship is turned off. When turned on, it distributes the dscp evenly among the different priorities.

This command is used to set the mapping relationship between the 64 DSCP values of the system and the 8 hardware priority queues.

The system supports configuring DSCP priority mapping relationships based on group mode. different ports can refer to different groups and use different DSCP priority mapping relationships.

manipulate	command	clarification
Go to System View	system-view	
Enable dscp-map mapping function	queue-scheduler dscp-map	
Disable the dscp-map mapping function	undo queue-scheduler dscp-map	
Configure the dscp-map mapping relationship	queue-scheduler dscp-map group-id dscp-value queue-number	The system currently supports only 1 dscp-map group configuration
Enter port view	interface { { ethernet interface-num } | interface-name }	
Port reference dscp-map mapping	queue-scheduler dscp-map *group-id*	The port references the dscp-map mapping relationship corresponding to group 1 by default

[Example]

! Configure dscp-map for group 1 to map DSCP priority 30 messages to hardware priority queue 7

[GPON]queue-scheduler dscp-map 1 307

! Ethernet port 7 references DSCP protocol priority 30 mapped to hardware priority queue 7

[GPON-ethernet-0/0/7] queue-scheduler dscp-map 1

15.2.12 Configuring Egress Bandwidth Limiting

Egress bandwidth limiting is port-based egress rate limiting, which can limit the total rate of output messages from a port.

You can use the following commands for egress bandwidth limit configuration.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configuring Egress Bandwidth Limiting	bandwidth egress kbps *target-rate*	Egress bandwidth limit can be configured in the range of 64-10000000kbps, the port does not do egress bandwidth limit by default
Removal of exit bandwidth speed limit	undo bandwidth egress	

[Example]

! Set the egress bandwidth of Ethernet port 7 to 2048kpbs

[GPON-ethernet-0/0/7] bandwidth egress kbps 2048

15.2.13 Configuring Ingress Bandwidth Limiting

Ingress bandwidth limiting is a port-based ingress rate limitation that limits the total rate of incoming messages to a port.

You can use the following command for ingress bandwidth limit configuration.

manipulate	command	instructions
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configuring Egress Bandwidth Limiting	bandwidth ingress kbps *target-rate*	Ingress bandwidth limit can be configured in the range of 64-10000000kbps, the port does not do ingress bandwidth limit by default
Removal of exit bandwidth speed limit	undo bandwidth ingress	

[Example]

! Set the ingress bandwidth of Ethernet port 7 to 1024kpbs

[GPON-ethernet-0/0/7] bandwidth egress kbps 1024

15.2.14 QOS Monitoring and Maintenance

The system supports the management and viewing of QoS-related configuration and monitoring information, which can be viewed by executing the following commands under any attempt.

manipulate	command	instructions
Displays the parameter settings for all QoS actions	display qos-info all	

Display statistics for all QoS actions	display qos-info statistic	
Displays the parameter settings for flow supervision	display qos-interface ethernet [*interface-num*] rate-limit	
Displays the parameter settings for priority marking	display qos-info traffic-priority	
Displays the parameter settings for stream mirroring	display qos-info mirrored-to	
Displaying Traffic Statistics	display qos-info traffic-statistic	
Displays the parameter settings for message redirection	display qos-info traffic-redirect	
Parameter settings for displaying message copies to the CPU	display qos-info traffic-copy-to-cpu	
Display queue scheduling mode and parameters	display queue-scheduler [*group-id*]	
Displays the mapping between hardware priority queues and 802.1p protocol priorities	display queue-scheduler cos-map [*group-id*]	
Displays the mapping between hardware priority queues and dscp protocol priorities	display queue-scheduler dscp-map [*group-id*]	
Display QoS configuration information for all ports	display qos-interface all	
Display QoS configuration for individual ports	display qos-interface interface ethernet [*interface-num*]	
Display QoS configuration statistics for all ports	display qos-interface statistic	Ports with QoS actions configured will display this statistic; ports with no QoS actions configured will not display it

15.3 QACL Configuration Example

15.3.1 Using QACL for bandwidth control

1. Introduction to bandwidth control

Bandwidth control refers to limiting the rate of a particular stream. This can be accomplished using QACL.

2. Configuration examples

Use QACL to implement the bandwidth control function for streams with a source mac address of 00:01:02:03:04:05, an upstream port of Ethernet port 1, and a downstream port of Ethernet port 8, setting the upstream rate to 2 Mbps and the downstream rate to 4 Mbps.

The configuration steps are as follows:

1) Define the required ACLs

! Define the ACL for forwarding messages whose source port is Ethernet port 8 and whose source MAC address is 00:01:02:03:04:05

[GPON]acl 200 permit ingress 00:01:02:03:04:05 0:0:0:0:0:0 interface ethernet 0/0/8 egress any

! Define the ACL for forwarding messages whose source port is Ethernet port 1 and whose source MAC address is 00:01:02:03:04:05

[GPON]acl 201 permit ingress 00:01:02:03:04:05 0:0:0:0:0:0 interface ethernet 0/0/1 egress any

2) Configure traffic supervision

Please configure the following in system view

[GPON]rate-limit input link-group 2002048

[GPON]rate-limit input link-group 2014096

15.3.2 Deny all packet expect using QACLs

1.Deny all packet expect function introduction

The Deny all packet expect function is to drop all packets other than those specified by the user to be forwarded. This function can be realized by configuring QACL rules.

2. Configuration examples

Configure the deny all packet expect PPPoE function. the protocol numbers of PPPoE messages are 0x8863 (34915 in decimal) and 0x8864 (34916 in decimal). Therefore the following QACL rules can be configured:

1) Discard all messages

2) Forwarding PPPoE messages

The configuration steps are as follows:

1) Define the required ACLs

! Configure an ACL to drop all messages

[GPON]acl 200 deny ingress any egress any

! Configuring ACLs for Forwarding PPPoE Messages

[GPON]acl 200 permit 34915 ingress any egress any

[GPON]acl 200 permit 34916 ingress any egress any

2) Activate ACL

[GPON]access-group link-group 200

15.3.3 Using QACL Anti-Virus

1. Introduction to QACL Antivirus

Reasonable configuration of QACL rules can play the role of a firewall to prevent viruses from spreading through the network and mitigate the impact of viruses on the network. Since different viruses will have different attack behaviors (e.g., attacking different ports), it is necessary to configure different QACL rules for different viruses in order to play an effective preventive role. As for the attack behaviors of various viruses, you can obtain them from professional anti-virus companies.

2. Configuration examples

Use QACL to prevent the spread of the Shockwave virus.

The Shockwave virus attacks the computer's TCP port 135 and spreads the virus through UDP port 69 and TCP port 4444. Therefore, as long as you configure QACL rules in the device that block the forwarding of these messages, you can effectively prevent the virus from spreading in the network.

The configuration steps are as follows:

1) Define the required ACLs

! Configure an ACL to block TCP messages with destination port 135

```
[GPON]acl 100 deny tcp any any eq 135
```

! Configure an ACL to block UDP packets with destination port 69

```
[GPON]acl 100 deny udp any any eq 69
```

! Configure an ACL to block TCP packets with destination port 4444

```
[GPON]acl 100 deny tcp any any eq 4444
```

2) Activate ACL

```
[GPON]access-group ip-group 100
```

Chapter 16 SSH Configuration

16.1 Introduction to SSH

SSH is an abbreviated form of "Secure Shell". Users can log in to the device through a standard SSH client to establish a secure connection with the device. The data transmitted through the SSH connection is encrypted, which ensures that sensitive data such as passwords and management and configuration data transmitted between the user and the device are not overheard or illegally accessed by third parties.

SSH can replace Telnet and provide a means for users to securely manage and configure devices.

16.2 SSH Configuration

16.2.1 SSH Configuration Task List

SSH configuration includes the following tasks.

Configuration tasks	clarification	Detailed Configuration
Enable/disable device SSH function	compulsory	16.2.2
Configuring SSH Keys	selectable	16.2.3
Clearing the key configuration	selectable	16.2.4
Configure a limit on the number of SSH user logins	selectable	16.2.5
SSH Monitoring and Maintenance	selectable	16.2.6

▪

16.2.2 Enable/disable SSH function

Turn the device SSH function on or off in system view. Users cannot log on to the device using the SSH client when the SSH function is off. To enable users to log on to the device with the SSH client, in addition to turning on the SSH function of the device, you must configure the correct key on the device and load the key.

manipulate	command	clarification
Go to System View	system-view	
Enabling SSH	ssh-server	
Disable SSH function	undo ssh-server	

[Example]

! Turn on the SSH function:

```
[GPON]ssh-server
```

16.2.3 Configuring SSH Keys

Configure the key used for SSH in privileged user view. Users cannot log on to the device through the SSH client without a configured key, with an incorrectly configured key, or with a key that is not loaded. In order for users to be able to log on to the device through the SSH client, in addition to configuring the correct key on the device and loading that key, you must also turn on the SSH function of the device.

Configured key algorithms include RSA, DSA, and ECCDSA keys. Initially the device is not configured with any keys. The device's default key must be generated from the command line before it can be used by the device. Configured keys can be used by the device only after they have been loaded. The configured keys are stored in Flash memory and are loaded at system startup. Keys saved in Flash memory can also be loaded via the command line while the system is running.

Configure the default key command as follows:

manipulate	command	clarification
Go to System View	system-view	

Configuring SSH Keys	ssh-server key create { rsa | dss | ecdsa }	

[Example]

! Configure the SSH key with the algorithm RSA:

```
[GPON]ssh-server key create rsa
```

16.2.4 Clearing the key configuration

The key file saved in the device Flash can be cleared with the command.

Load the key configuration via FTP, TFTP as follows:

manipulate	command	clarification
Go to System View	system-view	
Delete SSH secret key	ssh-server key delete { rsa | dss | ecdsa }	

[Example]

! Clear the configured SSH RSA key:

```
[GPON]ssh-server key delete rsa
```

16.2.5 Configure a limit on the number of SSH user logins

You can limit the number of SSH users logging in to the device by using the command, the configuration command is as follows:

manipulate	command	clarification
Go to System View	system-view	
Configure a limit on the number of SSH user logins	ssh-server limit *limit-num*	The limit-num configuration range is 0-5, the default value is 5

[Example]

! Configure the SSH user login limit to 3:

```
[GPON]ssh-server limit 3
```

16.2.6 SSH Monitoring and Maintenance

The SSH monitoring and maintenance configuration is as follows:

manipulate	command	clarification
Viewing the SSH Configuration	display ssh-server	This command displays the version number of SSH, the status of SSH functions turned on/off, and whether the SSH key file is available or not.The status of the SSH key file is displayed as "available" only when the key file is configured and loaded.)
View SSH user login restriction configuration	display ssh-server limit	
View the status of logged-in SSH clients	display login-users	This command displays the status of all logged-in Telnet clients and SSH clients
Force termination of logged-in SSH clients	stop username	

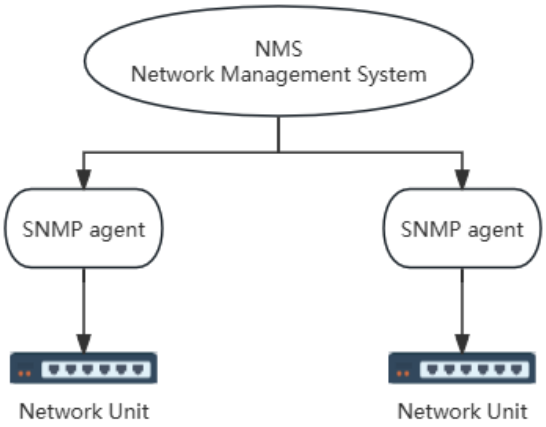
The device allows up to 5 SSH clients to log in at the same time. However, if a Telnet client is already logged on to the device, the total number of SSH clients and Telnet clients must not exceed 5. For example, if 2 Telnet clients are already logged on to the device, up to 3 SSH clients can also be allowed to log on.

Chapter 17 SNMP Configuration

17.1 Introduction to SNMP

SNMP (SimpleNetwork Management Protocol) is a network management standard based on the TCP/IP family of protocols, and is a standard protocol for managing network nodes (e.g., servers, workstations, routers, switches, etc.) in an IP network.The SNMP protocol gives the possibility of centralized management of a large network, and its The goal is to ensure that management information is transmitted between any two points, making it easy for network administrators to retrieve information, make modifications, find faults, and accomplish troubleshooting, capacity planning, and report generation at any node on the network.

The SNMP-managed network consists of three main parts: the managed devices, the SNMP Agent, and the Network Management System (NMS).The NMS (Network ManagementStation), is the workstation that runs the client program, and the SNMP Agent is the server-side software that runs on the managed devices on the network. The relationship between the three of them is shown in the following figure:



A Management Information Base (MIB) exists for each managed device in the network to collect and store management information. The NMS has access to this information through the SNMP protocol. Managed devices, also known as network units or network nodes, can be routers, switches, servers, or hosts that support the SNMP protocol, and so on.

The SNMP Agent Agent is a network management software module on the managed device that holds relevant management information about the local device and is used to convert it into an SNMP-compatible format for delivery to the NMS.

The NMS runs applications to perform the function of monitoring and controlling the managed devices. In addition, the NMS provides a large number of handlers and necessary storage resources for network management.

The NMS can send GetRequest, GetNextRequest and SetRequest messages to the Agent. When the Agent receives the request message from the NMS, it will perform Read or Write operations on the management variables according to the message type and generate Response messages to return to the NMS. On the other hand, the Agent will also actively send Trap messages to NMS to report the events that occur when the device has an abnormal situation such as cold/hot start.

This series of devices supports three versions of SNMP v1, v2c, and v3. v1 provides a simple authentication mechanism, does not support manager-to-manager communication, and v1 Trap does not have an acknowledgement mechanism. v2c enhances the management model (security enhancement) of v1, the management information structure, the protocol operation, and the manager-to-manager communication capability, increases the creation and deletion of tables, and reduces the agent-side storage operation. v3 implements a user authentication mechanism and a message encryption

mechanism, and greatly improves the security of SNMP protocol. communication capabilities, reducing storage operations on the agent side. v3 implements a user authentication mechanism and a message encryption mechanism, which greatly improves the security of the SNMP protocol.

17.2 SNMP Configuration

17.2.1 SNMP Configuration Task List

The main configuration tasks for SNMP are listed below.

Configuration tasks	clarification	Detailed Configuration
Configuring SNMP Access Group Names	compulsory	17.2.2
Configure the administrator contact sysContact	selectable	17.2.3
Configure device location	selectable	17.2.4
Configure the device name	selectable	17.2.5
Configure the notification target host address	selectable	17.2.6
Enabling Notification and Configuring Notification Sending Methods	selectable	17.2.7
Configuring the Trap Source Address	selectable	17.2.8
Configuring the Engine ID	selectable	17.2.9
Configure the maximum SNMP message length	selectable	17.2.10
configuration view	selectable	17.2.11
Configuring Access Control Groups	selectable	17.2.12
Configure Users	selectable	17.2.13
Display SNMP configuration information	selectable	17.2.14

17.2.2 Configuring SNMP Access Group Names

SNMP uses a group name authentication scheme, and SNMP messages that do not match the system-recognized group name will be discarded.SNMP groups (Community) are named by a string, called the group name (CommunityName). Different groups can have read-only or read-write access. Groups with read-only access can only query system information, while groups with read-write access can also configure the system. The system can be configured with up to 8 group names, and there is no group name setting by default.

The Configure SNMP Access Group Name command is shown below:

manipulate	command	clarification
Go to System View	system-view	
Configuring Access Group Names	snmp-agent community *community-name* { ro | rw } { deny | permit } [view *view-name*]	The access group name string is 1 to 20 printable characters. ro, rw indicate read-only, read-write access respectively. permit, deny means whether the community is available or not. View-name is the view configured for this group name, and by default will configure the view iso
Delete access group	undo snmp-agent community *community-*	

name	*name*	

[Example]

! Add a user with group name test, read/write permissions and active

[GPON]snmp-agent community test rw permit

! Delete the user with the group name test

[GPON]undo snmp-agent community test

17.2.3 Configure the administrator contact sysContact

sysContact is an administrative variable in the system group of MIB II that contains the system administrator contact method.

The Configure Administrator command is shown below:

manipulate	command	clarification
Go to System View	system-view	
Configuration Manager Contacts	snmp-agent contact *syscontact*	Administrator contact information string, the length of 1 to 255 characters, the value of the range of printable characters
Delete administrator contact information	undo snmp-agent contact	

[Example]

[GPON]snmp-agent contact support@sina.com.cn

17.2.4 Configure device location

SysLocation is a management variable in the system group of the MIB that indicates the location of the managed device.

The Configure System Location command is shown below:

manipulate	command	clarification
Go to System View	system-view	
Configure device location	snmp-agent location *syslocation*	syslocation is the system location information string, the length is 1 to 255 characters, the value range is printable characters, if there is a space between the input string, it is required to be enclosed in quotation marks.
Delete Device Location	undo snmp-agent location	

[Example]

Configure the device location as "sample sysLocation factory"! Configure the device location as "sample sysLocation factory".

[GPON]snmp-agent location "sample sysLocation factory"

Description:

If there are spaces between the input strings, it is required to enclose them in quotation marks.

17.2.5 Configure the device name

sysName is a management variable in the system group in MIB II, and its content is the device name.

The Configure System Name command is shown below:

manipulate	command	clarification
Go to System View	system-view	
Configure the device name	snmp-agent name *sysname*	sysname is the device name string, the length is 1 to 255 characters, the value range is printable characters, if there are spaces between the input string, it is required to be enclosed in quotation marks.
Delete device name	undo snmp-agent name	

[Example]

! Configure the device name as SwitchABCD

[GPON]snmp-agent name "SwitchABCD"

17.2.6 Configure the notification target host address

This configuration task is used to set or remove the IP address and port number of the target host that sends the announcement message.

The Configure Announcement Destination Host Address command is shown below:

manipulate	command	clarification
Go to System View	system-view	
Configure the notification target host address	snmp-agent host *host-addr* [version { 1 | 2c | 3 [auth | noauth | priv] }] *community-string* [udp-port *port*] [notify-type [*notifytype-list*]]	
Delete the notification target host address	undo snmp-agent host *ip-address community-string* { 1 | 2c | 3 }	

The parameter ip-address indicates the IP address in the snmp-agent trap table. community-string indicates the security name corresponding to the IP in the snmp-agent notification table entry. For snmpv1 and snmpv2c, the security name is the group name, and for snmpv3, the security name is the user name. 1, 2c, and 3 indicate the SNMP version. The version number defaults to 1 if no version number is specified. port indicates the port number to which the notification will be sent. notifytype-list indicates the optional notification types. No selection is made all notification types are selected by default. Only the selected notification types will be sent to the target host.

[Example]

! Configure the snmp-agent notification table entry with ip address 192.168.0.100, version 2c, and group name user

```
[GPON]snmp-agent host 192.168.0.100 version 2c user
```

! Delete the entry announcing that the target host address is 192.168.0.100 and the group name is user.

```
[GPON]undo snmp-agent host 192.168.0.100 user
```

17.2.7 Enabling Notification and Configuring Notification Sending Methods

After you configure the notification target host, the notification function is disabled by default. You need to enable the notification sending and select the notification sending method as TRAP or INFORM before the notification will be sent to the target host address. You can turn on and off the sending switches for various types of announcements by configuring the Announcement Type Sending switch.

The commands to enable notification and configure the notification sending method are shown below:

manipulate	command	clarification
Go to System View	system-view	
Enabling Notification and Configuring Notification Sending Methods	snmp-agent enable { informs | traps } [*notificationtype-list*]	
Turning off announcements and configuring how announcements are sent	undo snmp-agent enable traps/informs [*notificationtype-list*]	

notificationtype-list A system-defined list of available notification types. Selecting one or more of these toggles the selected notification type on or off. If no selection is made, all notification types are toggled on or off.

Types of notices include the following:

bridge: turn spanning tree enable on/off

interfaces: port LinkUp/LinkDown

snmp: access control, system cold start/hot start

gbnsavecfg: configuration save

rmon: RMON trap

gbn: Custom Traps such as Port Blocking, CAR, Loop Detection

[Example]

! Turn on the send switch for the announcement type bridge

```
[GPON]snmp-agent enable traps bridge
```

17.2.8 Configuring the Trap Source Address

This configuration task is used to configure the source IP address of Trap messages. When the configured Trap source IP address is the device Layer 3 interface IP, the Trap message is encapsulated with this configured source IP address, and if the configured Trap source IP address is not the interface IP, the device sends the Trap message encapsulated with the outgoing interface IP address.

The Configure Trap Source Address command is shown below:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Trap Source Address	snmp-agent trap-source *ipaddress*	
Remove Trap source address	undo snmp-agent trap-source	

[Example]

! Configure the trap source address to 192.168.1.100

[GPON] snmp-agent trap-source 192.168.1.100

17.2.9 Configuring the Engine ID

This configuration task is used to configure the engine ID of the local snmp entity and the engine ID of the remote snmp entity that can be recognized locally. the local engine id is 134640000000000000000000000 by default, and can be modified but cannot be deleted. There is no identifiable remote engine ID by default. remote engine IDs can be added and deleted. Once an identifiable remote engine is deleted, all its corresponding users will also be deleted. The maximum number of remote engines that can be configured is 32.

The Configure Engine ID command is shown below:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Engine ID	snmp-agent engineoid { local engineid-string | remote ip-address [udp-port port-number] engineid-string }	
Delete Engine ID	undo snmp-agent engineid { local | remote *ip-address* [*udp-port port-number*] }	

engineid-string is an identifier that uniquely identifies an engine within a network. This system only supports entering printable characters to identify an engine ID, and the engine ID cannot contain spaces;

Ip-address is the ip address of the remote engine, the system does not allow local ip to be entered;

Port-number is the port number of the remote engine, if not configured the default port number will be 162.

[Example]

! Configure the local engine id to 123456

[GPON] snmp-agent engineid local 123456

! Configure a remote engine that can be recognized locally. The ip of the remote engine is 10.1.2.3, the port number is 1111, the id is 5678

[GPON] snmp-agent engineid remote 10.1.2.3 udp-port 11115678

17.2.10 Configure the maximum SNMP message length

The system supports configuring the maximum SNMP message length, and SNMP messages exceeding the maximum length will no longer be processed.

Please configure the following under system view.

manipulate	command	clarification
Go to System View	system-view	
Configure the maximum SNMP message length	snmp-agent max-packet-length *length*	Length is configurable from 484-8000 Byte, default is 1000 Byte.
Restore the default SNMP maximum message length	undo snmp-agent max-packet-length	

[Example]

! Configure the maximum SNMP message length to 1230Byte

[GPON] snmp-agent max-packet-length 1230

17.2.11 configuration view

This configuration task is used to configure the views and the subtrees they contain that are available for view access control. By default, there are three views iso, internet, and sysview, and the maximum number of views that can be configured is 64. The view internet is prohibited from being deleted and modified.

The configuration view commands are shown below:

manipulate	command	clarification
Go to System View	system-view	
configuration view	snmp-agent view *view-name oid-tree* { included | excluded }	
Deleting Views	undo snmp-agent view *view-name* [oid-tree]	

view-name is the view name of the view to be added. The length is 1-32, and the view name cannot contain spaces;

Oid-tree is the subtree contained in the view, it corresponds to a mib node, such as "1.3.6.1"; OID contains a substring must be an integer from 0 to 2147483647;

The sum of the number of characters contained in the view name string plus the number of nodes contained in the OID plus 2 must not exceed 64.

Configuring a view subtree type of exclude only means that nodes under that subtree are not accessible, it does not mean that nodes outside that subtree are accessible. When you configure the target host of a notification, if the security name is Community, sending a notification is not affected by the view; if the security name is SNMPv3 user, sending a notification is controlled by the notification view of the user. The notification view controls whether the node to which the variable carried by the notification belongs is accessible, and does not affect the access attributes of the trap OID node to which the notification belongs. If the notification does not contain bound variables, the notification can always be sent independent of the view.

[Example]

Add the view view1, configure the subtree "1.3.6.1" for it! Add view view1, configure subtree "1.3.6.1" for it.

[GPON] snmp-agent view view1 1.3.6.1 include

! Add the subtree "1.3.6.2" to the existing view view1.

[GPON] snmp-agent view view1 1.3.6.2 include

! Delete existing view view1

[GPON] undo snmp-agent view view1

17.2.12 Configuring Access Control Groups

This configuration task can be used to configure an access control group. The groups that exist by default are as follows:(1) groupinitial with security model v3 and security level discriminating (2) groupinitial with security model v3 and security level discriminating encrypted. up to 64 groups can be configured. Configure the access control group commands as shown below:

manipulate	command	clarification
Go to System View	system-view	
Configuring Access Control Groups	snmp-agent group *groupname* { 1 | 2c | 3 [auth | noauth | priv] [context *context-name*]} [read *readview*] [wrete *writeview*] [notify *notifyview*]	
Deleting Access Control Groups	undo snmp-agent group *groupname* {1 | 2c | 3 [auth | noauth | priv] [context *context-name*]}	

groupname is the group name, the length is 1-32, the group name cannot contain spaces;
readview is a view name, configured to indicate read access within the scope of this view, not entered will default to the group not containing readable views;
writeview is a view name, configured to indicate read and write permissions within the scope of this view, not entered will default to the group does not contain read-write views;
notifyview is a view name that, when configured, indicates that there is permission to send notices within the scope of this view; failure to enter it will result in the default that the group does not contain a view to which notices can be sent;
context-name is the device context, not entering context-name will default to the local device.
[Example]
! Add group group1 to the local device, using security model 1, containing all three views as internet

```
[GPON] snmp-agent group group1 1 read internet write internet notify internet
```

! Delete the group configured for the local device group1

```
[GPON] undo snmp-agent group group1 1
```

17.2.13 Configure Users

This configuration task is used to configure users for the local engine or an identifiable remote engine. the following users exist by default:
(1) initialmd5 (requires md5 identification), (2) initialsha (requires sha identification), and (3) initialnone (does not require identification). The above three users are reserved for system use and cannot be used by users. When configuring a user, you need to ensure that the engine to which the user belongs is recognizable. When an identifiable engine is deleted, the user it contains will also be deleted. Up to 64 users can be configured. The commands for configuring users are shown below:

manipulate	command	clarification
Go to System View	system-view	
Configure Users	snmp-agent user *username groupname* [remote *host* [udp-port *port*]] [auth { md5 | sha } { authpassword { encrypt-authpassword *authpassword* | *authpassword* } | authkey { encrypt-authkey *authkey* | *authkey* } } [priv des { privpassword { encrypt-privpassword *privpassword* | *privpassword* } | privkey { encrypt- privkey *privkey* | *privkey* } }]	

Delete User	undo snmp-agent user *username* [remote *host* [udp-port *port*]]	

username is the username to be configured, the length is 1-32 and cannot contain spaces in between;
groupname is the name of the group that the user wants to join, the length is 1-32 and cannot contain spaces in between;
host is the ip address of the remote engine, not entering it will default to the local engine;
port is the port number of the remote engine, not entering it will default the port number to 162;
authpassword is the authentication password, the length of the unencrypted password is 1-32, in order to prevent the password from leaking on the Internet, you can use encryption algorithms to encrypt the password configuration. To configure the encrypted password, you need to encrypt the unencrypted password with a client that supports this system's encryption algorithm, and then use the encrypted cipher text to configure the password. The length of the encrypted ciphertext varies depending on the encryption algorithm. To configure the ciphertext from the command line, enter the ciphertext in hexadecimal format. For example, enter a 16-byte ciphertext "a20102b32123c45508f91232a4d47a5c";
Privpassword is an encrypted passphrase. The length of the unencrypted passphrase is 1-32. To prevent the passphrase from being leaked on the Internet, you can configure the passphrase to be encrypted using an encryption algorithm. To configure the encrypted password, you need to encrypt the unencrypted password with a client that supports the encryption algorithm of this system, and configure the encrypted password with the encrypted cipher text. The length of the encrypted ciphertext varies depending on the encryption algorithm. To configure the ciphertext from the command line, enter the ciphertext in hexadecimal format. For example, enter a 16-byte ciphertext "a20102b32123c45508f91232a4d47a5c";
The authkey is the authentication key. The length of the unencrypted authentication key is 16 bytes (hashed using the md5 algorithm) or 20 bytes (hashed using the SHA-1 algorithm), and the length of the encrypted authentication key is 16 bytes (hashed using the md5 algorithm) or 24 bytes (hashed using the SHA-1 algorithm);
privkey is the encryption key, the unencrypted encryption key is 16 bytes long and the encrypted authentication key is 16 bytes long; keywords encrypt-authpassword, encrypt-authkey, encrypt-privpassword, encrypt-privkey
Used only in decompiled generated command lines to prevent leakage of user-configured plaintext passphrases and keys. Users cannot use the above keywords when configuring SNMP users via the command line.
[Example]
! Add user user1 to the local engine, join group group1, this user does not use authentication and encryption

```
[GPON] snmp-agent user user1 group1
```

! Add user user2 to the local engine, add group group2, this user is identified using md5, no encryption is used, and the input passphrase is 1234.

```
[GPON] snmp-agent user user2 group2 auth md5 auth-password 1234
```

Add user user3 to the local engine, add group3! Add user user3 to the local engine, join group3, this user uses md5 authentication and des encryption, the authentication password is 1234 and the encryption password is 4321.

```
[GPON] snmp-agent user user3 group3 auth md5 auth-password 1234 priv des priv-password 4321
```

17.2.14 Display SNMP configuration information

SNMP configuration information can be displayed at any attempt:

manipulate	command	clarification
Show SNMP Access Group Nominations	display snmp community	
Show administrator contact information	display snmp contact	
Display Engine ID	display snmp engineid { local | remote }	
Show Access Control Groups	display snmp group	

Displays the address of the notification host	display snmp host	
Show device location	display snmp location	
Display the maximum SNMP message length	display snmmpax-packet-length	
Display device name	display snmp name	
Display Notice Type	display snmpnotify	
Display SNMP User Configuration	display snmpuser	
Displaying SNMP View Configuration	display snmp view	

Chapter 18 Info-center Configuration

18.1 Introduction to Info-center

Info-center is the information center of the system, completing the unified processing and output of information. Other modules in the system send the information to be output to Info-center, which determines the output format of the information according to the user's configuration, and outputs the information to the specified display device according to the information switch and filtering rules of each output direction configured by the user.

Each function module that outputs information does not need to care whether the information needs to be output to the console, Telnet terminal, or log host (Info-center server), etc. It only needs to output the information to the Info-center. Consoles, Telnet terminals, history buffers, logging hosts, and SNMP Agents can choose to accept the information they need and discard the information they don't need as they wish, as long as they are configured with the appropriate filtering rules.

The Info-center information levels are referenced below:

severity rating	protocol description	Relevant cross-references
0: emergencies	Extremely urgent error	Error requiring reboot;
1: alerts	Mistakes to be corrected immediately	Self-loop; hardware error;
2: Critical	critical error	Memory, resource allocation failure;
3: errors	Mistakes that need attention but are not critical	General error; illegal parameters that are difficult to recover;
4: Warnings	Warning that there may be some kind of error	Alarms; non-significant packet loss, message loss; The external server is out of contact;
5: notifications	Information to be noted	Trap backup output;
6: informational	General tips	Command line operation log; The set operation on a MIB node;
7: Debugging	Debugging Information	Debugging output; process data for business protocols;

18.2 Info-center Configuration

18.2.1 Info-center configuration task list

The list of major configuration tasks for Info-center is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable the device Info-center function	compulsory	18.2.2
Configuring Info-center Serial Number Display	selectable	18.2.3
Configuring the Info-center timestamp type	selectable	18.2.4
Configuring Info-center terminal output	selectable	18.2.5
Configuring Info-center History Buffer Outputs	selectable	18.2.6
Configuring Info-center Flash Memory Outputs	selectable	18.2.7
Configuring Info-center Log Host Output	selectable	18.2.8
Configuring Info-center SNMP Agent Outputs	selectable	18.2.9

Configuration Module Debug Switch	selectable	18.2.10
Display Info-center related configuration information	selectable	18.2.11

18.2.2 Enable/disable the device Info-center function

Turn the Info-center function on or off in system view. No information is output when the Info-center function is off.

The configuration commands are shown below:

manipulate	command	clarification
Go to System View	system-view	
Enable Info-center function	info-center	
Disable the Info-center function	undo info-center	

[Example]

! Turn on the Info-center function:

[GPON] info-center

18.2.3 Configuring Info-center Serial Number Display

Configure the display or non-display of the global sequence number in the Info-center output message under system view with the following configuration commands:

manipulate	command	clarification
Go to System View	system-view	
Enable display of Info-center serial number	info-center sequence-numbers	
Disable display of Info-center serial numbers	undo info-center sequence-numbers	

[Example]

! Configure to display the global sequence number in the Info-center output message:

[GPON]info-center sequence-numbers

18.2.4 Configuring the Info-center timestamp type

Configure the type of timestamp displayed in the Info-center output message under system view. There are three types of timestamps: no time display, show boot time, and show datetime, and the configuration commands are shown below:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Info-center timestamp type	info-center timestamps { notime | uptime | datetime }	
Restore default Info-center timestamp type	undo info-center timestamps	The default timestamp type is uptime

[Example]

! Configure to display the datetime as a timestamp in Info-center output messages:

[GPON]info-center timestamps datetime

18.2.5 Configuring Info-center terminal output

Configure the message output switches, message display switches, and filtering rules for Info-center terminal output in system view.

manipulate	command	clarification
Enter privileged user view	enable	
Turn on the message output switch	terminal monitor	
Turn off the message output switch	undo terminal monitor	
Go to System View	system-view	
Enable Info-center information terminal output	info-center monitor { all | *monitor-nu* }	A monitor-nu of 0 indicates a console, and 1 to 5 indicates a Telnet terminal.
Close the Info-center information terminal output.	undo info-center monitor { all | *monitor-nu* }	
Configure terminal information output filtering rules	info-center monitor { all | *monitor-nu* } { *level* | none | level-list { *level* [to *level*] } &<1-8> } [module { xxx | ... } *]	xxx indicates the name of the module, ... omits the names of other modules
Canceling terminal information output filtering rules	undo info-center monitor { all | *monitor-nu* } filter	

[Example]

! Turns on the current terminal information display switch:

```
[GPON]terminal monitor
```

! Turns on the console message output switch:

```
[GPON]info-center monitor 0
```

! Set the console filter rule to allow all modules to output information with a level of 0 to 7:

```
[GPON]info-center monitor 0 7
```

18.2.6 Configuring Info-center History Buffer Outputs

Configure information output switches and filtering rules for Info-center history buffer output in system view.

The configuration commands are shown below:

manipulate	command	clarification
Go to System View	system-view	
Enable history buffer information output	info-center buffered	
Turn off history buffer information output	undo info-center buffered	
Configuring History Buffer Information Output Filtering Rules	info-center buffered { *level* | none | level-list { *level* [to *level*] } &<1-8> } [module { xxx | ... } *]	xxx indicates the name of the module, ... omits the names of other modules

Remove the history buffer message output filter rule	undo info-center buffered filter	

[Example]

! Turns on the history buffer output switch:

[GPON]info-center buffered

! Set the history buffer filtering rule to allow all modules to output information with a level of 0 to 6:

[GPON]info-center buffered 6

18.2.7 Configuring Info-center Flash Memory Outputs

Configure message output switches and filter rules for Info-center Flash memory output in system view.

The configuration commands are shown below:

manipulate	command	clarification
Go to System View	system-view	
Enable Flash memory information output	info-center flash	
Turn off Flash memory information output	undo info-center flash	
Configuring Flash Memory Message Output Filtering Rules	info-center flash { *level* | none | level-list { *level* [to *level*] } &<1-8> } [module { xxx | ... } *]	xxx indicates the name of the module, ... omits the names of other modules
Remove the Flash memory message output filter rule	undo info-center flash filter	

[Example]

! Turn on the Flash memory output switch:

[GPON]info-center flash

! Set the Flash memory filtering rule to allow all modules to output information at levels 0, 1, 2, and 6:

[GPON]info-center flash level-list 0 to 2 6

18.2.8 Configuring Info-center Log Host Output

Configure the server address, message output switch, filtering rules, and logging tool and fixed source address for Info-center log host output under system view. The configuration commands are shown below:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Log Host Server Address	info-center *ip-address*	
Delete log host server address	undo info-center *ip-address*	
Enable log host information output	info-center host { all | *ip-address* }	

Turn off log host information output	undo info-center host { all | *ip-address* }	
Configure log host information output filtering rules	info-center host { all | *ip-address* } { *level* | none | level-list { *level* [to *level*] } &<1-8> } [module { xxx | ... } *]	xxx indicates the name of the module, ... omits the names of other modules
Remove the log host information output filter rule	undo info-center host { all | *ip-address* } filter	
Configuration Log Host Configuration Tool	info-center facility { xxx | ... }	xxx denotes the name of the logging tool, including ftp, mail, ntp, kernel, etc., ... omits the names of other tools
Unlog Host Configuration Tool	undo info-center facility	
Configure the source address used by the logging host	info-center source *ip-address*	The ip-address must be the address of one of the interfaces of the configured device.
Cancel the source address used by the log host	undo info-center source	

[Example]

! Configure the server address to 192.168.1.100

[GPON]info-center 192.168.1.100

! Turn on the log host 192.168.1.100 output switch

[GPON]info-center host 192.168.1.100

! Set the log host 192.168.1.100 filter rule to only allow vlan modules to output level 7 information:

[GPON]info-center host 192.168.1.100 none

[GPON]info-center host 192.168.1.100 level-list 7 module vlan

! Configure the log host logging tool to localuse7

[GPON]info-center facility localuse7

! Configure log host output to use fixed source address 192.168.1.200

[GPON]info-center source 192.168.1.200

18.2.9 Configuring Info-center SNMP Agent Outputs

Configure message output switches and filtering rules for Info-center SNMP Agent output in system view. To enable Info-center information to be sent as Trap messages to SNMP Workstation, the Trap host address must also be configured, see the description in the SNMP Configuration section. The configuration commands are as follows:

manipulate	command	clarification
Go to System View	system-view	
Enable SNMP Agent information output	info-center snmp-agent	
Turn off SNMP Agent	undo info-center snmp-agent	

message output		
Configure SNMP Agent message output filtering rules	info-center snmp-agent { *level* | none | *level-list* { *level* [to *level*] } &<1-8> } [module { xxx | ... } *]	xxx indicates the name of the module, ... omits the names of other modules
Cancel SNMP Agent message output filtering rules	undo info-center snmp-agent filter	

[Example]

! Turn on the SNMP Agent output switch:

[GPON]info-center snmp-agent

! Set the SNMP Agent filter rule to allow all modules to output information with a level of 0 to 5:

[GPON]info-center snmp-agent 5

18.2.10 Configuration Module Debug Switch

Enable/disable the module debugging switch under system view. After enabling the debugging switch, you can print out info-center related debugging information. The configuration commands are shown below:

manipulate	command	clarification
Go to System View	system-view	
Enable module debug switch	debug { all | { xxx | ... } * }	xxx indicates the name of the module, ... omits the names of other modules
Turn off the module debug switch	undo debug { all | { xxx | ...} * }	

[Example]

! Turn on the debug switch for the vlan module:

[GPON]debug vlan

18.2.11 Display Info-center related configuration information

You can view info-center related configuration information in any view:

manipulate	command	clarification
View info-center configuration information	display info-center	
Viewing info-center buffer log messages	display info-center buffered	
Viewing info-center flash zone log messages	display info-center flash	
View info-center filtering level configuration information	display info-centerfilter { buffered | flash | host *ip-address* | monitor *monitor-nu* | snmp-agent }	

[Example]

! Displays info-center configuration information:

[GPON]display info-center

Chapter 19 Three-tier functional configuration

19.1 Three-Layer Functional Profile

This OLT device supports hardware-based Layer 2 and Layer 3 forwarding. Hosts in the same VLAN use Layer 2 forwarding when they access each other, and hosts in different VLANs support Layer 3 forwarding when they access each other.

19.2 Three-tier functional configuration

19.2.1 Layer 3 Functional Configuration List

The list of Layer 3 functional configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Creating VLANs and VLAN Layer 3 interfaces	compulsory	19.2.2
Create/delete common VLAN Layer 3 interfaces	compulsory	19.2.3
Create/Delete Supervlan Interface	compulsory	19.2.4
Add/Remove Supervlan Sub-VLANs	compulsory	19.2.5
Creating/Deleting Loopback Interfaces	selectable	19.2.6
Configure/delete Layer 3 interface IP addresses	compulsory	19.2.7
Configure/delete Layer 3 interface access IP address ranges	selectable	19.2.8
Configuring the Layer 3 Interface ARP Proxy	selectable	19.2.9
Displaying Layer 3 Interface Configuration	selectable	19.2.10
Configuring Layer 3 Message Forwarding Mode	selectable	19.2.11
Configure the destination host unknown message forwarding mode	selectable	19.2.12

19.2.2 Create VLAN and VLAN Layer 3 interfaces

Refer to the VLAN Configuration section in Chapter 8 for specific configuration of creating VLANs.

Layer 3 interfaces are divided into normal VLAN interfaces and SuperVLAN interfaces. normal VLAN interfaces are interfaces created in a specific VLAN, while SuperVLAN interfaces are created on top of SuperVLANs. superVLANs are nonexistent VLANs, which do not contain any ports, and SuperVLANs can contain multiple sub-VLANs (sub-VLANs are specific existing VLANs). VLANs are specific existent VLANs).

The system can create up to 128 Layer 3 interfaces, including normal VLAN interfaces and SuperVLAN interfaces. The maximum number of VLANs contained in all Layer 3 interfaces is 128, and each VLAN exists in only one Layer 3 interface. in SuperVLAN, a port can be an untagged member in only one sub-VLAN, and it must be a tagged member in all other sub-VLANs.

19.2.3 Create/delete common VLAN Layer 3 interfaces

VLAN interfaces need to be configured for each VLAN that performs Layer 3 forwarding. creating and deleting common VLAN Layer 3 interfaces are configured as follows:

manipulate	command	clarification
Go to System View	system-view	

Create a normal VLAN Layer 3 interface	interface vlan-interface *vlan-id*	The vlan-id needs to be a created vlan in the range of 1-4094, otherwise the configuration will fail.
Delete a normal VLAN Layer 3 interface	undo interface vlan-interface *vlan-id*	

[Example]

! Configured as a Layer 3 interface for VLAN 100:

```
[GPON]interface vlan-interface 100
```

19.2.4 Create/delete SuperVLAN Layer 3 interfaces

SuperVLAN interface realizes the communication between hosts located in different VLANs but belonging to the same network segment. sub-VLANs can be added under the SuperVLAN interface and the communication between sub-VLANs is realized through ARP proxy.

Creating and deleting common VLAN Layer 3 interfaces are configured as follows:

manipulate	command	clarification
Go to System View	system-view	
Create Supervlan Layer 3 interface	interface supervlan-interface *vlan-id*	The vlan-id can be left uncreated and configured in the range of 1-128
Delete Supervlan Layer 3 interface	undo interface supervlan-interface *vlan-id*	

[Example]

! Create Supervlan 128

```
[GPON]interface supervlan-interface 128
[GPON-superVLANInterface-128]
```

19.2.5 Adding/Removing SuperVLAN Sub-VLANs

SuperVLAN To realize the communication between hosts with different VLANs but belonging to the same network segment, you need to add sub-VLANs under the SuperVLAN interface, and the communication between sub-VLANs is realized through ARP proxy.

Adding and removing Supervlan sub-VLANs is configured as follows:

manipulate	command	clarification
Go to System View	system-view	
Create Supervlan Layer 3 interface	interface supervlan-interface *vlan-id*	The vlan-id of the Supervlan can be left uncreated and configured in the range of 1-128
Adding a Supervlan Sub-VLAN	subvlan vlan-list	The vlan-list for a subvlan must be created first and contain member ports that are untagged in one subvlan only and cannot be untagged in any other subvlan. vlan-list can be a single vlan or multiple vlan
Delete the Supervlan sub-VLAN	undo subvlan [*vlan-list*]	When vlan-list is not entered, delete all subvlan

[Example]

! Creating Sub-VLANs 3 and 4 of Supervlan 128

[GPON]interface supervlan-interface 128

[GPON-superVLANInterface-128] subvlan 3

[GPON-superVLANInterface-128] subvlan4

! Deleting Sub-VLAN 3 of Supervlan 128

[GPON-superVLANInterface-128]undo subvlan 3

19.2.6 Configure/delete loopback interfaces

The loopback interface is mainly used to test whether the Layer 3 interface is working properly:

manipulate	command	clarification
Go to System View	system-view	
Creating a Loopback Interface	interface loopback-interface *loopback-id*	The loopback interface ID supports configuration of two interfaces, 0 and 1
Delete Loopback Interface	undo interface loopback-interface *loopback-id*	

[Example]

! Create loopback interface 0

[GPON] interface loopback-interface 0

19.2.7 Configure/delete Layer 3 interface IP addresses

Each normal VLAN Layer 3 interface, SuperVLAN Layer 3 interface, and loopback interface can be configured with up to eight IP addresses, and the IP addresses of these interfaces cannot be in the same network segment. The first configured IP address of an interface is automatically elected as the primary IP address, and when the primary IP address is deleted, the interface automatically elects another IP address of this interface as the primary IP address, or you can manually specify an already configured IP address as the primary IP address. For example, if the IP address of VLAN interface 1 is 192.168.0.1/16, other interfaces cannot be configured with an IP address belonging to the 192.168.0.0/16 segment (such as 192.168.1.254/24).

Configure the Layer 3 interface IP address configuration as follows:

manipulate	command	clarification
Go to System View	system-view	
Access to common VLAN Layer 3 interfaces	interface vlan-interface *vlan-id*	
Configure the Layer 3 interface IP address	ip address [primary] *ip-address mask*	IP addresses are class A~C addresses, multicast IP addresses, broadcast IP addresses, and full host IP addresses are illegal addresses not allowed to be configured. When primary is not specified, the first configured IP address is the primary IP address
Configure to obtain an IP address via DHCP	dhcp-client [ipv4 | ipv6]	

Delete the Layer 3 interface IP address	undo ip address [*ip-address mask*]	When the IP address parameter is not entered, it indicates that all IP addresses under this Layer 3 interface are deleted
Access to Supervlan Layer 3 interface	interface supervlan-interface *vlan-id*	
Configure the Layer 3 interface IP address	ip address [primary] *ip-address mask*	
Delete the Layer 3 interface IP address	undo ip address [*ip-address mask*]	
Access to the loopback interface	interface loopback-interface *loopback-id*	
Configure the Layer 3 interface IP address	ip address [primary] *ip-address mask*	
Delete the Layer 3 interface IP address	undo ip address [*ip-address mask*]	

[Example]

! Common VLAN interface 100 is configured with an IP address of 192.168.1.100/24:

[GPON-vlanInterface-2]ip address 192.168.1.100 255.255.255.0

! Delete the IP address of VLAN interface 100:

[GPON-vlanInterface-100]undo ip address

19.2.8 Configuring the Layer 3 Interface ARP Proxy

Because ARP request messages are broadcast messages and cannot traverse VLANs, if the ARP proxy function is activated, it enables hosts in sub-VLANs in the same superVLAN to interact with ARP. When ARP proxy is off, hosts in sub-VLANs in a SuperVLAN interface cannot communicate. Please configure it under SuperVLAN interface view.

manipulate	command	clarification
Go to System View	system-view	
Access to common vlan Layer 3 interfaces	interface vlan-interface *vlan-id*	
Enable arp proxy	local-arp-proxy	The arp proxy is off by default
Disable arp proxy	undo local-arp-proxy	
Access to Supervlan Layer 3 interface	interface supervlan-interface *vlan-id*	
Enable arp proxy	local-arp-proxy	The arp proxy is off by default
Disable arp proxy	undo local-arp-proxy	

[Example]

! Enable ARP Proxy

[GPON]interface supervlan-interface 128

[GPON-superVLANInterface-128] local-arp-proxy

! Disable ARP Proxy

[GPON]interface supervlan-interface 128

[GPON-superVLANInterface-128] undo local-arp-proxy

19.2.9 Displaying Layer 3 Interface Configuration

Each created VLAN interface or superVLAN interface has its own configuration information, including the VLAN number, IP address, and mask, etc. The following commands are used to display the configuration information of all Layer 3 interfaces, specified normal VLAN interfaces, or Super VLAN interfaces, and you can view the configuration information of Layer 3 interfaces in any view:

manipulate	command	clarification
Display all Layer 3 interface configurations	display ip interface	
Displaying Common VLAN Layer 3 Interface Configuration	display ip interface vlan-interface *vlan-id*	
Displaying Common Supervlan Layer 3 Interface Configuration	display ip interface supervlan-interface *supervlan-id*	
Displaying Loopback Interface Configuration	display ip interface loopback-interface [*loopback-id*]	When loopback-id is not specified, display all loopback interface information

[Example]

! Displays configuration information for common VLAN interface 100:

[GPON]display ip interface vlan-interface 100

! Displays configuration information for superVLAN interface 128:

[GPON]display ip interface supervlan-interfac 128

19.2.10 Configuring Layer 3 Message Forwarding Mode

The device supports two message forwarding modes: stream forwarding mode and network topology forwarding mode. In flow forwarding mode failed routes will be sent to the CPU for further processing. the device will generate ICMP messages to the source address of the message where the destination segment is unreachable. while in network topology forwarding mode these messages will be directly discarded. The default is flow forwarding mode.

manipulate	command	clarification
Go to System View	system-view	
Configuring Flow Forwarding Mode	ip dlf cpu	Defaults to stream forwarding mode
Configure the network topology forwarding mode	undo ip dlf cpu	

[Example]

! Configure the Layer 3 message forwarding mode as stream forwarding mode

[GPON] ip dlf cpu

19.2.11 Configure the destination host unknown message forwarding mode

In addition to supporting forwarding control processing for messages that fail to find a route, the device also supports whether to send CPU control for messages that fail to find a route to the destination host.

When send CPU processing is turned on, the message will be sent to the CPU for further processing, and the device will generate a destination host unreachable ICMP message to the source address of the message, and when send CPU processing is turned off, the message will be discarded. The default configuration is to send CPU processing.

manipulate	command	clarification
Go to System View	system-view	
Enter vlan interface view	interface vlan-interface *vlanid*	
Configuring Unknown Host Message Delivery CPU	ip host-dlf cpu	The default is to send it to the cpu for processing.
Turn off unknown host message delivery to CPU	undo ip host-dlf cpu	

[Example]

! Configure the destination host unknown message forwarding mode for VLAN interface 100 to send CPU

```
[GPON-vlanInterface-100]ip host-dlf cpu
```

Chapter 20 ARP Function Configuration

20.1 ARP Function Introduction

An ARP table is a table that holds the IP and MAC correspondences, including both dynamic and static types. Dynamic ARP table entries are learned through the ARP protocol, and static ARP table entries are added manually through commands.

20.2 ARP Function Configuration

20.2.1 ARP Feature Configuration Task List

The list of configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Adding and deleting ARP table entries	compulsory	20.2.2
Bind dynamic ARP table entries to static ARP table entries	selectable	20.2.3
Display ARP table entries	selectable	20.2.4
Configure and restore ARP aging time	selectable	20.2.5
Display ARP aging time	selectable	20.2.6

20.2.2 Adding and deleting ARP table entries

This command enables you to add or delete a static or dynamic ARP table entry in the device. the ARP table entry contains not only the correspondence between IP and MAC but also the local VLAN and physical port number through which frames with the parameter MAC as the destination address are sent. please configure it under system view.

manipulate	command	clarification
Go to System View	system-view	
Adding ARP table entries	arp ip-address mac mac-address vid vlan-id port interface-num	
Delete ARP table entries	undo arp { all | static | dynamic | *ip-address* }	

[Example]

! Add a static ARP table entry with an IP of 192.168.0.100, a MAC address of 00:01:02:03:04:05, a corresponding VLAN interface of 100, and a physical port of 3

[GPON]arp 192.168.0.100 mac00:01:02:03:04:05 vid 100 port 0/0/3

! Delete an ARP table entry with the IP address 192.168.0.100.

[GPON]undo arp 192.168.0.100

! Delete all static ARP table entries

[GPON]undo arp static

! Delete all ARP table entries

[GPON]undo arp all

20.2.3 Bind dynamic ARP table entries to static ARP table entries

This command enables you to bind dynamic arp table entries learned by the device to static arp table entries. In this way, when the network is normal, you can quickly bind dynamic arp to static arp for subsequent control on security.

manipulate	command	clarification
Go to System View	system-view	
Bind dynamic ARP table entries to static ARP table entries	arp bind dynamic { *ip-address* | all }	When IP address is specified, the dynamic ARP table entries corresponding to the specified IP address are bound to static ARP. when ALL is specified, all dynamic ARP table entries are bound to static ARP table entries.

[Example]

! Bind dynamic arp with ip 192.168.1.100 to static arp

[GPON]arp bind dynamic 192.168.1.100

! Bind all valid dynamic arp table entries to static arp

[GPON]arp bind dynamic all

20.2.4 Display ARP table entries

With this command, you can display static, dynamic, specified IP address and all table entries, and you can execute the display command in any view.

manipulate	command	clarification
Display ARP table entries	display arp { all | static | dynamic | *ip-address* | interface { vlan-interface *vlan-id* | supervlan-interface *vlan-id* } }	

[Example]

! Display all ARP table entries

[GPON]display arp all

! Displays the ARP table entry for the IP address 192.168.1.100:

[GPON]display arp 192.168.1.100

! Displays ARP table entries belonging to vlan interface 100:

[GPON]display arp interface vlan-interface 100

20.2.5 Configure and restore ARP aging time

Modify the ARP aging time with this command. configure it in system view.

manipulate	command	clarification
Go to System View	system-view	
Configuring ARP Aging Time	arp aging-time *aging-time*	arp aging time range of 3-2880 minutes
Restore ARP aging time	undo arp aging-time	Default arp aging time is 20 minutes

[Example]

! Configure the ARP aging time to 30 minutes

[GPON] arp aging-time 30

20.2.6 Display ARP aging time

ARP aging time can be viewed in any view:

manipulate	command	clarification
Display arp aging time	display arp aging-time	

[Example]

! Display ARP aging time

[GPON] display arp aging-time

Chapter 21 Anti-ARP attack function

21.1 Introduction to Anti-ARP Attack Function

The anti-ARP attack function consists of two parts of functions: one is the anti-ARP flood attack function and the other is the anti-ARP spoofing function.

ARP anti-flood attack is to prevent the same MAC from sending a large number of ARP messages, which affects the device's processing of normal ARP messages. After this feature is enabled, if the number of ARP messages received by the device per second from a fixed source MAC address exceeds the set threshold, the user using the MAC address is considered to be conducting ARP attacks, and the system issues an anti-attack table entry to filter the MAC address, and the filtering policy is categorized into filtering only the ARP messages of the source MAC or filtering all the messages of the source MAC. After the system issues an anti-attack table entry, the user is banned. By default, the ARP anti-flood attack function is off.

Anti-ARP spoofing means, checking whether ARP messages match the configured static ARP. When this function is enabled, all ARPs passing through the device will be redirected to the CPU for checking. In turn, it determines whether the ARP message matches exactly with the static ARP table entry, whether it matches exactly with the ip-source-guard static binding table entry, and whether it matches exactly with the dhcp-snooping table entry, and if there exists an exact match, then it will no longer carry out the subsequent checking, and it is allowed to be forwarded. Otherwise, if there is not an exact match, the ARP is recognized as an illegal message and is processed according to the set anti-spoofing policy: discarded or flooded (sent to each port). By default, the ARP anti-spoofing attack function is off by default.

21.2 Configuration of Anti-ARP Attack Function

21.2.1 Anti-ARP Attack Feature Configuration Task List

The list of configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable protection against ARP flooding attacks	compulsory	21.2.2
Configure the anti-ARP flood attack resistance action type and rate thresholds	selectable	21.2.3
Configuring Anti-ARP Flood Attack Banned MAC Auto Recovery Time	selectable	21.2.4
Manual recovery of banned MACs against ARP flooding attacks	selectable	21.2.5
Display anti-ARP flooding attack information	selectable	21.2.6
Bind the MAC address generated by the anti-ARP flooding attack to the general black hole MAC	selectable	21.2.7
Enable/disable anti-ARP spoofing attack	selectable	21.2.8
Configuring an Anti-Unknown ARP Message Spoofing Policy	selectable	21.2.9
Enable/disable ARP message source MAC consistency checking	selectable	21.2.10
Enable/disable ARP anti-gateway impersonation	selectable	21.2.11
Display anti-ARP spoofing flood attack information	selectable	21.2.12
Configuring Trusted Ports for Anti-ARP Attacks	selectable	21.2.13

21.2.2 Enable/disable protection against ARP flooding attacks

Enable disable anti-ARP flood attack configuration as follows:

manipulate	command	clarification
Go to System View	system-view	
Enable protection against ARP flooding attacks	arp anti-flood	
Turn off protection against ARP flooding attacks	undo arp anti-flood	

21.2.3 Configure the anti-ARP flood attack resistance action type and rate thresholds

The anti-ARP flood attack has two resisting actions for the source MAC of ARP overrun, one is to prohibit the passage of ARP messages from this MAC only, and the other is to prohibit the passage of all messages from this MAC.

manipulate	command	clarification
Go to System View	system-view	
Configure the global rate threshold for ARP flooding attack prevention	arp anti-flood threshold *rate-limit*	Globally configure the rate threshold, which ranges from 1 to 100 pps.
Configure boycott action types and rate thresholds	arp anti-floodaction { deny-arp [threshold *rate-limit*] | deny-all [threshold *rate-limit*]] }	The threshold range is 1-100 pps. When the threshold parameter is not specified, i.e., the default threshold of 16 pps is used. When both global thresholds as well as action type thresholds are configured, the last configured threshold takes precedence.
Restore the anti-ARP flood attack rate threshold to its default value	undo arp anti-flood threshold	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring the Port Anti-ARP Attack Rate Thresholds	arp anti-flood threshold *rate-limit*	If the port is configured with this threshold then the port threshold is used, otherwise the global threshold is still used

[Example]

! Configure the boycott action to block all messages with a rate threshold of 10 pps

[GPON]arp anti-flood action deny-all threshold 10

21.2.4 Configuring Anti-ARP Flood Attack Banned MAC Auto Recovery Time

MACs banned from ARP flooding attack will automatically recover after a certain period of time has elapsed and can communicate again, and the recovery time is configurable.

manipulate	command	clarification
Go to System View	system-view	
Configure the automatic recovery time for banned MACs	arp anti-flood recover-time *time*	The auto-recovery time can be configured from 0 to 1440 minutes, with a default of 10 minutes. If the recovery time is configured as 0, it means that it will never be automatically recovered
Recovering a banned MAC auto-recovery time	undo arp anti-flood recover-	

	time	

[Example]

! Configure the banned MAC recovery time to 20 minutes

[GPON]arp anti-flood recover-time 20

21.2.5 Manual recovery of banned MACs against ARP flooding attacks

In addition to automatically restoring the banned MACs after the restoration time has elapsed, you can also manually restore the specified banned MACs or all banned MACs. configure the following:

manipulate	command	clarification
Go to System View	system-view	
Restore Banned MAC	arp anti-flood recover { *mac* | all }	When ALL is selected, it means to restore all banned MAC addresses

[Example]

! Restore banned MAC: 00:E1:4B:15:E5:1C

[GPON]arp anti-flood recover 00:E1:4B:15:E5:1C

! Restore all banned macs

[GPON]arp anti-flood recover all

21.2.6 Display anti-ARP flooding attack information

Anti-ARP flood attack information can be displayed in any view.

manipulate	command	clarification
Display anti-ARP flooding attack information	display arp anti-flood	

[Example]

! Display anti-ARP flood attack information

[GPON]display arp anti-flood

21.2.7 Bind the black hole MAC generated by the anti-ARP flooding attack to the general black hole MAC

The system supports binding black hole MACs generated by anti-ARP flooding attacks (which do not generate decompilations) to general black hole MACs (which do generate decompilations).

manipulate	command	clarification
Go to System View	system-view	
Bind the black hole MAC generated by the anti-ARP flooding attack to the general black hole MAC	arp anti-flood bind blackhole { *mac* | all }	When ALL is selected, it means binding all banned MAC addresses as black hole AMCs

[Example]

! Bind the banned MAC to the Black Hole MAC: 00:E1:4B:15:E5:1C

[GPON]arp anti-flood bind blackhole 00:E1:4B:15:E5:1C

! Bind all blackhole MACs generated by arp anti-flood

[GPON]arp anti-flood bind blackhole all

21.2.8 Enable/disable ARP anti-spoofing attack

Enable disable anti-ARP spoofing attack configuration as follows:

manipulate	command	clarification
Go to System View	system-view	
Enable anti-ARP spoofing attack	arp anti-spoofing	
Turn off protection against ARP spoofing attacks	undo arp anti-spoofing	

[Example]

! Enable anti-ARP spoofing attack

[GPON]arp anti-spoofing

21.2.9 Configuring an Anti-Unknown ARP Message Spoofing Policy

The system supports the setting of ARP anti-spoofing unknown packet processing policies, including discard policy and flood policy. discard policy means to discard unknown arp packets that do not have corresponding static arp table entries, and flood policy means to forward floods to each port. The default is discard policy.

manipulate	command	clarification
Go to System View	system-view	
Enable anti-ARP spoofing attack	arp anti-spoofing	
Configuring an Anti-Unknown ARP Message Spoofing Policy	arp anti-spoofing unknown { discard | flood }	

[Example]

! Set the unknown arp packet processing policy to flood

[GPON]arp anti-spoofing unknow flood

21.2.10 Enable/disable ARP message source MAC consistency checking

The source MAC in the Ethernet data frame header of some ARP attack packets is different from the source MAC in ARP protocol packets. When this function is turned on, it will check whether the Ethernet source address MAC of ARP packets delivered to the CPU is the same as the source MAC of ARP protocol packets, and discard such packets if they are different. This function is turned on by default.

manipulate	command	clarification
Go to System View	system-view	
Enable anti-ARP spoofing attack	arp anti-spoofing	
Enable ARP message source MAC consistency checking	arp anti-spoofing valid-check	
Disable ARP message source MAC consistency checking	undo arp anti-spoofing valid-check	

[Example]

! Disables the ARP message source MAC consistency check:

[GPON]undo arp anti-spoofing valid-check

! Turn on ARP message source MAC consistency checking:

[GPON]arp anti-spoofing valid-check

21.2.11 Enable/disable ARP anti-gateway impersonation

ARP gateway impersonation means that an attacker imitates a gateway address and sends a free ARP message inside the LAN whose source IP address is the gateway address. When the hosts in the LAN receive this message, they will change their original gateway address to the attacker's address, which will eventually cause all the hosts in the LAN to be unable to access the network. To solve this problem, you can enable the arp anti-gateway impersonation function. When this feature is turned on, if the device cpu receives an ARP message that conflicts with the gateway address, it drags the source MAC in the ARP protocol message into the MAC black hole and sends out its own free ARP. This check is mainly for ARP broadcast messages, and for non-device-specific ARP unicast messages that are not targeted at the device, if they are not on the cpu, no check is done. This feature is off by default.

manipulate	command	clarification
Go to System View	system-view	
Enable anti-ARP spoofing attack	arp anti-spoofing	
Enable ARP anti-gateway impersonation	arp anti-spoofing deny-disguiser	
Turn off ARP anti-gateway impersonation	undo arp anti-spoofing deny-disguiser	

[Example]

! Enable ARP anti-gateway impersonation:

[GPON]arp anti-spoofing deny-disguiser

! Turn off ARP anti-gateway impersonation:

[GPON]undo arp anti-spoofing deny-disguiser

21.2.12 Display anti-ARP spoofing attack information

You can display each configuration of ARP anti-spoofing in any view.

manipulate	command	clarification
Display anti-ARP flooding attack information	display arp anti-spoofing	

[Example]

! Displays anti-ARP spoofing flood attack information:

[GPON] display arp anti-spoofing

21.2.13 Configuring Trusted Ports for Anti-ARP Attacks

With this command, you can set the port as a trusted port, then ARP messages from this port are not checked for flooding attack and spoofing. Please configure it under port view.

manipulate	command	clarification
Go to System View	system-view	

Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the attack trust port	arp anti trust	
Remove attack trusted ports	undo arp anti trust	

[Example]

! Configure port 0/0/1 as a trusted port

[GPON-ethernet-0/0/1]arp anti trust

Chapter 22 DHCP-Relay Function

22.1 DHCP-Relay Function Introduction

DHCP messages are generally broadcast messages, so when the device is in a three-layer network structure and uses DHCP for IP address allocation, it is necessary to place a DHCP server in each VLAN broadcast domain, for the use of the device to form a three-layer network, it is necessary to place a DHCP server in each VLAN, which is a serious waste of resources, a better solution is to configure the DHCP relay function on the device to send DHCP messages to a DHCP server for processing, so that only one DHCP server needs to be configured. A better solution is to configure the DHCP relay function on this device to send DHCP messages to a DHCP server for processing, so that you only need to configure one DHCP server.

The system supports the following DHCP features:

Supports the DHCP relay function;

Supports assigning DHCP servers separately for each Layer 3 interface;

Supports built-in DHCP server;

Supports up to 128 address pools and up to 8 segments per address pool;

Support DHCP client to get system IP;

22.2 DHCP-Relay Function Configuration

22.2.1 DHCP-Relay Function Configuration List

The list of DHCP-Relay related feature configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable DHCP-Relay function	compulsory	22.2.2
Configuring the DHCP Server	compulsory	22.2.3
Layer 3 Interface Binding DHCP Server	compulsory	22.2.4
Displaying DHCP Server Configuration	selectable	22.2.5
Hide DHCP server	selectable	22.2.6
Configuring the DHCP Option82 Feature	selectable	22.2.7

22.2.2 Enable/disable DHCP-Relay function

By default, DHCP relay is turned off, if you want to turn on DHCP relay, please configure it under system view.

manipulate	command	clarification
Go to System View	system-view	
Start DHCP-Relay	dhcp-relay	
Disable DHCP-Relay	undo dhcp-relay	
Show DHCP-Relay	display dhcp-relay	

[Example]

! Enable DHCP relay function

```
[GPON]dhcp
```

! Disable the DHCP relay function

```
[GPON]undo dhcp
```

22.2.3 Configuring the DHCP Server

After enabling the DHCP relay function, you also need to configure the DHCP server and then assign the DHCP server to the appropriate interface. If the IP address of the DHCP server is configured as the IP address of any interface of the system or 127.0.0.1, the built-in DHCP server is used. You need to configure the IP address pool before using the built-in DHCP server.

manipulate	command	clarification
Go to System View	system-view	
Start the DHCP server and specify the appropriate interface IPs.	dhcp-server group-num ip ip-address	When the IP address of the server points to the IP of the system's own Layer 3 interface, it means that the system's own built-in DHCP server is used.
Shutting down the DHCP server	undo dhcp-server *group-num*	

[Example]

! Set the IP address of DHCP server 1 to 192.168.0.100

[GPON]dhcp-server 1 ip 192.168.0.100

! Shutting down the DHCP server 1

[GPON]undo dhcp-server 1

22.2.4 Layer 3 Interface Binding DHCP Server

After creating a DHCP server, you need to specify a DHCP server for each Layer 3 interface. The system relays DHCP messages to the DHCP server bound to that interface when that Layer 3 interface receives DHCP messages. use this command in Layer 3 interface configuration mode.

manipulate	command	clarification
Go to System View	system-view	
Entering Layer 3 interface mode	interface vlan-interface *vlan-id*	You can also enter Supervlan Layer 3 interface mode for configuration
Layer 3 Interface Binding DHCP Server	dhcp-server *group-num*	
Remove Layer 3 interface DHCP server bindings	undo dhcp-server *group-num*	

[Example]

! Specify the use of DHCP server 1 for VLAN interface 1

[GPON-vlanInterface-1]dhcp-server 1

! Delete the DHCP server for VLAN interface 1

[GPON-vlanInterface-1]undo dhcp-server

Description:

1. The Layer 3 interface can bind multiple DHCP servers. when the Layer 3 interface receives a DHCP message. it will relay this DHCP message to multiple DHCP servers at the same time;

2. When the DHCP server IP bound to the Layer 3 interface is the system's own Layer 3 interface IP, it means that it is

using its own built-in DHCP server;

22.2.5 Displaying DHCP Server Configuration

You can view the DHCP server configuration in any view. you can view the DHCP server configuration in two ways. one is to view all DHCP server groups. and the other is to view the DHCP servers of the Layer 3 interfaces.

manipulate	command	clarification
Displays the DHCP server configuration for all or a specified group number	display dhcp-server [*group-num*]	When group-num is not specified, displays all configured dhcp-server
Display the DHCP server configuration for a Layer 3 interface	display dhcp-server inerface [{ supervlan-interface | vlan-interface } *vlan-id*]	When no specific VLAN interface is specified, the DHCP-Server configuration for all VLAN interfaces is displayed

[Example]

! Show all DHCP servers

[GPON]display dhcp-server

! Display the first set of DHCP servers

[GPON]display dhcp-server 1

! Display the DHCP server for VLAN interface 1

[GPON]display dhcp-server interface vlan-interface 1

22.2.6 Hide DHCP server

When this function is activated, the DHCP server IP address in the IP address information requested by the DHCP client is not the real DHCP server IP address, but is replaced with the main IP address of the device's Layer 3 interface, so as to achieve the purpose of hiding the DHCP server IP.

When there are multi-level DHCP relays, if you use this function, you need all the relays to turn on this function, otherwise the network is not normal.

manipulate	command	clarification
Go to System View	system-view	
Hide DHCP server	dhcp-relay hide server-ip	
Unhide the DHCP server	undo dhcp-relay hide server-ip	

22.2.7 Configuring the DHCP Option82 Feature

DHCP Option82 is the Relay Agent Information option in the DHCP message defined in RFC 3046, which records the location information of the DHCP client. When a DHCP client sends a request message to a DHCP Relay or DHCP Snooping device, it will add Optin82 to the message. The administrator can get the location information of the DHCP client from Option 82 in order to locate the DHCP client and realize the control of the client such as security and billing.

Servers that support DHCP Option 82 can also specify an assignment policy for IP addresses and other parameters based on the information in this option, providing a more flexible address assignment scheme. DHCP Option 82 in this chapter now supports sub-option 1 (Circuit ID, Circuit ID sub-option) and sub-option 2 (Remote ID, Remote ID sub-option). Users

can configure the contents of Option 82 in two ways:

User-defined method: The user manually specifies the contents of Option 82;

Non-user-defined mode: the default normal mode or verbose mode is used to populate Option 82.

When the relay device receives the DHCP_DISCOVER and DHCP_REQUEST messages from the client, it adds the option82 content and then sends them to the server, while when it receives the server's response message, it strips the option82 content from the message and then forwards it to the client.

DHCP Option82 is configured as follows:

manipulate	command	clarification
Go to System View	system-view	
Turn on the Option82 function	dhcp option82	
Disable the Option82 function	undo dhcp option82	
Configure the fill mode for the option82 option	dhcp option82 format { extend | standard }	
Restore the default value of the fill mode for option82 option	undo dhcp option82 format	Defaults to standard mode
Configure the option82 detail message format	dhcp option82 information format { ascii | hex }	
Restore default option82 detail message format	undo dhcp option82 information format	Defaults to hex format
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the port's policy for handling option82 request messages	dhcp option82 strategy { append | drop | keep | replace }	Defaults to the replace policy
Restore the port's processing policy for option82 request messages	undo dhcp option82 strategy	
Configure the contents of the user-defined Circuit ID sub-option	dhcp option82 circuit-id string *circuit-id*	
Uncomment the user-defined Circuit ID sub-option	undo dhcp option82 circuit-id string	
Configuring the contents of the user-defined Remote ID sub-option	dhcp option82 remote-id string *string*	
Eliminate the user-defined Remote ID sub-option	undo dhcp option82 remote-id string	
Display option82 related configuration information	display dhcp option82	

Chapter 23 DHCP S nooping function

23.1 Introduction to DHCP Snooping Features

DHCP Snooping belongs to the Layer 2 function. The device records the user's IP and MAC address information by listening to DHCP messages. When this function is enabled, the device will filter all DHCP messages to the CPU for processing.

To allow users to be able to assign IP addresses through legitimate DHCP servers, DHCP Snooping categorizes ports into trusted ports and untrusted ports, and only trusted ports receive DHCP messages sent by DHCP servers that are forwarded normally, which prevents interference from illegal DHCP servers.

In terms of security, DHCP Snooping also allows configuration of the maximum number of DHCP clients that can exist on a

port or VLAN to prevent malicious application attacks. In addition, the DHCP Snooping feature can be used in conjunction with the IP-source-guard feature configured on the port to prevent IP address theft or users from setting static IP addresses privately.

23.2 DHCP Snooping Function Configuration

23.2.1 DHCP Snooping Feature Configuration List

The configuration list of DHCP Snooping-related features is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable DHCP Snooping function	compulsory	23.2.2
Configuring DHCP Snooping Trusted Ports	compulsory	23.2.3
Configuring the Maximum Number of Clients for DHCP Snooping	selectable	23.2.4
Configuring the DHCP Snooping Port Linkdown Fast Aging Table Entry Function	selectable	23.2.5
Enable/disable port IP-source-guard function	compulsory	23.2.6
Configure IP-source-guard static binding table entries	selectable	23.2.7
Display DHCP Snooping configuration information	selectable	23.2.8
Display DHCP Snooping user information	selectable	23.2.9
Delete the DHCP Snooping table entry	selectable	23.2.10

23.2.2 Enable/disable DHCP Snooping function

By default, DHCP Snooping is turned off, if you want to turn on DHCP Snooping, configure it in global mode.

manipulate	command	clarification
Go to System View	system-view	
Start DHCP Snooping	dhcp snooping	
Disable DDHCP Snooping	undo dhcp snooping	

[Example]

! Start the DHCP Snooping function

[GPON] dhcp snooping

23.2.3 Configuring DHCP Snooping Trusted Ports

Specifies a port as a trusted port. Normally, legitimate DHCP servers are connected over trusted ports.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Specify the trusted port	dhcp-snooping trust	
Specify an untrusted port	undo dhcp-snooping trust	Ports default to untrusted ports

[Example]

! Configuring Ethernet Port 1 as a DHCP Snooping Trusted Port Feature

[GPON-ethernet-0/0/1]dhcp-snooping trust

23.2.4 Configuring the Maximum Number of Clients for DHCP Snooping

The system supports configuring the maximum number of clients for a port or VLAN, which prevents DOS attacks on IP applications from malicious users and protects the DHCP server.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configure the maximum number of clients on a port	dhcp-snooping max-clients *num*	The maximum number of clients is configured in the range 0-2048, and a configuration of 0 means that no user is allowed to apply for an IP address.
Enter VLAN view	vlan vlan-id	
Configure the maximum number of clients for a VLAN	dhcp-snooping max-clients *num*	The maximum number of clients is configured in the range 0-2048, and a configuration of 0 means that no user is allowed to apply for an IP address.

[Example]

! Configure Ethernet port 1 for DHCP Snooping with a maximum number of clients of 100

[GPON-ethernet-0/0/1]dhcp-snooping max-clients 100

 Description:

When the maximum number of clients is configured for both the port and the VLAN, and both are in effect at the same time, the smallest value configured is the final value in effect.

23.2.5 Configuring the DHCP Snooping Port linkdown Fast Aging Table Entry Function

The system supports configuring the function of fast aging DHCP Snooping table entries when the port is linkdown. When the fast aging function is turned on, when a port experiences a linkdown, the corresponding DHCP Snooping table entry of the port will be aged immediately. When the fast aging function is disabled, when the port experiences linkdown, the DHCP Snooping table entry corresponding to the port will not be aged immediately, but will wait for the timeout to be aged.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Fast Aging Table Entry Function	dhcp-snooping port-down-action fast-remove	The device enables the port Linkdown fast aging table entry function by default
Disable fast aging table entries	undo dhcp-snooping port-down-action fast-remove	

[Example]

! Enable the DHCP Snooping port Linkdown fast aging table entry feature

[GPON]dhcp-snooping port-down-action fast-remove

23.2.6 Enable/disable port IP-source-guard function

By configuring the port IP-source-guard function, you can effectively prevent IP address theft or users from setting static IP addresses privately. After the IP-source-guard function is enabled, the device forwards data messages only to users who obtain IP addresses dynamically through DHCP or meet the requirements of statically binding IP-source-guard table entries.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Enable ip-source-guard function	ip-source-guard	
Disable ip-source-guard function	undo ip-source-guard	

[Example]

! Enable the Ethernet port 1 IP-source-guard feature

[GPON-ethernet-0/0/1]ip-source-guard

23.2.7 Configuring IP-source-guard Static Binding Table Entries

By configuring the IP source guard static binding table entry, the user corresponding to this table entry can forward data messages normally without obtaining an IP address through dhcp.

manipulate	command	clarification
Go to System View	system-view	
Configuring static ip-source-guard table entries	ip-souce-guard bind ip *ip-address* [mac *mac-address* [interface ethernet *interface-num*]]	When no MAC address or port number is specified, the user can match the static table entry by meeting the IP address to be forwarded
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the ip-source-guard matching method for the port	ip-source-guard { ip | ip-mac | ip-mac-vlan }	If selected as IP, it means that the port only needs to match the IP field in the data message

[Example]

! Bind Ethernet port 1 IP-source-guard table entry with MAC address 00:E0:4C:15:E5:1C, IP address 192.168.1.100, VLAN 100

[GPON]ip-source-guard bind ip 192.168.1.100 mac 00:E0:4C:15:E5:1C interface ethernet 0/0/1

23.2.8 Display DHCP Snooping configuration information

You can display DHCP Snooping configuration information in any view.

manipulate	command	clarification
Display DHCP Snooping configuration information for a port	display dhcp-snooping interface [ethernet *interface-num*]	When the port number is not specified, it means to display information of all ports
Display DHCP Snooping	display dhcp-snoopingvlan [*vlan-*	When vlan-id is not specified, it means

configuration information for a VLAN	*id*]	displaying information for all vlan's

[Example]

! Display DHCP Snooping configuration information

[GPON]display dhcp-snooping interface

23.2.9 Display DHCP Snooping user information

You can display DHCP Snooping user information in any view, including the user's IP address, MAC address, ingress VLAN, and ingress port information.

manipulate	command	clarification
Display DHCP Snooping user information	display dhcp-snooping clients	

[Example]

! Display DHCP Snooping user information

[GPON]display dhcp-snooping clients

23.2.10 Delete the DHCP Snooping table entry

The system supports deleting specific dhcp snooping table entries with the command. configured as follows:

manipulate	command	clarification
Go to System View	system-view	
Delete the DHCP Snooping table entry	clear dhcp-snooping [mac *mac-address* | ip *ip-address* | interface ethernet *interface-num* | vlan *vlan-id*]	

[Example]

! Delete all DHCP Snooping table entries

[GPON]clear dhcp-snooping

Chapter 24 Local IP address pool configuration

24.1 Local IP Address Pool Introduction

The local IP address pool is a database of IP addresses assigned to DHCP clients by the DHCP server, through which the DHCP server assigns IP addresses to DHCP clients. The IP address pool allows you to configure the parameters that the DHCP server assigns to DHCP clients. Configuration options include: gateway and mask for DHCP clients, DNS servers, WINS servers, lease period, range of IP addresses to be assigned to DHCP clients, and prohibition of assigning specific IP addresses. The local IP address pool must be configured before the system's built-in DHCP server can assign IP addresses to DHCP clients.

24.2 Local IP address pool configuration

24.2.1 Local IP Address Pool Configuration Task List

The list of configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enter IP address pool view	compulsory	24.2.2
Configure the local IP address pool gateway and subnet masks	compulsory	24.2.3
Configure local IP address pool segments	compulsory	24.2.4
Disable/activate the specified IP address in the local IP address pool	selectable	24.2.5
Configuring the Local IP Address Pool Lease Period	selectable	24.2.6
Configuring Local IP Address Pool DNS	selectable	24.2.7
Configuring the Local IP Address Pool WINS	selectable	24.2.8
Display the local IP address pool configuration	selectable	24.2.9
Configuring the dhcp-client bind function	selectable	24.2.10
Show dhcp-client bind configuration	selectable	24.2.11
Add/remove dhcp-client client list	selectable	24.2.12
Display dhcp-client client list configuration information	selectable	24.2.13

24.2.2 Enter IP address pool view

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Create and enter IP address pool view	ip pool ippoolname	If no IP address pool has been created, this is the Create IP Address Pool command.
Delete IP address pool	undo ip pool *ippoolname*	

[Example]

! Enter the IP address pool view

[GPON]ip pool test

! Delete IP address pool test

[GPON]undo ip pool test

24.2.3 Configure the local IP address pool gateway and subnet masks

Please make the following configurations under the local IP address pool view.

manipulate	command	clarification
Go to System View	system-view	
Enter IP address pool view	ip pool ippoolname	
Configure IP address pool gateways and masks	gateway ip-address mask	

[Example]

! Configure the local IP address pool gateway and subnet mask

[GPON-ip-pool-test]gateway 192.168.1.100 255.255.255.0

 Attention:

All IP addresses in the local IP address pool must be within the address area determined by this gateway and subnet mask, and the IP addresses in the address pool cannot contain gateway addresses.

24.2.4 Configure local IP address pool segments

Please make the following configurations under the local IP address pool view.

manipulate	command	clarification
Go to System View	system-view	
Enter IP address pool view	ip pool ippoolname	
Configure IP address pool segments	section section-id from-ip to-ip	section-id is the section number of this address pool, up to 8 groups can be assigned. from-ip is the starting address of this address segment and to-ip is the ending address of this address segment. These two addresses must be within the address area determined by the gateway and subnet mask, and must not contain the gateway address.
Deleting an IP address pool segment	undo section *section-id*	

[Example]

! Create the network segment of the local IP address pool test

[GPON-ip-pool-test] section 0 192.168.1.100 192.168.1.200

! Delete segment 0 from the local IP address pool test

[GPON-ip-pool-test]undo section 0

24.2.5 Disable/activate the specified IP address in the local IP address pool

Please perform the following configurations under the local IP address pool view.

manipulate	command	clarification
Go to System View	system-view	
Enter IP address pool view	ip pool ippoolname	
Disable/activate the specified IP address in the local IP address pool	ip { disable | enable } *ip-address*	

[Example]

! Disable the address specified in the local IP address pool segment 192.168.1.100

[GPON-ip-pool-test]ip disable 192.168.1.100

! Activate the address specified in the local IP address pool segment 192.168.1.100

[GPON-ip-pool-test]ip enable 192.168.1.100

24.2.6 Configuring the Local IP Address Pool Lease Period

Please make the following configurations under the local IP address pool view.

manipulate	command	clarification
Go to System View	system-view	
Enter IP address pool view	ip pool ippoolname	
Configuring the Local IP Address Pool Lease Period	lease day:hour:min	day:hour:min is the rental time, accurate to the minute, the shortest is 0:0:1, the longest is 999:23:59, the default rental period for 1 day

[Example]

! Configuration rental period 1 day 1 hour 1 minute

[GPON-ip-pool-test]lease 1:1:1

24.2.7 Configuring Local IP Address Pool DNS

Please make the following configurations under the local IP address pool view.

manipulate	command	clarification
Go to System View	system-view	
Enter IP address pool view	ip pool ippoolname	
Configuring Local IP Address Pool DNS	dns { primary-ip | second-ip | third-ip | fourth-ip } *ip-address*	Supports configuration of four DNS
Delete the local IP address pool DNS	undo dns { primary-ip | second-ip | third-ip | fourth-ip }	
Configuring DNS Suffixes	dns suffix *suffix-name*	
Remove the DNS suffix	undo dns suffix	

[Example]

! Configure Primary DNS

[GPON-ip-pool-test]dns primary-ip 192.168.0.100

! Delete primary DNS

[GPON-ip-pool- test]undo dns primary-ip

24.2.8 Configuring the Local IP Address Pool WINS

Please make the following configurations under the local IP address pool view.

manipulate	command	clarification
Go to System View	system-view	
Enter IP address pool view	ip pool ippoolname	
Configuring the Local IP Address Pool WINS	wins { primary-ip | second-ip } *ip-address*	Supports configuration of 2 WINS
Delete local IP address pool WINS	undo wins { primary-ip | second-ip }	

[Example]

! Configure the master WINS

[GPON-ip-pool- test]wins primary-ip 192.168.1.100

! Delete primary WINS

[GPON-ip-pool- test]undo wins primary-ip

24.2.9 Display the local IP address pool configuration

The IP address pool configuration can be viewed in either view.

manipulate	command	clarification
Display IP address pool configuration	display ip pool [ippool-name [section-num]]	When no IP address pool or section is specified, all IP address pool information is displayed

[Example]

! Show all IP address pool configurations

[GPON]display ip pool

24.2.10 Configuring the dhcp-client bind function

After configuring the dhcp-client bind function, when a client applies for an IP address through DHCP, the DHCP server will assign an IP address bound to the client based on its MAC address information. If the client MAC address information is not bound, the DHCP server will not assign an IP address to the client. Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Turning on dhcp-clien bindings	dhcp-client bind	
Disable dhcp-clien binding function	undo dhcp-client bind	

[Example]

! Turn this feature on

[GPON] dhcp-client bind

! Disable this function

[GPON]undo dhcp-client bind

24.2.11 Show dhcp-client bind configuration

You can view the dhcp-client bind feature configuration in any view.

manipulate	command	clarification
Display the dhcp-client bind function	display dhcp-client bind	

[Example]

! Display the dhcp-client bind configuration

[GPON]display dhcp-client bind

24.2.12 Add/remove dhcp-client client list

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Turning on dhcp-clien bindings	dhcp-client bind	
Add a list of dhcp-client clients	dhcp-client mac-address ip-address vlan-id username	After the client list is added, clients that match the mac address table entry are assigned the IP address bound in the entry
Delete the dhcp-client client list	undo dhcp-client { *mac-address vlan-id* | all }	

[Example]

! Add client with mac address 00:E1:4B:15:E5:1C, vlan 100, and ip address 192.168.1.100 with username test.

[GPON]dhcp-client00:E1:4B:15:E5:1C 192.168.1.100 100 test

! Delete client with mac address 00:E1:4B:15:E5:1C and vlan 100.

[GPON]undo dhcp-client00:E1:4B:15:E5:1C 100

24.2.13 Display dhcp-client client list configuration information

You can view dhcp-client configuration information in any view:

manipulate	command	clarification
Display dhcp-client client list configuration information	display dhcp-client [ip *ip-address*] | [mac *mac-address*]	When no IP or MAC parameters are entered, this means that all dhcp-client information is displayed

[Example]

! Display all dhcp-client client list configuration information

[GPON]display dhcp-client

Chapter 25 IGMP Snooping Configuration

25.1 Introduction to IGMP Snooping Protocol

IGMP (Internet Group Manangement Protocol) is a part of the IP protocol that supports and manages IP multicast between hosts and multicast routers. ip multicast allows IP datagrams to be transmitted to a collection of hosts that form a multicast group, where the relationship of the multicast group members is dynamic, and hosts can dynamically join or leave the group, thus minimizing the network load and enabling efficient data transmission over the network.

IGMP Snooping is used to listen to IGMP messages between hosts and routers, and can dynamically create, maintain, and delete multicast address tables based on the joining and leaving of group members, and multicast data frames are forwarded based on their respective multicast address tables.

25.2 IGMP Snooping Configuration

25.2.1 IGMP Snooping Configuration Task List

The list of IGMP Snooping configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable the IGMP Snooping function	compulsory	25.2.2
Configuring IGMP Snooping Member Port Aging Time	selectable	25.2.3
Configuring Maximum Response Time for IGMP Snooping Queries	selectable	25.2.4
Configuring the IGMP Snooping Port Fast Leave Function	selectable	25.2.5
Configuring the IGMP Snooping Port Learning Multicast Groups Limit	selectable	25.2.6
Configuring IGMP Snooping Black and White Lists	selectable	25.2.7
Configuring the IGMP Snooping Route Port Forwarding Function	selectable	25.2.8
Configuring the IGMP Snooping Querier Switch	selectable	25.2.9
Configuring the IGMP Snooping Querier Send Message Interval	selectable	25.2.10
Configuring the IGMP Snooping Generic Query Message Sending VLANs	selectable	25.2.11
Configuring IGMP Snooping General Query Maximum Response Time	selectable	25.2.12
Configuring IGMP Snooping Generic Query Message Source IP Addresses	selectable	25.2.13
Configuring IGMP Snooping Route Port Aging	selectable	25.2.14
Add/Remove IGMP Snooping Routing Ports	selectable	25.2.15
Configuring Multicast VLANs for IGMP Snooping Ports	selectable	25.2.16
Display IGMP Snooping configuration information	selectable	25.2.17
Enable/disable IGMP Snooping multicast preview function	selectable	25.2.18
Configuring IGMP Snooping Multicast Preview Control Parameters	selectable	25.2.19
Configuring IGMP Snooping Multicast Preview Channels	selectable	25.2.20
Display IGMP Snooping Multicast Preview Information	selectable	25.2.21
Create/Delete IGMP Snooping profile	selectable	25.2.22
Configuring IGMP Snooping profile type and address range	selectable	25.2.23
Reference IGMP Snooping profile configuration	selectable	25.2.24
Display IGMP Snooping profile configuration information	selectable	25.2.25
Configuring the IGMP Snooping mvr Function	selectable	25.2.26

Display the multicast table entries learned by IGMP Snooping	selectable	25.2.27

25.2.2 Enable/disable the IGMP Snooping function

To control whether IGMP Snooping establishes a mac address multicast forwarding table at Layer 2, you can use the following commands to enable/disable the IGMP Snooping function:

manipulate	command	clarification
Go to System View	system-view	
Enable igmp-snooping function	igmp-snooping	By default, the igmp-snooping function is disabled
Disabling the igmp-snooping Function	undo igmp-snooping	

[Example]

! Enabling IGMP Snooping

```
[GPON] igmp-snooping
```

25.2.3 Configuring IGMP Snooping Member Port Aging Time

Configure the IGMP Snooping member port aging time with the following command in system view:

manipulate	command	clarification
Go to System View	system-view	
Configure member port aging time	igmp-snooping host-aging-time *seconds*	Member aging time configuration range is 10-1000000S, the default value is 300S
Restore the default member port aging time	undo igmp-snooping host-aging-time	

[Example]

! Configure the aging time for dynamic multicast port members learned through IGMP Snooping to be 10 seconds

```
[GPON]igmp-snooping host-aging-time 10
```

25.2.4 Configuring Maximum Response Time for IGMP Snooping Queries

The function of querying the maximum response time is to delete the maximum waiting time of group member ports when the device receives an IGMP leave message. the relevant configurations are as follows:

manipulate	command	clarification
Go to System View	system-view	
Configuring the Maximum Response Time for Queries	igmp-snooping max-response-time *seconds*	The maximum response time for query is configured from 1-100S, and the default value is 10S.
Restore default query maximum response time	undo igmp-snooping max-response-time	

[Example]

! Configure the maximum response time for IGMP Snooping to be 15 seconds

```
[GPON]igmp-snooping max-response-time 15
```

25.2.5 Configuring the IGMP Snooping Port Fast Leave Function

Configure the fast leave function of a port. after a member port enables the fast leave function and receives an IGMP leave message, it will immediately age the group member port:

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring the Port Fast Leave Function	igmp-snooping fast-leave	Port defaults to disable Quick Leave
Disable port fast leave feature	undo igmp-snooping fast-leave	

[Example]

! Enable fast leave on Ethernet port 1

[GPON-ethernet-0/0/1]igmp-snooping fast-leave

25.2.6 Configuring IGMP Snooping Port Learning Multicast Number Limits

After you configure the maximum number of multicast groups that a port is allowed to learn, when the system receives multicast group IGMP Report messages that exceed the limit value, the system will no longer learn multicast groups that exceed the limit number and discard the messages that exceed the limit.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configure the port multicast learning number limit	igmp-snooping group-limit *limit*	The limit value is configured in the range of 0-1023, and a configuration of not 0 indicates that no multicast groups are learned. The default value is the maximum value of 1023
Remove the limit on the number of ports for multicast learning	undo igmp-snooping group-limit	

[Example]

! Configure the maximum number of multicast groups allowed to be learned on Ethernet port 1 to 10

[GPON-ethernet-0/0/1]igmp-snooping group-limit 10

25.2.7 Configuring IGMP Snooping Black and White Lists

Configure the black-and-white list of igmp-snooping and the default group learning rule. after configuration. the system will learn the rule according to the learning rule. Confirm whether to learn multicast groups.

Configure the multicast group learning mode in system view and the black and white list of igmp-snooping in port view. after configuring the global multicast group learning mode, if no multicast join message matches the black and white list list configured in port view, it will be controlled according to the global black and white list mode:

manipulate	command	clarification

Go to System View	system-view	
Configuring System Multicast Group Learning Mode	igmp-snooping { permit | deny } group all	The system learns all multicast groups by default
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configure the port multicast learning number limit	igmp-snooping { permit | deny } { group *group-address* vlan *vlan-id* | group-range *group-address* multi-count *count* vlan *vlan-id* }	When a single group is configured, it indicates black and white list control for a single multicast group. When group-range is configured, it indicates black and white list control for a group of multicast groups.
Remove the limit on the number of ports for multicast learning	undo igmp-snooping group-limit	

[Example]

! Configure the system to learn all multicast groups by default

[GPON]igmp-snooping permit group all

! Configure Ethernet port 1 not to learn group 01:00:5e:01:02:03 of VLAN 100

[GPON-ethernet-0/0/1]igmp-snooping deny group 01:00:5e:01:02:03 vlan 100

! Configure Ethernet port 1 not to learn the 32 consecutive multicast MAC addresses starting with group 01:00:5e:01:02:03 for VLAN 100

[GPON-ethernet-0/0/1]igmp-snooping deny group-range 01:00:5e:01:02:03 multi-count 32 vlan 100

25.2.8 Configuring the IGMP Snooping Route Port Forwarding Function

The port in a device port that receives IGMP query messages is called a multicast routing port. Configure whether to automatically join the routing port to the dynamic multicast learned by IGMP Snooping. not by default. Perform the following configuration under system view.

manipulate	command	clarification
Go to System View	system-view	
Configuring Routed Port Forwarding	igmp-snooping route-port forward	Route port forwarding is not enabled by default
Eliminate Route Port Forwarding	undo igmp-snooping route-port forward	

[Example]

! Configure to auto-join routed ports to the dynamic multicast learned by IGMP Snooping

[GPON]igmp-snooping route-port forward

25.2.9 Configuring the IGMP Snooping Querier Switch

In order to establish a multicast routing table, multicast routers maintain multicast table entries with IGMP generic query

messages sent proactively; the unit that sends the messages is called the querier.

The IGMP Snooping protocol itself does not define the function of sending general query messages. you can configure the IGMP Snooping querier to allow the device to send general query messages to achieve the maintenance of multicast table entries. the system does not enable the querier function by default. the relevant configuration is as follows.

manipulate	command	clarification
Go to System View	system-view	
Open the Finder	igmp-snooping querier	Disable the querier function by default
Close Finder	undo igmp-snooping querier	

[Example]

! will turn on the querier and cause it to send IGMP generic query messages

[GPON] igmp-snooping querier

25.2.10 Configuring the IGMP Snooping Querier Send Message Interval

Configure the interval between every two times that the querier sends IGMP general query messages, the default is 60s.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Querier Message Transmission Interval	igmp-snooping query-interval *seconds*	The querier send message interval configuration range is 1-30000S, the default value is 60S
Restore the default querier message sending interval	undo igmp-snooping query-interval	

[Example]

! Configure the querier to send generic query messages at an interval of 90 seconds

[GPON] igmp-snooping query-interval 90

25.2.11 Configuring IGMP Snooping Generic Query Message Sending VLANs

When sending an IGMP general query, you must specify a vlan, after which the message is forwarded to all ports of that vlan. Configure the vlan to which the IGMP generic query sent by the querier is to be sent; the default is vlan 1.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Generic Query Message Sending VLAN	igmp-snooping querier-vlan *vlan-id*	The default VLAN is 1
Restore the default generic query message sending VLANs	undo igmp-snooping query-interval	

[Example]

! Configure the querier to send a generic query message to vlan 10

[GPON] igmp-snooping querier-vlan 10

25.2.12 Configuring IGMP Snooping General Query Maximum Response Time

Configure the maximum response time of the host after receiving a generic query, that is, the value of the response field carried by the IGMP generic query message sent by the querier, which is 10 seconds by default. if the host does not respond to the multicast answer message within the maximum response time, the member port will be deleted.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Maximum Response Time for Generic Queries	igmp-snooping query-max-response *seconds*	Maximum response time configuration range is 1-25S, default value is 10S
Restore default generic query maximum response time	undo igmp-snooping query-interval	

[Example]

! Configure the maximum response time of the host after a generic query to 15s

[GPON] igmp-snooping query-max-respon 15

25.2.13 Configuring IGMP Snooping Generic Query Message Source IP Addresses

Configure the source IP address carried by the generic query message, the purpose of which is to indicate the destination IP of the host in response to that query, which is 0.0.0.0 by default.

manipulate	command	clarification
Go to System View	system-view	
Configure a generic query source IP address	igmp-snooping general-query source-ip *ipaddress*	The default source IP address is 0.0.0.0
Restore the default generic query source IP address	undo igmp-snooping general-query source-ip	

[Example]

! Configure the source IP address of IGMP query messages sent by the querier to be 192.168.1.100

[GPON] igmp-snooping general-query source-ip 192.168.1.100

25.2.14 Configuring IGMP Snooping Route Port Aging

The port of a device port that receives an IGMP query message is called a multicast routing port. The system supports configuring whether a routing port is aging or not, and routing ports are aging-capable by default.

manipulate	command	clarification
Go to System View	system-view	
Configuring Routed Port Aging	igmp-snooping router-port-age { on | off | *age-time* }	The aging time is configurable from 10 to 1000000, and the default value is 300S.
Cancel routed port aging	undo igmp-snooping router-port-age	

[Example]

! Configure routed port aging to be on

[GPON]igmp-snooping router-port-age on

! Configure the routing port to be removed (aged) after a period of time until the

[GPON]igmp-snooping router-port-age 60

25.2.15 Add/Remove IGMP Snooping Routing Ports

IGMP Snooping routing port, the uplink port on which the device receives an IGMP leave or report message from the host and needs to forward it, that is, the uplink routing port on which the host is configured to respond to the message.

manipulate	command	clarification
Go to System View	system-view	
Adding a Routing Port	igmp-snooping route-port vlan *vlan-id* interface ethernet *interface-list*	
Deleting Routed Ports	undo igmp-snooping route-port vlan *vlan-id* interface ethernet *interface-list*	

[Example]

! Configure Ethernet port 1 of vlan 100 as an IGMP Snooping routing port

[GPON]igmp-snooping route-port vlan 100 interface ethernet 0/0/1

25.2.16 Configuring Multicast VLANs for IGMP Snooping Ports

This command is used to specify a vlan for a port. all IGMP messages listened to through IGMP Snooping are considered to be from this VLAN and the VLAN ID carried in the IGMP message is ignored. this function can be applied to distinguish the user's unicast from multicast services as well.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configuring Multicast VLANs	igmp-snooping multicast vlan *vlan-id*	
Deleting Routed Ports	undo igmp-snooping multicast vlan	

[Example]

! Configure the multicast vlan for Ethernet port 1 to vlan 100

[GPON-ethernet-0/0/1]igmp-snooping multicast vlan 100

25.2.17 Display IGMP Snooping configuration information

You can view IGMP Snooping related configuration information under any attempt. The displayed information includes aging time configuration, routing port configuration, multicast VLAN configuration, black and white list configuration, multicast learning limit configuration, and so on.

manipulate	command	clarification
View all IGMP Snooping configuration information	display igmp-snooping	
Viewing Multicast Host Records	display igmp-snooping record-host	
View multicast dynamic routing port aging information	display igmp-snooping router-dynamic	
View multicast static route port aging information	display igmp-snooping router-static	
Viewing Multicast Message Statistics	display igmp-snooping statistics { vlan *vlan-id* | interface ethernet *interface-list* }	

[Example]

! Configuring IGMP Snooping Configuration Information

[GPON]display igmp-snooping

25.2.18 Enable/disable IGMP Snooping multicast preview function

IGMP Snooping provides multicast preview function, multicast users can preview and watch multicast programs under the control of preview parameter, you can use the following commands to enable/disable the IGMP Snooping multicast preview function.

manipulate	command	clarification
Go to System View	system-view	
Enable Multicast Preview	igmp-snooping preview	By default, the preview function is turned off
Turn off multicast preview	undo igmp-snooping preview	

[Example]

! Enable IGMP Snooping multicast preview function

[GPON]igmp-snooping preview

25.2.19 Configuring IGMP Snooping Multicast Preview Control Parameters

The IGMP Snooping multicast preview function can limit the single preview duration, preview interval, preview reset duration, and number of allowed previews for multicast. You can use the following commands to configure the IGMP Snooping multicast preview control parameters.

manipulate	command	clarification
Go to System View	system-view	
Configuring Multicast Preview Parameters	igmp-snooping preview { time-once *time-once* time-interval *time-interval* time-reset *time-reset* permit-times *preview-times* }	
Restore the default configuration of multicast preview parameters	undo igmp-snooping preview { time-once | time-interval | time-reset | permit-times }	

[Parameter Description]

time-once: time duration of single preview, range 60-300s, default value 180s

time-interval: preview interval, range 180-600s, default 300s

time-reset: preview reset time, range 1800-7200s, default value 3600s

preview-times: allow preview times, range 1-10, default value 5

[Example]

! Configure the IGMP Snooping single preview duration to 100s, the preview interval to 200s, and the number of allowed previews to 5

[GPON]igmp-snooping previewtime-once 100 time-interval 200 permit-times 5

25.2.20 Configuring IGMP Snooping Multicast Preview Channels

The IGMP Snooping multicast preview function is valid only for specific multicast channels. you can use the following commands to add or remove IGMP Snooping multicast preview channels.

manipulate	command	clarification
Go to System View	system-view	
Configuring Multicast Preview Channels	igmp-snooping preview group-ip *ip-address* vlan *vlan-id* interface ethernet *interface-num*	

Delete Multicast Preview Channel	undo igmp-snooping preview group-ip *ip-address* vlan *vlan-id* interface ethernet *interface-num*	

[Parameter Description]

A.B.C.D: multicast ip address, range 224.0.0.1-239.255.255.254

vlan-id: multicast vlan, range 1-4094

interface-num: multicast port number, range determined by device type

[Example]

! Add an IGMP Snooping Multicast Preview Channel

```
[GPON]igmp-snooping preview group-ip 224.0.0.9 vlan 100 interface ethernet 0/0/1
```

25.2.21 Display IGMP Snooping Multicast Preview Information

You can display IGMP Snooping multicast preview information in any view mode.

manipulate	command	clarification
Display multicast preview information	display igmp-snooping preview	

[Example]

! Display the current multicast preview configuration information for IGMP Snooping

```
[GPON]display igmp-snooping preview
```

25.2.22 Create/Delete IGMP Snooping profile

IGMP Snooping provides the black and white list function in the profile mode. first create several profiles under system view and then configure the list of profiles referenced by the port under port view. You can use the following commands to create/delete an IGMP Snooping profile.

manipulate	command	clarification
Go to System View	system-view	
Create and enter the profile view	igmp-snooping profile *profile-id*	
Delete the specified profile	undo igmp-snooping profile [*profile-list*]	Do not allow deletion of profiles that are already referenced by a port

[Parameter Description]

profile-id: profile identifier, range 1-16

profile-list: profile list, range 1-16

[Example]

Create IGMP Snooping profile 1! Create IGMP Snooping profile 1

```
[GPON]igmp-snooping profile 1
```

25.2.23 Configuring IGMP Snooping profile type and address range

You can use the following commands to configure/delete the type and range of IGMP Snooping profile, where type means permit/deny and range can be configured using multicast IP address or MAC address.

manipulate	command	clarification

Go to System View	system-view	
Enter the profile view	igmp-snooping profile *profile-id*	
Specify the type of profile	profile limit { permit | deny }	The default is the permit type, which does not allow modification of profiles that are already referenced by the port
Configuring Multicast IP Address Ranges	ip range start-ip end-ip [vlan vlan-id]	Not specifying a vlan means that any vlan applies.
Configuring Multicast MAC Address Ranges	mac range start-mac end-mac [vlan vlan-id]	
Deleting Multicast IP Ranges	undo ip range [*start-ip end-ip* [vlan *vlan-id*]]	
Delete multicast MAC range	undo mac range [*start-mac end-mac* [vlan *vlan-id*]]	

[Parameter Description]

Profile type: there are two types of profiles, when the profile is configured as the permit type, it means that only the multicast groups specified in the profile are allowed to be learned, and when the profile is configured as the deny type, it means that the multicast groups specified in the profile are not allowed to be learned.

start-ip: start address of IP range, range 224.0.0.1-239.255.255.254

end-ip: end address of the IP range, range 224.0.0.1-239.255.255.254

start-mac: start address of the MAC range, in the range 01:00:5e:H:H:H, i.e., must start with 01:00:5e

end-mac: end address of the MAC range, in the range 01:00:5e:H:H:H, i.e. it must start with 01:00:5e

vlan-id: vlan used for multicast services, range 1-4094

[Example]

! Set the IP range and MAC range in IGMP Snooping profile 1 and specify it as deny type

[GPON-igmp-profile-1]ip range 224.0.0.1 224.0.0.10vlan 100

[GPON-igmp-profile-1]mac range01:00:5e:01:02:03 01:00:5e:01:02:13

[GPON-igmp-profile-1] profile limit deny

25.2.24 Reference IGMP Snooping profile configuration

IGMP Snooping profiles take effect only when they are referenced by a port, and when a port is configured to reference a profile, the types of the profiles must be the same, that is, the same port can only reference one type of profile (permitted or denied). When a port references a permit profile, it can only learn the multicast groups defined by the corresponding profile; when a port references a deny profile, it can learn all multicast groups except those defined by the profile; when a port does not reference any profile, it learns multicast groups as normal. The following commands can be used to configure/de-reference a port to an IGMP Snooping profile.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Specify the list of profiles referenced by the port	igmp-snooping profile refer *profile-list*	

Cancel the list of port-referenced profiles	undo igmp-snooping profile refer [*profile-list*]	When profile-list is not specified, it means that all the profile-list references for this port are canceled.

[Example]

! Configure Ethernet port 1 to reference profiles 1 and 3

[GPON-ethernet-0/0/1]igmp-snooping profile refer 1,3

25.2.25 Configuring IGMP Snooping MVR Features

Under the traditional multicast on-demand method, users in each VLAN have to perform multicast on-demand separately, and the multicast data is copied in each VLAN, wasting bandwidth. After enabling MVR, these different user VLANs can be added to a specified multicast VLAN, so that the multicast source only needs to send a multicast data message down.

The principle of realization is as follows:

1. When the device receives a Report message, it first searches for mvr table entries with the message's vlanID as the c-vlan keyword, and if it cannot find any table entries, both c-vlan and sp-vlan are equal to the message's vlanID, and then learns the multicast group with the c-vlan (i.e., the message's own vlanID), and finally modifies the message's vlanID to sp-vlan to the routing port;

2. the device receives Leave messages with similar processing as REPORT messages, leaving with c-vlan and forwarding with sp-vlan to the routing port;

3. When the device receives a Query message, it first searches for mvr table entries with the vlanID of the message as the sp-vlan keyword, and if it cannot find one, both c-vlan and sp-vlan are equal to the vlanID, and then learns the routing ports with the sp-vlan, and finally forwards the Query message to all c-vlan multicast member ports under the sp-vlan.

manipulate	command	clarification
Go to System View	system-view	
Configure mvr table entries	igmp-snooping mvr c-vlan *vlan-list* sp-vlan *vlan-ID*	
Delete mvr table entries	undo igmp-snooping mvr c-vlan *vlan-list* sp-vlan *vlan-ID*	
Delete the mvr table entry associated with c-vlan.	undo igmp-snooping mvr c-vlan *vlan-list*	
Delete the mvr table entry associated with sp-vlan.	undo igmp-snooping mvr sp-vlan *vlan-id*	
View all mvr table entries	display igmp-snooping mvr	
Display the mvr table entries related to c-vlan.	display igmp-snooping mvrc-vlan *vlan-list*	
Display the mvr table entries related to sp-vlan.	display igmp-snooping mvr sp-vlan *vlan-ID*	

[Example]

! Configure the mvr function with a user c-vlan of 10 and multicast sp-vlan of 20

[GPON] igmp-snooping mvr c-vlan 10 sp-vlan 20

25.2.26 Display IGMP Snooping profile configuration information

IGMP Snooping profile configuration information can be displayed at any attempt:

manipulate	command	clarification
Go to System View	system-view	
Display profile configuration information as a list of profiles	display igmp-snooping profile [*profile-list*]	When profile-list is not specified, it means to display all the profile information.
Display profile configuration	display igmp-snooping profile	When the port number is not specified, the

information as a list of ports	interface [ethernet *interface-list*]	profile information for all ports is displayed.
Display profile configuration information in VLAN format	display igmp-snooping profile vlan [*vlan-id*]	When vlan-id is not specified, it means to display profile information of all VLANs

[Example]

! Display configuration information for profiles 1, 2, 3, 4, and 5

[GPON]display igmp-snooping profile 1-5

25.2.27 Display the multicast table entries learned by IGMP Snooping

You can display the multicast table entries learned by IGMP Snooping at any attempt.

manipulate	command	clarification
View all multicast table entries	display multicast	This command displays only multicast table Layer 2-related information, including multicast MAC, VID, Port
View multicast table entries based on multicast MACs	display multicast mac-address *mac-address*	This command displays only multicast table Layer 2-related information, including multicast MAC, VID, Port
View multicast table entries based on port	display multicast igmp-snooping interface [ethernet *interface-list*]	This command displays multicast table multicast MAC, multicast IP, VID, Port, and aging time information
View multicast table entries based on multicast IP	display multicast ip-address *ip-address*	This command displays multicast table multicast MAC, multicast IP, VID, Port, and aging time information

[Example]

! Show all multicast table entries

[GPON]display multicast

! Displays the multicast table entries corresponding to the multicast IP of 224.1.1.1.

[GPON]display multicast ip-address 224.1.1.1

Chapter 26 MLD Snooping Configuration

26.1 MLD Snooping Protocol Profile Configuration

The MLD (Multicast Listener Discovery) network group management protocol is part of the IPv6 protocol that supports and manages IP multicast between hosts and multicast routers. ip multicast allows IP datagrams to be transmitted to a collection of hosts that make up a multicast group, and multicast group members are dynamically related so that hosts can dynamically join or leave the group. groups, thereby minimizing network load and enabling efficient data transmission over the network.

MLD Snooping is used to listen to multicast messages between hosts and routers, and can dynamically create, maintain, and delete multicast address tables based on the joining and leaving of group members, and multicast data frames are forwarded based on their respective multicast address tables.

26.2 MLD Snooping Configuration

26.2.1 MLD Snooping Configuration Task List

The list of MLD Snooping configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable the MLD Snooping function	compulsory	26.2.2
Configuring MLD Snooping Member Port Aging Time	selectable	26.2.3
Configuring the Maximum Response Time for MLD Snooping Queries	selectable	26.2.4
Configuring the MLD Snooping Port Fast Leave Function	selectable	26.2.5
Configure a limit on the number of multicast groups learned by an MLD Snooping port	selectable	26.2.6
Configuring MLD Snooping Black and White Lists	selectable	26.2.7
Configuring the MLD Snooping Route Port Forwarding Function	selectable	26.2.8
Configuring the MLD Snooping Querier Switch	selectable	26.2.9
Configuring the MLD Snooping Querier Send Message Interval	selectable	26.2.10
Configuring the Maximum Response Time for MLD Snooping Generic Queries	selectable	26.2.11
Configuring MLD Snooping Route Port Aging	selectable	26.2.12
Add/Remove MLD Snooping Routing Ports	selectable	26.2.13
Configuring Multicast VLANs for MLD Snooping Ports	selectable	26.2.14
Display MLD Snooping configuration information	selectable	26.2.15
Display MLD Snooping Learned Multicast Table Entries	selectable	26.2.16

26.2.2 Enable/disable the MLD Snooping function

To control whether MLD Snooping establishes a mac address multicast forwarding table at Layer 2, you can use the following commands to enable/disable the MLD Snooping function.

manipulate	command	clarification
Go to System View	system-view	
Enabling mld-snooping	mld-snooping	By default, mld-snooping is disabled

Disable the mld-snooping function	undo mld-snooping	

[Example]

! Enabling MLD Snooping

[GPON] mld-snooping

26.2.3 Configuring MLD Snooping Member Port Aging Time

Configure the mld snooping member port aging time with the following command in system view.

manipulate	command	clarification
Go to System View	system-view	
Configure member port aging time	mld-snooping host-aging-time *seconds*	Member aging time configuration range is 10-1000000S, the default value is 300S
Restore the default member port aging time	undo mld-snooping host-aging-time	

[Example]

! Configure the aging time for dynamic multicast port members learned through mld snooping to 10 seconds

[GPON]mld-snooping host-aging-time 10

26.2.4 Configuring the Maximum Response Time for MLD Snooping Queries

The function of querying the maximum response time is to delete the maximum waiting time of a group member port when the device receives a leave message. the relevant configuration is as follows.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Maximum Response Time for Queries	mld-snooping max-response-time *seconds*	The maximum response time for query is configured from 1-100S, and the default value is 10S.
Restore default query maximum response time	undo mld-snooping max-response-time	

[Example]

! Configure the maximum response time for MLD Snooping to 15 seconds

[GPON]mld-snooping max-response-time 15

26.2.5 Configuring the MLD Snooping Port Fast Leave Function

Configure the fast leave function of a port. after a member port enables the fast leave function and receives a leave message, it will immediately age the group member port.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configuring the Port Fast Leave Function	mld-snooping fast-leave	Port defaults to disable Quick Leave

Disable port fast leave feature	undo mld-snooping fast-leave	

[Example]

! Enable fast leave on Ethernet port 1

[GPON-ethernet-0/0/1]mld-snooping fast-leave

26.2.6 Configuring MLD Snooping Port Learning Multicast Number Limits

After you configure the maximum number of multicast groups that a port is allowed to learn, and the system receives multicast group join messages that exceed the limit value, the system will no longer learn multicast groups that exceed the limit number and discard the messages that exceed the limit.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the port multicast learning number limit	mld-snooping group-limit *limit*	The limit value is configured in the range of 0-1023, and a configuration of not 0 indicates that no multicast groups are learned. The default value is the maximum value of 1023
Remove the limit on the number of ports for multicast learning	undo mld-snooping group-limit	

[Example]

! Configure the maximum number of multicast groups allowed to be learned on Ethernet port 1 to 10

[GPON-ethernet-0/0/1]mld-snooping group-limit 10

26.2.7 Configuring MLD Snooping Black and White Lists

Configure the black-and-white list of mld-snooping and the default group learning rule. after configuration. the system will confirm whether to learn a multicast group according to the learning rule.

Configure the multicast group learning mode in system view and the black-and-white list of mld-snooping in port view. after you configure the global multicast group learning mode, if no multicast join message matches the black-and-white list configured in port view, it will be controlled according to the global black-and-white list mode.

manipulate	command	clarification
Go to System View	system-view	
Configuring System Multicast Group Learning Mode	mld-snooping { permit | deny } group all	The system learns all multicast groups by default
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configure the port multicast learning number limit	mld-snooping { permit | deny } { group *group-address* vlan *vlan-id* | group-range *group-address* multi-count *count* vlan *vlan-id* }	When a single group is configured, it indicates black and white list control for a single multicast group. When group-range is configured, it

		indicates black and white list control for a group of multicast groups.
Remove the limit on the number of ports for multicast learning	undo mld-snooping group-limit	

[Example]

! Configure the system to learn all multicast groups by default

[GPON]mld-snooping permit group all

! Configure Ethernet port 1 not to learn group 01:00:5e:01:02:03 of VLAN 100

[GPON-ethernet-0/0/1]mld-snooping deny group 01:00:5e:01:02:03 vlan 100

! Configure Ethernet port 1 not to learn the 32 consecutive multicast MAC addresses starting with group 01:00:5e:01:02:03 for VLAN 100

[GPON-ethernet-0/0/1]mld-snooping deny group-range 01:00:5e:01:02:03 multi-count 32 vlan 100

26.2.8 Configuring the MLD Snooping Route Port Forwarding Function

The port in a device port that receives a multicast query message is called a multicast routing port.

Configure whether to automatically join the routed ports to the dynamic multicasts learned by MLD Snooping. not by default.

Perform the following configuration under system view.

manipulate	command	clarification
Go to System View	system-view	
Configuring Routed Port Forwarding	mld-snooping route-port forward	Route port forwarding is not enabled by default
Eliminate Route Port Forwarding	undo mld-snooping route-port forward	

[Example]

! Configure to auto-join routed ports to dynamic multicasts learned by MLD Snooping

[GPON]mld-snooping route-port forward

26.2.9 Configuring the MLD Snooping Querier Switch

To establish a multicast routing table, multicast routers maintain multicast table entries with multicast generic query messages sent proactively; the unit that sends the messages is called the querier.

The MLD Snooping protocol itself does not define the function of sending general query messages. you can configure the MLD Snooping querier to allow the device to send general query messages to achieve the maintenance of multicast table entries. the system does not enable the querier function by default. the relevant configurations are as follows.

manipulate	command	clarification
Go to System View	system-view	
Open the Finder	mld-snooping querier	Disable the querier function by default
Close Finder	undo mld-snooping querier	

[Example]

! will open the querier to send multicast generic query messages

[GPON] mld-snooping querier

26.2.10 Configuring the MLD Snooping Querier Send Message Interval

Configure the interval between sending multicast general query messages every two times for the querier, the default is 60s.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Querier Message Transmission Interval	mld-snooping query-interval *seconds*	The querier send message interval configuration range is 1-30000S, the default value is 60S
Restore the default querier message sending interval	undo mld-snooping query-interval	

[Example]

! Configure the querier to send generic query messages at an interval of 90 seconds

[GPON] mld-snooping query-interval 90

26.2.11 Configuring the Maximum Response Time for MLD Snooping Generic Queries

Configure the maximum response time of the host after receiving a generic query, that is, the value of the response field carried by the multicast generic query message sent by the querier, which is 10 seconds by default. if the host does not respond to the multicast answer message within the maximum response time, the member port will be deleted.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Maximum Response Time for Generic Queries	mld-snooping query-max-response *seconds*	Maximum response time configuration range is 1-25S, default value is 10S
Restore default generic query maximum response time	undo mld-snooping query-interval	

[Example]

! Configure the maximum response time of the host after a generic query to 15s

[GPON] mld-snooping query-max-respon 15

26.2.12 Configuring MLD Snooping Route Port Aging

The port of a device port that receives a multicast query message is called a multicast routing port. The system supports configuring whether a routing port is aging or not, and routing ports are aging-capable by default.

manipulate	command	clarification
Go to System View	system-view	
Configuring Routed Port Aging	mld-snooping router-port-age { on | off | *age-time* }	The aging time is configurable from 10 to 1000000, and the default value is 300S.
Cancel routed port aging	undo mld-snooping router-port-age	

[Example]

! Configure routed port aging to be on

[GPON]mld-snooping router-port-age on

! Configure the routing port to be removed (aged) after a period of time until the

[GPON]mld-snooping router-port-age 60

26.2.13 Add/Remove MLD Snooping Routing Ports

MLD Snooping routing port, the uplink port on which the device receives a multicast leave or report message from a host that needs to be forwarded, that is, the uplink routing port on which the host is configured to respond to the message.

manipulate	command	clarification
Go to System View	system-view	
Adding a Routing Port	mld-snooping route-port vlan *vlan-id* interface ethernet *interface-list*	
Deleting Routed Ports	undo mld-snooping route-port vlan *vlan-id* interface ethernet *interface-list*	

[Example]

! Configure Ethernet port 1 of vlan 100 as an MLD Snooping routing port

[GPON]mld-snooping route-port vlan 100 interface ethernet 0/0/1

26.2.14 Configuring Multicast VLANs for MLD Snooping Ports

This command is used to specify a vlan for a port. all multicast messages listened to through MLD Snooping are considered to be from this VLAN and the VLAN ID carried in the multicast message is ignored. this function can be applied to differentiate the user's unicast from multicast services as well.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring Multicast VLANs	mld-snooping multicast vlan *vlan-id*	
Deleting Routed Ports	undo mld-snooping multicast vlan	

[Example]

! Configure the multicast vlan for Ethernet port 1 to vlan 100

[GPON-ethernet-0/0/1]mld-snooping multicast vlan 100

26.2.15 Display MLD Snooping configuration information

You can view MLD Snooping related configuration information under any attempt. The displayed information includes aging time configuration, routing port configuration, multicast VLAN configuration, black and white list configuration, multicast learning limit configuration, and so on.

manipulate	command	clarification
View all MLD Snooping configuration information	display mld-snooping	
View multicast dynamic routing port aging information	display mld-snooping router-dynamic	
View multicast static route port aging information	display mld-snooping router-static	

[Example]

! Configuring MLD Snooping Configuration Information

[GPON]display mld-snooping

26.2.16 Displaying MLD Snooping Learned Multicast Table Entries

You can display the multicast table entries learned by MLD Snooping under any attempt.

manipulate	command	clarification
View all multicast table entries	display mld-snooping group	

[Example]

! Displays the multicast table entries learned by MLD Snooping

```
[GPON]display mld-snooping group
```

Chapter 27 Static Multicast Configuration

27.1 Introduction to Static Multicast

The static multicast configuration commands are used to create multicast groups and add member ports in multicast groups. If the device supports the multicast function, when the device receives a multicast service packet, it first detects whether this multicast group exists in the device, and if it does not exist, the device floods this multicast service packet within the VLAN. If this multicast group exists on the device, it forwards this multicast service message to all member ports of this multicast group.

27.2 Static Multicast Configuration

27.2.1 Static Multicast Configuration Task List

The list of static multicast configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Create/delete static multicast groups	compulsory	27.2.2
Add/remove static multicast group member ports	compulsory	27.2.3
Add/remove static multicast groups based on IP addresses	selectable	27.2.4
Display static multicast group configuration information	selectable	27.2.5

27.2.2 Create/delete static multicast groups

Creating/deleting multicast groups can be configured in system view using the following commands.

manipulate	command	clarification
Go to System View	system-view	
Adding a Static Multicast Group	multicast mac-address *mac-address* vlan *vlan-id*	
Delete static multicast group	undo multicast [mac-address *mac-address* vlan *vlan-id*]	When no multicast group address is specified, it means delete all multicast groups.

[Parameter Description]

mac-address: Indicates the mac address of the multicast group, which is required to be expressed in the form of multicast address, such as: 01:00:5e:**:**:**.

vlan-id: VLAN ID, the value range is 1 to 4094, the VLAN it belongs to must be an already existing VLAN, when the VLAN belonging to the added static multicast group does not exist, adding the multicast group fails.

[Example]

! Create 1 multicast group with mac address 01:00:5e:01:02:03, VLAN ID 100

```
[GPON]multicast mac-address 01:00:5e:01:02:03 vlan 100
```

27.2.3 Add/remove static multicast group member ports

Creating/deleting multicast groups can be configured in system view using the following commands.

manipulate	command	clarification
Go to System View	system-view	

Add static multicast group member ports	multicast mac-address *mac-address* vlan *vlan-id* interface { all | ethernet *interface-list* }	
Delete static multicast group member ports	undo multicast mac-address *mac-address* vlan *vlan-id* interface { all | ethernet *interface-list* }	

[Example]

! In the created multicast group 01:00:5e:01:02:03, add Ethernet ports 2,3,4,8

[GPON]multicast mac-address 01:00:5e:01:02:03 vlan 100 interface ethernet 0/0/2 to ethernet 0/0/4 ethernet 0/0/8

27.2.4 Add/remove static multicast groups based on IP addresses

Creating/deleting IP address-based static multicast groups can be configured in system view using the following commands.

manipulate	command	clarification
Go to System View	system-view	
Add static multicast groups based on IP addresses	multicast ip-address *ip-address* vlan *vlan-id*	
Delete static multicast groups based on IP addresses	undo multicast ip-address *ip-address* vlan *vlan-id*	
Add static multicast group member ports based on IP addresses	multicast ip-address *ip-address* vlan *vlan-id* interface { all | ethernet *interface-list* }	
Delete IP address-based static multicast group member ports	undo multicast ip-address *ip-address* vlan *vlan-id* interface { all | ethernet *interface-list* }	

[Example]

! Create a static multicast group based on IP address 224.1.1.1 and add member port 1

[GPON]multicast ip-address 224.1.1.1 vlan 100 interface ethernet 0/0/1

27.2.5 Display static multicast group configuration information

Static multicast group configuration information can be viewed under any attempt:

manipulate	command	clarification
Display static multicast group configuration information based on MAC address	display multicast mac-address *mac-address*	When no multicast group is specified, all multicast group information is displayed, and this command also includes displaying dynamically learned multicast group information.
Display IP address-based static multicast group configuration information	display multicast ip-address *ip-address*	

[Example]

! Display multicast group information with MAC address 01:00:5e:01:02:03

[GPON]display multicast mac-address 01:00:5e:01:02:03

Chapter 28 IGMP Configuration

28.1 Introduction to IGMP

IGMP defines the mechanism for establishing and maintaining multicast membership between hosts and devices, and is the basis for the entire IP multicast. Hosts join a multicast group by sending IGMP report messages. Multicast routers use IGMP to be informed of the existence of multicast group membership on the subnets connected to the router.

If a user on a LAN announces its membership in a multicast group through IGMP, the multicast router on the LAN propagates the information through the multicast routing protocol, and eventually joins the LAN into the multicast tree (a collection of paths for multicast message distribution) as a branch. After a host in a branch of the multicast tree starts sending and receiving multicast messages as a member of a multicast group, the multicast router connected to the branch will periodically query the multicast group to check whether there are still members of the multicast group in the branch. As long as there is still a host in the branch participating in sending and receiving multicast information, the multicast router continues to receive multicast data; when all users in a branch exit the multicast group, the branch is removed from the multicast tree.

Currently, the widely used IGMP protocols are Version 1 and Version 2, of which IGMP Version 2 specifies three message types: group member query messages, group member report messages, and group member leave messages.

Group member query message: according to different group addresses, it is divided into general group query message and specific group query message. The device understands what multicast members are on the network through the generic group query message, and the specific group query message is used to query the members of a specific multicast group, which can avoid the members belonging to other multicast groups from sending response messages.

Group membership report message: when a host receives a group membership query message for a generic group or a specific group, it transmits the group membership report message to the multicast-enabled device. After receiving the group membership report, the device adds the group members in the report to the group membership list of the network where the device is located. If the device does not receive any group membership report within a specific response time period, it knows that there is no local group membership and stops transmitting multicast data service messages to the network to which it is connected.

Group member leave message: when a host leaves a multicast group, IGMP will send a group member leave message to all multicast-enabled switches in the network.

IGMP is asymmetric between hosts and devices: hosts need to respond to IGMP query messages from devices (responding with membership report messages). The device needs to send a generic group query message at regular intervals and, based on the response received, determine whether any hosts on its subnet have joined a particular multicast group.

28.2 IGMP Configuration

28.2.1 IGMP Configuration Task List

To configure the IGMP protocol, you must enable multicast routing before you can configure the individual features of the IGMP protocol.

The list of IGMP configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable Multicast Protocol	compulsory	28.2.2
Specifies that the interface is running the IGMP protocol	compulsory	28.2.3
Configure the version number of the interface running IGMP	selectable	28.2.4
Configure the time interval for sending generic query messages	selectable	28.2.5

Configure the interval for sending last member queries	selectable	28.2.6
Configuring robustness variables	selectable	28.2.7
Configure the interface to limit the number of multicast groups that can be joined	selectable	28.2.8
Configuring IGMP Maximum Query Response Time	selectable	28.2.9
Configuring Interface Access Control Lists	selectable	28.2.10
Configure static IP multicast table entries	selectable	28.2.11
Configure a port to statically join a multicast group	selectable	28.2.12
Configuring the IGMP-Proxy Function	selectable	28.2.13
Configuring the SSM-Mapping Function	selectable	28.2.14
Enter IGMP view	selectable	28.2.15
Configuring SSM-Mapping Static Group Address Mapping Rules	selectable	28.2.16
IGMP Monitoring and Maintenance	selectable	28.2.17

▪

28.2.2 Enable Multicast Protocol

Other multicast-related configurations can take effect only if the multicast protocol is enabled.

manipulate	command	clarification
Go to System View	system-view	
Enable Multicast Protocol	ip multicast-routing	By default, the system disables multicast protocols
Blocking Multicast Protocols	undo ip multicast-routing	

[Example]

! Enable Multicast Protocol

[GPON] ip multicast-routing

28.2.3 Specifies that the interface is running the IGMP protocol

Start the IGMP protocol on the interface to enable the device to send multicast messages.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Enable IGMP protocol	ip igmp	By default, the igmp protocol is disabled
Disable IGMP protocol	undo ip igmp	

[Example]

! Enable the IGMP protocol for VLAN interface 100

[GPON-vlanInterface-100]ip igmp

 Attention:

Before a VLAN interface can enable IGMP, it must globally enable the multicast protocol. The following commands for interface attribute configuration are subject to this restriction.

28.2.4 Configure the version number of the interface running IGMP

All systems on the same subnet should support the same IGMP version, but the device cannot automatically detect the IGMP version number that the interface is currently running.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configure the IGMP protocol version number	ip igmp version { 1 | 2 | 3 }	By default, version 2 is running
Restore the default IGMP protocol version number	undo ip igmp version	

[Example]

! Configure the IGMP protocol version number of VLAN interface 100 to version 2

[GPON-vlanInterface-100] ip igmp version 2

28.2.5 Configure the time interval for sending generic query messages

The device needs to periodically send Membership Query Message to the network it is connected to, and this interval is set by the Query Interval timer. Users can configure the Query Interval timer to modify the time interval for IGMP hosts to send query messages.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configuring the Generic Query Message Transmission Interval	ip igmp query-interval *seconds*	The time interval configuration range is 15-30000S, and the default interval is 125S.
Restore the default universal query message sending interval	undo ip igmp query-interval	

[Example]

! Configure the IGMP general query message sending interval for VLAN interface 100 to be 200 seconds

[GPON-vlanInterface-100]ip igmpquery-interval 200

28.2.6 Configure the interval for sending last member queries

After the device receives the leave message as a querier, it sends a group-specific query message in order to know whether there are still group members in the multicast group more quickly, and the user can configure this value to modify the interval for the device to send the group-specific query message.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface{ vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configure the last member query message sending interval	ip igmp last-member-query-interval *seconds*	The time interval configuration range is 1-25S, and the default interval is 1S.

Restore the default last member query message sending interval	undo ip igmp last-member-query-interval	

[Example]

! Configure the IGMP last member query message sending interval for VLAN interface 100 to be 2 seconds

[GPON-vlanInterface-100]ip igmp last-member-query-interval 2

 Attention:

IGMP Version V1 does not support the leave and last member query function, and this configuration takes effect only when the interface is running Version V2/V3.

28.2.7 Configuring robustness variables

The robustness variable is an important parameter that reflects the performance of the device running the IGMP protocol. It is mainly used to control the number of times the last-member query message is sent to prevent the message from being lost in the network and to enhance the robustness of the operation of the network protocol.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface{ vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configuring robustness variables	ip igmp robustness-variable *value*	The robustness variable is configured in the range 2-7, with a default interval of 2
Restore default robustness variables	undo ip igmp robustness-variable	

[Example]

! Configure the robustness variable for VLAN interface 100 to 3

[GPON-vlanInterface-100] ip igmp robustness-variable 3

28.2.8 Configure the interface to limit the number of multicast groups that can be joined

This function is used to limit the number of IGMP multicast groups joined on an interface, and the device will not process IGMP join messages after the limit is exceeded. By default, the number of IGMP groups joined on an interface is the maximum number of multicast groups supported by the system. During user configuration, if the number of IGMP groups joined on the interface has exceeded the configured value, the previously joined IGMP groups will not be deleted.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configure to limit the number of multicast groups joined	ip igmp limit-group *limit-num*	The number of multicast groups is configured in the range of 0-64, and the default value is 64; a configuration of 0 means that no multicast group is learned
Restore the default limit on the	undo ip igmp limit-group	

number of multicast groups that can be joined		

[Example]

! Configure VLAN interface 100 to limit the number of multicast groups joined to 10

[GPON-vlanInterface-100]ip igmp limit-group 10

28.2.9 Configuring IGMP Maximum Query Response Time

When a host receives a periodic query message from the device, it starts a Delay Timers for each multicast group it joins, using a random number between (0, Max Response Time] as the initial value, where Max Response Time is the maximum response time specified in the query message (IGMP Version 1's maximum query response time is fixed at 10 seconds). The host should inform the device of the multicast group membership before the timer times out. If the device does not receive any group membership report after the Max Query Response Time timeout, it assumes that there is no more local group membership, and it no longer transmits the multicast messages it receives to the network to which it is connected.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configuring the Maximum Query Response Time	ip igmp query-max-response-time *seconds*	Maximum query response time configuration range is 1-3000S, the default value is 10S
Restore the default maximum query response time	undo ip igmp query-max-response-time	

[Example]

! Configure the maximum query response time for VLAN interface 100 to 20S

[GPON-vlanInterface-100]ip igmp query-max-response-time 20

Attention:

The maximum query response time for IGMP Version V1 is fixed at 10 seconds. This configuration takes effect only when the interface is running Version V2/V3.

28.2.10 Configuring Interface Access Control Lists

The multicast protocol identifies multicast groups and multicast group members by sending IGMP query messages. The device can configure an ACL on an interface to enable a host to join a multicast group for a specified IP as required by the configuration.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface{ vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configuring Interface Access Control Lists	ip igmp access-group *acl-number* [all | ethernet *interface-list*]	You need to configure an ACL first to specify the multicast table entries that are allowed or prohibited to be learned. the host can join any multicast group by default.

Deleting an Interface Access Control List	undo ip igmp access-group *acl-number* [all | ethernet *interface-list*]	

[Example]

! Configure VLAN interface 100 so that hosts can only join to the multicast groups 224.1.1.1, 224.1.2

[GPON] acl 4 deny 224.1.1.0 0.0.0.255

[GPON] acl 4 permit 224.1.1.1 0.0.0.0

[GPON] acl 4 permit 224.1.1.2 0.0.0.0

[GPON-vlanInterface-100] ip igmp access-group 4 all

28.2.11 Configure static IP multicast table entries

In addition to dynamically learning multicast table entries through IGMP messages, the system also supports the creation of static IP multicast table entries to realize the forwarding of multicast messages.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	Interface vlan-interface *vlan-id*	Normal VLAN interfaces differ from Supervlan interface configuration commands in that sub-VLANs are required to be specified under Supervlan interfaces
Configure static IP multicast table entries	ip igmp create-group *groups-address-list* source { * | *source-address* }	groups-address-list represents statically created IP multicast table entries, and can support to form configuration to create multiple consecutive static multicast table entries at a time. source-address indicates the multicast source IP address, the * sign indicates that the source IP address is not concerned, match any source IP address can be
Delete static IP multicast table entries	undo ip igmp create-group *groups-address-list* source { * | *source-address* }	
Enter VLAN interface view	interfacesupervlan-interface *vlan-id*	Sub-VLANs need to be specified under the Supervlan interface.
Configure static IP multicast table entries	ip igmp create-group groups-address-list source { * | source-address } vlan vlan-id	Vlan indicates a sub-VLAN of Supervlan
Delete static IP multicast table entries	undo ip igmp create-group *groups-address-list* source { * | *source-address* } vlan *vlan-id*	

[Example]

! Configure VLAN interface 100 to create static multicast table entries 224.1.1.1-224.1.10, with source IP addresses of *

[GPON-vlanInterface-100] ip igmp create-group 224.1.1.1 to 224.1.1.10 source *

28.2.12 Configure a port to statically join a multicast group

Configuring a device port to be a static multicast group member port enables the device to forward multicast data service packets to this port, and at the same time you can specify the source address list.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configuring Static Multicast Group Membership	ip igmp static-group { * | *groups-address* } { all | ethernet *interface-list* } sourcelist { * | *sourcelist* }	
Delete static multicast group members	undo ip igmp static-group { all | *groups-address* { all | ethernet *interface-list* } sourcelist { * | *sourcelist* } }	

[Example]

! Configure VLAN interface 100, host 192.168.1.100 to statically join multicast group 224.1.1.1

[GPON-vlanInterface-100] ip igmp static-group 224.1.1.1 all sourcelist 192.168.1.100

28.2.13 Configuring the IGMP-Proxy Function

After you enable the IGMP-Proxy proxy function of the device, the device is equivalent to a host, which reports the multicast information collected from the downstream member ports to the upstream multicast router through the IGMP proxy interface, so that the upstream multicast router forwards the corresponding multicast service data traffic to the device, and the device then forwards to the user according to these messages. When the device is placed at the edge of the network and only one interface is connected to the multicast router, you can enable the IGMP-Proxy proxy function on this interface for multicast service message forwarding, and at this time the device does not need to use the multicast routing protocol.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Enabling IGMP-Proxy	igmp-proxy	
Disable the IGMP-Proxy function	undo igmp-proxy	

[Example]

! Configure VLAN interface 100 to enable the IGMP-Proxy feature

[GPON-vlanInterface-100] igmp-proxy

28.2.14 Configuring the SSM-Mapping Function

SSM requires that on the user host segment, the router be able to know the specific multicast source that was specified when the host joined the group. If IGMPv3 is running between the user host and the router, specify the source address in the Report message for IGMPv3. If there are certain hosts in the network segment that can only run IGMPv1 or IGMPv2, the source address cannot be specified in the Report message. In this case, you need to configure the SSM Mapping function and static mapping rules on the router to map the (*, G) information contained in the Report message to (G, INCLUDE, (S1, S2...)) information.

In SSM networks, due to various possible limitations, some receiver hosts can only run IGMPv1 or IGMPv2. Therefore, in order to provide SSM services to these receiver hosts that only support IGMPv1 or IGMPv2, you can configure the IGMP SSM Mapping feature on the switch.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Turn on ssm-mapping	ip igmp ssm-mapping	By default, the SSM-Mapping feature is turned off
Turn off the ssm-mapping feature	undo ip igmp ssm-mapping	

[Example]

! Turn on ssm-mapping on VLAN interface 100

[GPON-vlanInterface-100] ip igmp ssm-mapping

28.2.15 Enter IGMP view

Configuring global parameters related to IGMP requires entering IGMP view.

manipulate	command	clarification
Go to System View	system-view	
Enter IGMP view	mroute igmp	
Exit IGMP view	quit	

28.2.16 Configuring SSM-Mapping Static Group Address Mapping Rules

The configuration enables the mapping of the same multicast group to multiple multicast source IPs within the specified SSM multicast group range.

Please configure it in IGMP view.

manipulate	command	clarification
Go to System View	system-view	
Enter IGMP view	mroute igmp	
Configuring ssm-mapping mapping rules	ssm-mapping ipaddress mask multicast-source-ipaddress	Ipaddress/ Mask is the multicast group address multicast-source-ipaddress is the multicast source IP address
Remove the ssm-mapping mapping rule	undo ssm-mapping { *ipaddress mask* | all }	

[Example]

! Configure 224.1.1.1 to map multicast source address 192.168.1.100

[GPON-router-igmp]ssm-mapping 224.1.1.1 32 192.168.1.100

28.2.17 IGMP Monitoring and Maintenance

IGMP configuration and operational information can be viewed at any attempt.

manipulate	command	clarification
Display information about interfaces running IGMP	display ip igmp interface [{ vlan-interface *vlan-id* } | { supervlan-interface *vlan-id* }]	If you do not specify a vlan interface, you can view igmp configuration information for all interfaces.
Displays statically configured and IGMP dynamically learned multicast group information	display ip igmp groups [*multicast-ip*]	When multicast IP is not specified, it means view all multicast group information
Displaying IGMP Proxy Information	display igmp-proxy	
Display SSM-Mapping Mapping Rules	display ip igmp ssm-mapping [*multicast-ip*]	When multicast IP is not specified, it means view all multicast group mapping rules

[Example]

! Display IGMP configuration information for VLAN interface 100

[GPON] display ip igmp interface vlan-interface 100

Chapter 29 PIM Configuration

29.1 Introduction to the PIM protocol

PIM is the abbreviation of Protocol Independent Multicast (PIM), which means that you can use static routes or unicast routing protocols (including RIP, OSPF, IS-IS, BGP, and so on) to generate a unicast routing table to provide routes for IP multicast. Multicast routing has nothing to do with the unicast routing protocols used, as long as the corresponding multicast routing table entries can be generated by unicast routing protocols.PIM forwards multicast messages with the help of the RPF (Reverse Path Forwarding) mechanism. When a multicast message arrives at the local device, it is first checked by RPF:

If the RPF check passes, the corresponding multicast routing table entries are created so that multicast messages can be forwarded; if the RPF check fails, the message is discarded.

Depending on the realization mechanism, PIM is divided into the following two modes:

PIM-DM (Protocol Independent Multicast-Dense Mode)

PIM-SM (Protocol Independent Multicast-Sparse Mode)

29.1.1 How PIM-DM works

PIM-DM is a dense-mode multicast routing protocol that uses "push mode" to transmit multicast data, and is usually suitable for small networks with relatively dense multicast group membership.

The basic principle of PIM-DM is as follows:

1, PIM-DM assumes that at least one multicast group member exists in every subnet in the network, so multicast data will be spread (Flooding) to all nodes in the network. Then, PIM-DM prunes the branches that do not have multicast data to forward, keeping only the branches that contain receivers. This "Spread-Prune" phenomenon occurs periodically, and the pruned branches can be periodically restored to the forwarding state.

2. When a member of a multicast group appears on the node of the pruned branch, in order to reduce the time required for the node to return to the forwarding state, PIM-DM uses the Graft mechanism to actively restore its forwarding of multicast data. Generally speaking, the forwarding path of packets in dense mode is a Source Tree, i.e., a forwarding tree with the multicast source as the "root" and the multicast group members as the "branches and leaves". Since the Source Tree uses the shortest path from the multicast source to the receiver, it is also called the Shortest Path Tree (SPT).

The working process of PIM-DM can be summarized as follows: neighbor discovery, diffusion-pruning process, and grafting phase.

(1) Neighbor Discovery In a PIM domain, a router constructs and maintains SPTs by periodically sending PIM Hello messages (hereafter referred to as Hello messages) in multicast mode to all PIM routers (224.0.0.13) to discover PIM neighbors and maintain PIM neighbor relationships among the routers.

(2) Diffusion-pruning process (construction of SPT tree)

PIM-DM Assume that all hosts on the network are ready to receive multicast data. When a multicast source S starts to send data to a multicast group G, the router receives the multicast packet and first performs an RPF check based on the unicast routing table; if the check passes, the router creates an (S, G) table entry, and then forwards (Floods) the data to all downstream PIM-DM nodes on the network. If it does not pass the RPF check, i.e., the multicast message is input from the wrong interface, the message is dropped. After this process, a (S, G) table entry is created throughout the PIM-DM multicast domain. If the downstream node has no multicast group membership, a prune (Prune) message is sent to the upstream node to inform the upstream node that it does not have to forward data to the downstream node. When the upstream node receives the prune message, it removes the corresponding interface from the list of output interfaces corresponding to its multicast forwarding table entries (S, G), thus creating an SPT (Shortest Path Tree) tree with the source S as the root. The pruning process is first initiated by the leaf routers. This process is called diffusion-pruning process. Each pruned node provides a timeout mechanism at the same time, and when the pruning timeout occurs, each router restarts the diffusion-pruning process again.The diffusion-pruning mechanism of PIM-DM periodically keeps on going.

In this process, PIM-DM uses RPF inspection to construct a multicast forwarding tree originating from the data source using the existing unicast routing table. When a multicast packet arrives, the router first determines the correctness of the arrival path. If the arriving interface is the interface to the multicast source indicated by the unicast route, the multicast packet is considered to have come from the correct path; otherwise, the multicast packet will be discarded as a redundant message and will not be multicast forwarded. The unicast routing information used as the basis for path determination can be derived from any unicast routing protocol, such as the routing information discovered by RIP and OSPF, and does not depend on a specific unicast routing protocol.

(3) Assert mechanism (assertion)

As shown in the following figure, if two multicast routers A and B on a LAN segment have their own reception paths to the multicast source S, they will forward the multicast data packet to the LAN after receiving the multicast data packet from the multicast source S. The multicast router C at the downstream node will receive two copies of the same multicast packet. When the multicast packet router forwarded by the upstream node detects this situation, it needs to select a unique forwarder through the Assert mechanism. If two or more paths have the same priority and metric, the one with the largest IP address is selected as the upstream neighbor of the (S,G) item, and it is responsible for forwarding the (S,G) multicast packet.

(4) Graft

When a pruned downstream node needs to be restored to the forwarding state, the node uses a graft message to notify the upstream node. To configure the IGMP protocol, you must enable the multicast routing function before you can configure the individual features of the IGMP protocol.

(5) State Refreshment Mechanism (SRM)

To avoid repeated diffusion-pruning, the new protocol standard adds this mechanism, where a router directly connected to the multicast source sends a state refresh message at regular intervals, and the PIM receives this message and refreshes the pruning state.

29.1.2 How PIM-SM works

PIM-DM uses SPTs constructed in a "spread-and-prune" fashion to transport multicast data. Although SPTs have the shortest paths, they are built inefficiently and are not suitable for medium to large networks.

PIM-SM belongs to the sparse mode multicast routing protocol, using the "pull" mode to transmit multicast data, usually applicable to multicast group members are relatively decentralized, wide range of medium and large networks.

The basic principle of PIM-SM is as follows:

1, PIM-SM assumes that all hosts do not need to receive multicast data, and only forward it to hosts that explicitly request multicast data.The core task of PIM-SM to realize multicast forwarding is to construct and maintain the RPT (Rendezvous Point Tree, Shared Tree or Sinking Tree), the RPT selects a certain router in the PIM domain as the common root node RP (Rendezvous Point) in the PIM domain, and multicast data is forwarded to receivers along the RPT through the RP;

2. The router connecting to the receiver sends a Join Message to the RP corresponding to a multicast group, which is delivered hop by hop to the RP, and the path it passes through forms a branch of the RPT;

If a multicast source wants to send multicast data to a multicast group, first the DR (Designated Router) is responsible for registering with the RP, and sends the registration message to the RP through unicast, which triggers the establishment of the SPT when it arrives at the RP, and then the multicast source sends the multicast data along the SPT to the RP. After that, the multicast source sends the multicast data along the SPT to the RP, and when the multicast data reaches the RP, it is copied and sent to the receiver along the RPT.

The working process of PIM-SM can be summarized as follows: neighbor discovery, DR election, RP discovery, construction of RP shared tree (RPT), multicast source registration, RPT to SPT switching, and assertion.

(1) Neighborhood discovery

PIM-SM uses a similar neighbor discovery mechanism as PIM-DM, see the "Neighbor Discovery" section for details.

(2) DR elections

With the help of Hello messages it is also possible to elect a DR for a shared network (e.g., Ethernet), which will act as the sole forwarder of multicast data in that shared network. Both the network connected to the multicast source and the network connected to the receiver need to elect DRs. the DR on the receiver side is responsible for sending join messages to the RP; the DR on the multicast source side is responsible for sending registration messages to the RP.

The election process for the DR is as follows:

1) Each router on the shared network sends Hello messages to each other (carrying parameters for campaign DR priority), and the router with the highest priority will become the DR;

2) If the priority is the same, or at least one router in the network does not support the parameter of campaigning for the DR priority in the Hello message, the campaign for the DR will be based on the size of the IP address of each router, and the router with the largest IP address will become the DR;

3) When the DR fails and the remaining routers do not receive a Hello message from the DR after a timeout, a new DR election process is triggered.

(3) RP Discovery

The RP is the core device in the PIM-SM domain. In a small network with a simple structure, the amount of multicast information is small, and the whole network relies on only one RP for the forwarding of multicast information, and at this time, the location of the RP can be statically specified on each router in the PIM-SM domain; however, in more cases, the PIM-SM domains are very large, and the amount of multicast information forwarded through the RP is huge. In order to alleviate the burden of RPs and optimize the topology of RPTs, you can configure multiple C-RPs (Candidate-RP, Candidate RP) in the PIM-SM domain, and dynamically elect the RPs through the bootstrap mechanism, so that different RPs serve different multicast groups, and at this time, you need to configure the BSR (BootStrap Router).The BSR is the management core of the PIM The BSR is the management core of a PIM-SM domain. There can be only one BSR in a PIM-SM domain, but multiple C-BSRs (Candidate-BSR, Candidate BSR) can be configured. In this way, in the event of a BSR failure, the remaining C-BSRs are able to manage the PIM-SM domain by self

The BSR is responsible for collecting the Advertisement Message from the C-RP in the network, which carries the address and priority of the C-RP as well as the range of groups it serves, and the BSR summarizes this information into an RP-Set (RP set, i.e., the mapping between multicast groups and RPs) and publishes it to the entire PIM-SM domain. The BSR summarizes this information into an RP-Set (RP set, i.e., a database of mapping relationships between multicast groups and RPs), encapsulates it in a Bootstrap Message, and publishes it throughout the PIM-SM domain. Each router in the network will use the same rules to select the corresponding RP for a specific multicast group from a large number of C-RPs based on the information provided by the RP-Set, as follows:

1) First compare the priority of C-RPs, the higher priority wins;

2) If the priority is the same, the hash value is calculated using the hash (Hash) function and the larger value wins;

3) If both priority and hash are equal, the larger C-RP address wins.

(4) Construct RP Shared Tree (RPT)

The RPT is constructed as follows:

1) When a receiver joins a multicast group G, it first notifies the DR directly connected to it via an IGMP message;

2) After the DR has information about the receivers of multicast group G, it sends a join message hop-by-hop in the direction of the RP corresponding to that group;

3) The routers passing from DR to RP form branches of the RPT, and these routers have generated (*, G) table entries in their forwarding tables, where "*" means from any multicast source. the RPT has RP as its root and DR as its leaf. When multicast data destined for multicast group G flows through the RP, the data reaches the DR along the established RPT and then reaches the receiver. When a receiver is no longer interested in the information of multicast group G, the DR directly connected to it sends a pruning message hop-by-hop against the RPT in the direction of the RP of the group; the upstream node receives the message and deletes the interface connected to the downstream node from its list of outgoing interfaces, and checks whether it owns the receivers of the multicast group, and if it does not, it continues to forward the pruning

message upstream of the upstream of the upstream of the upstream of the upstream of the upstream of the upstream of the upstream of the upstream of the upstream of the upstream of the upstream of the upstream.

(5) Multicast Source Registration

The process of registering a multicast source with an RP is as follows:

1) When a multicast source S sends a multicast message to a multicast group G, the DR that is directly connected to the multicast source encapsulates the message as a registration message when it receives it and sends it to the corresponding RP through unicast;

2) When the RP receives the message, it decapsulates the registration message and forwards the multicast message encapsulated in it to the receiver along the RPT on the one hand, and sends the (S, G) join message to the multicast source hop by hop on the other hand. In this way, the routers passing from the RP to the multicast source form branches of the SPT, and these routers all generate (S, G) table entries in their forwarding tables.The SPT takes the multicast source as its root and the RP as its leaf;

3) The multicast data from the multicast source arrives at the RP along the established SPT, and then the RP forwards the multicast data along the RPT to the receiver. When the RP receives the multicast data forwarded along the SPT, it sends a Register-Stop Message to the DR that is directly connected to the multicast source in unicast mode, and the process of registering the multicast source ends.

(6) RPT to SPT switchover

When the DR on the receiver side finds that the multicast data rate sent from the RP to the multicast group G exceeds a certain threshold, it will initiate the switchover from the RPT to the SPT as follows:

1) First, the receiver-side DR sends a hop-by-hop (S, G) join packet to the multicast source S and eventually delivers it to the multicast source-side DR, and all routers passing along the way generate (S, G) table entries in their forwarding tables, thus establishing the SPT branch;

2) Subsequently, the DR on the receiver side sends a pruning message containing the RP bits to the RP hop by hop, and the RP will continue to send pruning messages in the direction of the multicast source after receiving the message (assuming that there is only this one receiver at this time), so as to ultimately realize the switching from the RPT to the SPT. After switching from RPT to SPT, multicast data will be sent directly from the multicast source to the receiver. By switching from RPT to SPT, PIM-SM is able to establish SPT in a more economical way than PIM-DM.

(7) Assert mechanism (assertion)

PIM-SM uses a similar assertion mechanism as PIM-DM, see PIM-DM "Assertions".

29.1.3 How PIM-SSM works

According to the protocol standard, SSM usually relies on the PIM-SM implementation, which can coexist with PIM-SM in the same router, and decides whether to use SSM or PIM-SM based on the multicast addresses in the data and protocol messages.IANA assigns the SSM the address segment 232.0.0.0-232.255.255.255.255, and the multicast groups in this address segment will not be added to the shared tree , but are instead handled by the SSM. the SSM also needs to implement neighbor discovery and DR election between devices by sending periodic HELLO messages.

On the host side of the router, this is typically accomplished through IGMPv3, which adds source filtering compared to IGMPv2, allowing hosts to specify the data they need to receive from a particular group, and also to specify that they want to receive data from a particular source within that group. When the SSM receives an IS_IN message from IGMPv3 and learns that a host on the network connected to the interface receiving the IGMP message wants to receive datagrams destined for multicast group G from source S, it sends a PIM (S,G) source group join message hop-by-hop toward the source to the first-hop router connecting to the multicast source according to the unicast routing, thus establishing a shortest path tree between the multicast source and the last-hop router connecting to the receiver. thus establishing a shortest-path tree between the multicast source and the last-hop router connecting the receiver. When a multicast source

sends multicast data, the data travels along the shortest path tree to the receiver. For hosts that only support IGMPv1/IGMPv2 and do not support IGMPv3, you can configure ssm-mapping on the router to which they are connected, and the group join messages sent by IGMPv1/IGMPv2 are mapped as source group joins, so that you can apply SSM in the group network.

29.2 PIM Configuration

29.2.1 PIM Configuration Task List

Configuring PIM requires the following actions to be performed in sequence. it is recommended that PIM-DM be started on all interfaces of a non-border router when the router is operating in the PIM-DM protocol domain. and PIM-SM eliminates the need for PIM-SM to run on every interface. a list of the configuration tasks for PIM is shown below.

Configuration tasks	clarification	Detailed Configuration
Enable Multicast Protocol	compulsory	29.2.2
Specifies that the interface runs the PIM-DM protocol	compulsory	29.2.3
Specifies that the interface runs the PIM-SM protocol	compulsory	29.2.4
Configure the PIM protocol Hello message sending interval	selectable	29.2.5
Setting BSR domain boundaries	selectable	29.2.6
Enter the PIM view	selectable	29.2.7
Configuring Multicast Source Filtering	selectable	29.2.8
Configuring PIM Neighbor Filtering	selectable	29.2.9
Configure the maximum number of PIM neighbors for an interface	selectable	29.2.10
Configuring Static RP	selectable	29.2.11
Specify the candidate BSR	selectable	29.2.12
Specify the candidate RP	selectable	29.2.13
Configuring the SPT switching threshold	selectable	29.2.14
Configuring SSM Multicast Group Scope	selectable	29.2.15
PIM Monitoring and Maintenance	selectable	29.2.16

▪

29.2.2 Enable Multicast Protocol

Other multicast-related configurations can take effect only if the multicast protocol is enabled.

manipulate	command	clarification
Go to System View	system-view	
Enable Multicast Protocol	ip multicast-routing	By default, the system disables multicast protocols
Blocking Multicast Protocols	undo ip multicast-routing	

[Example]

! Enable Multicast Protocol

[GPON] ip multicast-routing

29.2.3 Specifies that the interface runs the PIM-DM protocol

The PIM-DM protocol needs to be started on each interface separately. After PIM-DM is configured on an interface, PIM-DM periodically sends PIM protocol Hello messages and processes protocol messages sent by PIM neighbors.

manipulate	command	clarification

Go to System View	system-view	
Enter VLAN interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Enable PIM-DM protocol	ip pim dense-mode	By default, the PIM-DM protocol is disabled
Disable the PIM-DM protocol	undo ip pim dense-mode	

[Example]

! Enable the PIM-DM protocol for VLAN interface 100

[GPON-vlanInterface-100]ip pim dense-mode

 Attention:

- Before a VLAN interface can enable IGMP, it must globally enable the multicast protocol. The following commands for interface attribute configuration are subject to this restriction.
- After starting the PIM-DM protocol on an interface, you cannot start the PIM-SM protocol on this interface and vice versa.

29.2.4 Specifies that the interface runs the PIM-SM protocol

The PIM-SM protocol needs to be started on each interface separately. After PIM-SM is configured on an interface, PIM-SM periodically sends PIM protocol Hello messages and processes protocol messages sent by PIM neighbors.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Enable PIM-SM protocol	ip pim sparse-mode	By default, the PIM-SM protocol is disabled
Disable the PIM-SM protocol	undo ip pim sparse-mode	

[Example]

! Enable the PIM-SM protocol for VLAN interface 100

[GPON-vlanInterface-100]ip pim sparse -mode

29.2.5 Configure the PIM protocol Hello message sending interval

After the interface starts the PIM protocol, it sends Hello messages periodically. The interval between Hello messages can be modified depending on the bandwidth and type of network connected to the interface.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configure the PIM protocol Hello	ip pim query-interval *seconds*	Transmit interval configuration range is 1-

message sending interval		65535S, the default value is 30S
Restore the default PIM protocol Hello message sending interval	undo ip pim query-interval	

[Example]

! Configure the PIM-DM protocol Hello message sending interval for VLAN interface 100 to 60 seconds

[GPON-vlanInterface-100] ip pim query-interval 60

 Attention:

Before configuring the PIM attributes of an interface, you must first enable the interface to run the PIM protocol. the following configuration interface attributes are all the same.

29.2.6 Configuring BSR Boundaries

Configure the interfaces of the device as BSR domain boundaries for PIM. When this command is configured on an interface to set the PIM domain boundary, all Bootstrap Messages cannot traverse the domain boundary, but other PIM messages can pass through the domain boundary. By this method, users can effectively partition the network running PIM-SM into multiple domains, with a different Bootstrap Router on each domain. Please note: This command does not establish a multicast boundary; it only establishes a PIM bootstrap message boundary.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configuring BSR Boundaries	ip pim bsr-border	By default interfaces are not BSR boundaries
Delete the BSR boundary configuration	undo ip pim bsr-border	

[Example]

! Configure VLAN interface 100 as a BSR boundary

[GPON-vlanInterface-100] ip pim bsr-border

29.2.7 Enter the PIM view

Configuring global parameters related to PIM requires entering PIM view.

manipulate	command	clarification
Go to System View	system-view	
Enter the PIM view	mroute pim	
Exiting the PIM View	quit	

29.2.8 Configuring Multicast Source Filtering

You can filter multicast packets based on the source address encapsulated in the multicast packet to improve the security of the network. please configure it in PIM mode.

manipulate	command	clarification

Go to System View	system-view	
Enter the PIM view	mroute pim	
Configuring Multicast Source Filtering	source-policy *acl-number*	You need to configure an ACL first, specifying the IP address of the multicast source to be filtered; by default, no multicast source is filtered
Remove multicast source filtering	undo source-policy	

[Example]

! Configure multicast source filtering to only allow multicast sources from 192.168.1.100 to be forwarded

[GPON] acl 4 denyany

[GPON] acl 4 permit 192.168.1.100 0.0.0.0

[GPON-router-pim] source-policy 4

29.2.9 Configuring PIM Neighbor Filtering

You can configure a basic access control list to restrict only the routers that pass the filter to be the PIM neighbors of the current interface. please configure it under the VLAN or Supervlan interface.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configuring PIM Neighbor Filtering	ip pim neighbor-policy *acl-number*	By default, no filtering is performed on neighbors under PIM interfaces
Remove PIM Neighbor Filtering	undo ip pim neighbor-policy	

[Example]

! Configure VLAN interface 100 to filter PIM neighbor 192.168.1.200

[GPON] acl 4 deny192.168.1.200 0.0.0.0

[GPON-vlanInterface-100] ip pim neighbor-policy 4

29.2.10 Configure the maximum number of PIM neighbors for an interface

In order to prevent the router memory from being exhausted after establishing a large number of PIM neighbor relationships, which will lead to router failure, the number of PIM neighbors on the router interface can be limited. And the limitation of the total number of router PIM neighbors is defined internally by the system and cannot be changed by the user through commands, please configure it under the VLAN or Supervlan interface.

manipulate	command	clarification
Go to System View	system-view	
Enter VLAN interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	Normal VLAN interfaces or Supervlan interfaces can be specified.
Configure the maximum number of PIM neighbors	ip pim neighbor-limit *limit-num*	The maximum number of PIM neighbors is configured in the range of 0-128, and the default configuration is 128
Restore the default maximum	undo ip pim neighbor-limit	

number of PIM neighbors		

[Example]

! Configure VLAN interface 100 with a PIM neighbor count of 60

[GPON-vlanInterface-100] ip pim neighbor-limit 60

 Attention:

If the number of PIM neighbors on the interface has exceeded the configured value at the time of user configuration, the original PIM neighbors will not be deleted.

29.2.11 Configuring Static RP

Static RPs can be used as backups for dynamic RPs to improve the robustness of the network. configure it in PIM mode.

manipulate	command	clarification
Go to System View	system-view	
Enter the PIM view	mroute pim	
Configuring Static RP	static-rp ip-address	By default, PIM does not configure static RPs
Delete Static RP	undo static-rp	

If you use static RP, all routers in the PIM domain must have the same configuration. If the configured static RP address is the address of an interface whose state is UP on the local machine, the local machine acts as a static RP. the interface that acts as a static RP does not have to be enabled for the PIM protocol. The static RP does not function when the RP elected by the BSR mechanism is valid. The static RP is used when the acquisition of the dynamic RP fails.

[Example]

! Configure static RP 192.168.1.100

[GPON-router-pim] static-rp 192.168.1.100

29.2.12 Configuring candidate BSRs

In a PIM-SM domain, a unique BSR (Bootstrap Router) must exist to ensure that PIM-SM-enabled network devices (e.g., routers, Ethernet switches, etc.) function properly.The BSR is responsible for collecting and distributing RP information. Multiple C-BSRs elect the only recognized BSR through a self-reporting message (Bootstrap Message). the C-BSRs consider themselves to be the BSR until they learn about the BSR information. they broadcast the self-reporting message periodically in the PIM-SM domain. The self-report message contains the address and priority of the C-BSR, and the PIM elects the BSR by using the C-BSR priority and IP address.The C-BSR becomes a BSR based on the following: the C-BSR with the greater priority becomes the BSR, and, if the priority is the same, the C- BSR with the greater IP address becomes the BSR.After being configured as a C-BSR, the device sends a self-report message to all PIM neighbors, and the C -BSR address is specified as the IP address of the interface. Each PIM neighbor compares the address of the C-BSR to the address in the self-report message it previously received (which may have been received from more than one interface). If the C-BSR's address is the same as or greater than the previous address, then the PIM neighbor stores the current address and forwards the self-reported message; otherwise, the PIM neighbor discards the self-reported message from the C-BSR. The C-BSR considers itself to be the BSR until it receives a bootstrap message from another C-BSR with a higher priority (or the same priority but a larger IP address).Note: You can configure this command only on backbone network devices (routers or Ethernet switches) that are well connected to other network devices in the PIM domain.

Typically, only one C-BSR and one C-RP are configured in the network, and usually on the same network device (switch or router), which should generally be at the core of the network. Only one C-BSR can be configured on the same network device, and C-BSRs configured later replace the originally configured C-BSR.

Please configure it in PIM mode.

manipulate	command	clarification
Go to System View	system-view	
Enter the PIM view	mroute pim	
Configuring candidate BSRs	bsr-candidate { vlan-interface | supervlan-interface } *vlan-id hash-mask-length* [*priority*]	By default, PIM does not configure candidate BSRs. The priority configuration range is 0-255.
Deletion of candidate BSRs	undo bsr-candidate	

[Example]

! Configure VLAN interface 100 as a candidate BSR with a priority of 128

[GPON-router-pim]bsr-candidate vlan-interface 100 24 128

29.2.13 Configuring candidate RPs

After the election of a BSR, all C-RPs periodically send C-RP broadcast messages (C-RPAdvertisements) to the BSR. the BSR aggregates and diffusely publishes the RP information to the whole network (there may be multiple RPs in the network, which each have a different group service range), so that the RP information is available on all devices. When configuring C-RP, you can specify the scope of RP service, which can serve all multicast groups or only certain multicast groups.

Please configure it in PIM mode.

manipulate	command	clarification
Go to System View	system-view	
Enter the PIM view	mroute pim	
Configuring candidate RPs	rp-candidate { vlan-interface | supervlan-interface } *vlan-id* [group-list *acl-number* [*priority*]]	By default, PIM does not configure candidate RPs. The priority configuration range is 0-255.
Delete Candidate RP	undo rp-candidate { vlan-interface | supervlan-interface } *vlan-id* [group-list *acl-number*]	

[Example]

! Configure VLAN interface 100 as a candidate RP

[GPON-router-pim]rp-candidate vlan-interface 100

29.2.14 Configuring the SPT switching threshold

In PIM-SM mode, the receiving host usually joins to the RPT actively first, and then obtains the required multicast message through the RP. However, in general, the path in the RPT is often not the shortest path from the receiving host to the multicast source. In this case, the DR where the receiving host is located can choose to switch to join to the SPT to avoid the propagation delay of the multicast message. Currently, two fixed thresholds are supported, IMMEDIATELY and

INFINITY, where IMMEDIATELY is the default value.

Please configure it in PIM mode.

manipulate	command	clarification
Go to System View	system-view	
Enter the PIM view	mroute pim	
Configuring the SPT switching threshold	spt-threshold { immediately | infinity }	The default value is IMMEDIATELY
Restore the default SPT switching threshold	undo spt-threshold	

[Example]

! Configure the SPT switching threshold to infinity

[GPON-router-pim] spt-thresholdinfinity

29.2.15 Configuring SSM Multicast Group Scope

Whether the PIM-SSM model or the PIM-SM model is used in delivering information from a multicast source to a receiver depends on whether the multicast group in the receiver's subscription channel (S, G) is within the SSM multicast group range, and all interfaces with PIM-SM enabled will assume that the multicast groups that fall within the range use the PIM-SSM model.

Please perform the following configuration on all devices in the PIM-SM domain.

manipulate	command	clarification
Go to System View	system-view	
Enter the PIM view	mroute pim	
Configuring SSM Multicast Group Scope	ssm { default | range *acl-number*]}	By default, there is no SSM multicast group range
Delete SSM multicast group range	undo ssm { default | range *acl-number*]}	

[Example]

! Configure the SSM multicast group range to 224.1.1.1~224..1.1.2

[GPON] acl 4 denyany

[GPON] acl 4 permit 224.1.1.1 0.0.0.0

[GPON] acl 4 permit 224.1.1.2 0.0.0.0

[GPON-router-pim] ssm range 4

 Attention:

Ensure that the SSM multicast group address ranges configured on all devices in the domain are the same, otherwise multicast information will not be transmitted through the SSM model. If a multicast group belongs to the SSM multicast group range, but the members of the group use IGMPv1 or IGMPv2 to send join messages, the device will not trigger the (*, G) join message

29.2.16 PIM Monitoring and Maintenance

PIM configuration and operational information can be viewed at any attempt.

manipulate	command	clarification
Display information about interfaces running PIM	display ip pim interface [{ vlan-interface *vlan-id* } | { supervlan-interface *vlan-id* }]	When you do not specify a vlan interface, it means to view the pim configuration running information of all interfaces
Displaying PIM Neighbor Information	display ip pim neighbor	When multicast IP is not specified, it means view all multicast group information
Display the multicast routing table for PIM learning	display ip mroute *group-address* [static | dynamic]	The display includes static routing table entries and dynamic routing table entries.
Display the current RP information of PIM	displayip pim rp-info *group-address*	The display includes dynamically learned RPs and configured static RPs
Displaying BSR information	display ip pim bsr	The display includes information about the elected BSRs as well as information about locally configured candidate BSRs.
Display the configured SSM group address range	display ip pim ssm range	

[Example]

! Display PIM configuration information for VLAN interface 100

[GPON] display ip pim interface vlan-interface 100

Chapter 30 SNTP Client Configuration

30.1 Introduction to SNTP Protocol

SNTP stands for Simple Network Time protocol, which is currently an important engineering method for time synchronization on the Internet.

NTP protocol is an important method to provide accurate network time service.NTP protocol is the abbreviation of Network Time Protocol (Network Time Protocol), it is widely used for computer clock synchronization on the Internet, it is used to access the international standard time by providing a complete mechanism.In most cases, NTP is able to provide 1-50MS time accuracy depending on the synchronization source and network In most cases, NTP is able to provide a time accuracy of 1-50 MS depending on the synchronization source and network path.

NTP protocol in order to ensure a high degree of accuracy requires very complex algorithms. but in practice in many applications. second-level accuracy is sufficient. in this case. the SNTP protocol appeared. which by simplifying the original access protocols. under the premise of guaranteeing the accuracy of time. making it easy to develop and apply to the network time. the SNTP is mainly on the NTP protocol involves the security of the relevant access, Automatic server migration part has been scaled down.

The current version number of the SNTP protocol is SNTP V4, which is compatible with previous versions. More importantly, SNTP is interoperable with the NTP protocol, i.e., SNTP clients can work with NTP servers, and the same NTP clients can receive timing information from SNTP servers. This is because the packet formats of NTP and SNTP are the same, and the algorithms for calculating client time, time deviation, and packet round-trip delay are also the same. Therefore NTP and SNTP are practically inseparable.

SNTP works as follows:

SNTPv4 can work in three ways: unicast, wide (multicast), and anycast.

In unicast mode, the client actively sends a request to the server, and the server receives the request and constructs a response message to send back to the client based on the local time.

In broadcast and multicast mode, the server sends broadcast or multicast messages to the client at regular intervals, and the client passively receives the messages from the server.

In the anycast mode, the client first takes the initiative to use the local broadcast address or multicast address to send a request, at which time all the servers in the network will respond to the client, the client selects the server whose response message is received first as the server, discards the messages sent by the other servers, and elects a server, the working mode is the same as unicast.

In all modes, the client receives a response message and parses the message to get the current standard time, and calculates the network transmission delay and local time compensation through certain algorithms, and calibrates the current time by these data.

This device supports SNTP client, which can realize time synchronization with the server through the above three ways.

30.2 SNTP Client Configuration

30.2.1 SNTP Client Configuration Task List

The list of SNTP client configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable SNTP client function	compulsory	30.2.2
Configure how the SNTP client works	compulsory	30.2.3
Configuring Unicast Servers for SNTP Clients	selectable	30.2.4

Configure the broadcast delay for SNTP clients	selectable	30.2.5
Configure the polling interval for SNTP clients	selectable	30.2.6
Configure the timeout retransmission count and retransmission interval for SNTP clients	selectable	30.2.7
Configure the list of legitimate servers for SNTP clients	selectable	30.2.8
Configuring MD5 Authentication for SNTP Clients	selectable	30.2.9
Configuring Daylight Saving Time for SNTP Clients	selectable	30.2.10
Display SNTP client configuration information	selectable	30.2.11

30.2.2 Enable/disable SNTP client function

Turn on or off the configuration of the SNTP client function in system view. With the SNTP client function turned on, the device is able to obtain the standard time in the network and calibrate the local system time through the SNTP protocol, and the configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enable SNTP client	sntp client	Disable SNTP client functionality by default
Shutting down the SNTP client	undo sntp client	

[Example]

! Turn on the SNTP client function:

```
[GPON]sntp client
```

30.2.3 Configure how the SNTP client works

SNTPv4 can work in three ways: unicast, wide (multicast), and anycast. In unicast and anycast mode the client sends a request and receives a response, and corrects the system time after receiving the response. In broadcast and multicast mode the client passively waits for the broadcast message sent by the server and corrects the system time when it receives the response, the configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configure the SNTP client operating mode	sntpclient mode { broadcast | unicast | anycast [key *number*] | multicast }	The system works in broadcast mode by default
Restore the default SNTP client operating mode	undo sntp client mode	

[Example]

! Configure the SNTP client to work in anycast mode

```
[GPON]sntp client mode anycast
```

30.2.4 Configuring Unicast Servers for SNTP Clients

In unicast mode, the SNTP client must be configured with the server address, and the configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configuring Unicast Servers for SNTP Clients	sntp server ip-address [key number]	
Delete unicast servers for SNTP clients	undo sntp server	

[Example]

! Configure the unicast server address as 192.168.1.100

```
[GPON]sntp server 192.168.1.100
```

30.2.5 Configure the broadcast delay for SNTP clients

The configured transmission delay takes effect only in the wide (multicast) mode. After the transmission delay is configured, the SNTP client will automatically add the transmission delay to calibrate the current system time after obtaining the time from the server, with the following configuration commands.

manipulate	command	clarification
Go to System View	system-view	
Configure the broadcast delay for SNTP clients	sntp client broadcastdelay *milliseconds*	Broadcast delay configuration range is 1-9999ms, default value is 3ms
Restore the broadcast delay for the default SNTP client	undo sntp client broadcastdelay	

[Example]

! Configure the transmission delay for wide (multicast) to 10 milliseconds

```
[GPON]sntp client broadcastdelay 10
```

30.2.6 Configure the polling interval for SNTP clients

The configured polling intervals take effect only in unicast and anycast mode. the SNTP client initiates a request to the server at every polling interval to calibrate the current time. the configuration command is as follows.

manipulate	command	clarification
Go to System View	system-view	
Configure the polling interval for SNTP clients	sntp client poll-interval *seconds*	The polling interval is configured in the range of 64-1024S, and the default value is 1000S.
Restore the default SNTP client polling interval	undo sntp client poll-interval	

[Example]

! Configure the polling interval for SNTP requests to 500 seconds

```
[GPON]sntp client poll-interval500
```

30.2.7 Configure the timeout retransmission count and retransmission interval for SNTP clients

The configured timeout retransmission can take effect only in unicast and anycast mode. the SNTP request message is a UDP message and there is no guarantee that the request message will be delivered to the destination. you can use the timeout retransmission mechanism to configure the number of retransmissions and the retransmission interval. configure the following commands.

manipulate	command	clarification
Go to System View	system-view	
Configure the number of timeout retransmissions for SNTP clients	sntp client retransmit *times*	The timeout retransmission count is configured in the range of 1-10, and the default value is 3 times
Restore the timeout retransmission count for the default SNTP client	undo sntp client retransmit	
Configure the timeout retransmission interval for SNTP clients	sntp client retransmit-interval *seconds*	Timeout retransmission interval configuration range is 3-30S, the default value is 30S
Restore the timeout retransmission interval for the default SNTP client	undo sntp client retransmit-interval	

[Example]

! Configure the retransmission interval for SNTP requests to 10 seconds and the number of retransmissions to 5

[GPON]sntp client retransmit-interval10

[GPON]sntp client retransmit 5

30.2.8 Configure the list of legitimate servers for SNTP clients

The SNTP client, when working in broadcast or multicast mode, receives protocol messages from all servers without differentiation. In this way, when there is a malicious attacking server in the network (which provides incorrect time), the local time cannot be synchronized to the standard time. So SNTP can configure some legal server segments to filter the messages, and only the messages whose source address is in the list of legal servers will be received, the configuration command is as follows.

manipulate	command	clarification
Go to System View	system-view	
Configure the list of legitimate servers for SNTP clients	sntp client valid-server *ip-address wildcard*	Supports configuration of IP address segments by wildcard. The system does not have any legal server list configured by default.
Remove the list of legitimate servers for SNTP clients	undo sntp client valid-server { all | *ip-address* }	Selecting the all parameter means deleting the list of all legitimate servers.

[Example]

! Configure servers in network segment 192.168.1.0/24 as legitimate servers

[GPON] sntp client valid-server 192.168.1.0 0.0.0.255

30.2.9 Configuring MD5 Authentication for SNTP Clients

The SNTP client can use the list of legitimate servers to perform preliminary filtering of servers, but when some malicious attackers use the addresses of legitimate servers to forge server messages and deliberately attack the device, the device

can also filter the messages through MD5 authentication, and only authenticated messages are accepted by the client, with the following configuration commands.

manipulate	command	clarification
Go to System View	system-view	
Enabling MD5 Authentication for SNTP Clients	sntp client authenticate	The system disables MD5 authentication by default
Disabling MD5 Authentication for SNTP Clients	undo sntp client authenticate	
Configure keywords and passwords for SNTP client MD5 authentication	sntp client authentication-key *number* md5 *value*	Number is the authentication password ID. Value is the authentication password.
Remove the keyword for SNTP client MD5 authentication	undo sntp client authentication-key *number*	
Set keyword as trusted key	sntp trusted-key *number*	
Remove trusted key	undo sntp trusted-key *number*	

[Example]

! Turn on MD5 authentication for SNTP clients, configure the keyword ID as 1234 and the password as abcd, and set it as a trusted Key

```
[GPON]sntp client authenticate
[GPON]sntp client authentication-key 12 md5 abc
[GPON]sntp trusted-key 12
```

30.2.10 Configuring Daylight Saving Time for SNTP Clients

The SNTP client supports configuring the summer time band. When the time obtained by the SNTP client from the server is within the range of the configured Daylight Saving Time band, the SNTP client adds one hour to the obtained time as the system time; when the time obtained by the SNTP client from the server is outside the range of the configured Daylight Saving Time band, the SNTP client does not modify the obtained time and directly takes it as the system time, the configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configuring Daylight Saving Time for SNTP Clients	sntp client summer-time { dayly start-month start-day start-hh:mm:ss end-month end-day end-hh:mm:ss| weekly start-month start-week start-day start-hh:mm:ss end-month end-week end-day end-hh:mm:ss}	Defaults to a non-DST configuration
Delete Daylight Saving Time for SNTP Clients	undo sntp client summer-time	

[Example]

! Configure Daylight Saving Time from 0:00 on March 31 to 23:59:59 on October 31 of each year!

```
[GPON]sntp client summer-time dayly 3 31 00:00:00 10 31 23:59:59
```

30.2.11 Display SNTP client configuration information

SNTP client related configuration information can be viewed under any attempt.

manipulate	command	clarification
Displaying SNTP Client Configuration	display sntp client	
Show SNTP Daylight Saving Time Configuration	display sntp client summer-time	

[Example]

! Display SNTP client configuration information

[GPON]display sntp client

Chapter 31 802.1X Configuration

31.1 802.1X Protocol Introduction

The 802.1X protocol originated from the 802.11 protocol, which is the IEEE's protocol for wireless LANs, and was originally developed to solve the problem of authenticating wireless LAN users.The IEEE802LAN protocol defines the LAN The IEEE802LAN protocol defines a LAN that does not provide access authentication and allows users to access LAN devices or resources as long as they have access to a LAN control device (e.g., a LAN Switch). However, with the mobile office and the large-scale development of applications such as premises network operation, service providers need to control and configure user access. In particular, as WLAN applications and LAN access are carried out on a large scale on telecommunication networks, it is necessary to control ports to realize user-level access control and in addition there is a need for billing.

802.IX is a standard defined by the IEEE to address Port-Based Network Access Control. 802.1X is a port-based network access control technology that authenticates and controls access to a user at the physical access level of a LAN device, which in this case is the port of a Lan Switch (Ethernet switch) device's port. During the authentication process, the device acts as a proxy between the client and the authentication server, obtaining the user's identity information from the client device of the access device and verifying the information through the authentication server. If the user passes the authentication, the user is allowed to access the network within the LAN, otherwise the user is denied access.

802.1X is a standard for authenticating network clients (or ports) based on user ID or device. The process is called "port-level authentication". It uses the RADIUS (Remote Authentication Dial-In User Service) method and divides it into three different groups: the requesting party, the authenticating party, and the authorization server. The system implements the authentication system portion of IEEE 802.1X. To use the 802.1X authentication function, the following environment is also required: a RADIUS server is available and the system has access to that RADIUS server so that the system can pass the user's authentication information to the RADIUS server for authentication; and the 802.1X authentication client software needs to be installed in the user device (e.g., PC) that accesses the system.

31.2 AAA View Configuration

31.2.1 AAA view configuration task list

Before starting the 802.1X authentication function, you can configure the related parameters of the system or the Ethernet port. Each configuration parameter related to 802.1X authentication takes effect only after the 802.1X authentication function is activated. these configuration parameters remain after the 802.1X authentication function is shut down. the list of AAA view related configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enter AAA view	compulsory	31.2.2
Configure the device to restart the user re-authentication function	selectable	31.2.3
Enable/disable the H3C Cams compatibility feature	selectable	31.2.4
Configure the uplink/downlink bandwidth attribute number	selectable	31.2.5
Enable/disable sending client's version information to RADIUS server function	selectable	31.2.6
Enable/disable billing	selectable	31.2.7
Enable/disable billing message unresponsive cut-off user function	selectable	31.2.8
Enable/disable port 802.1P priority extension attributes	selectable	31.2.9
Enable/disable port PVID extended attributes	selectable	31.2.10
Enable/disable the port MAC address number limit extended attribute	selectable	31.2.11

Enable/disable port bandwidth control extended attribute configuration	selectable	31.2.12
Modify the extended attribute number	selectable	31.2.13
Configuring the default domain name	selectable	31.2.14

▪

31.2.2 Enter AAA view

AAA view completes the creation of the relevant domains and RADIUS schemes necessary for 802.1X authentication with the following configuration commands.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Exit AAA view	quit	

[Example]

! Enter AAA view

[GPON]aaa

[GPON-aaa]

31.2.3 Configure the device to restart the user re-authentication function

When the device is rebooted, the original online users on the RADIUS server cannot re-authenticate and log in, you can enable the user re-authentication function to be turned on. When this function is turned on, when the device is rebooted, if a user is authenticated, an Accounting-On message will be sent to the RADIUS server to notify the RADIUS server to force the user of the device to be taken offline, with the configuration commands as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enable device reboot user re-authentication	accounting-on enable *sendtimes*	The default is to turn off the re-authentication feature. Sendtimes indicates the number of times Accounting-On messages are sent, and the configuration range is 1-255.
Disable device reboot user re-authentication	accounting-on disable	

[Example]

! Enable the device reboot re-authentication feature, the device sends the Accounting-On message 10 times

[GPON-aaa]accounting-on enable 10

31.2.4 Enable/disable the H3C Cams compatibility feature

When the RADIUS server is H3C Cams, you can enable the related compatibility by the command, the configuration command is as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	

Enable H3C Cams compatibility	h3c-cams enable	Disable H3C Cams compatibility by default
Turn off H3C Cams compatibility	h3c-cams disable	

[Example]

! Enabling H3C Cams Compatibility

[GPON-aaa]h3c-cams enable

31.2.5 Configure the uplink/downlink bandwidth attribute number

The device supports configuring the attribute number of the uplink bandwidth/downlink bandwidth in the VendorSpecific attribute name through uprate-value/ dnrate-value, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Configure the uplink bandwidth attribute number	uprate-value rate-attribute	Attribute number configuration ranges from 1-32
Configure the downstream bandwidth attribute number	dnrate-value rate-attribute	Attribute number configuration ranges from 1-32

[Example]

! Configure the downstream bandwidth attribute number to 20

[GPON-aaa] dnrate-value 20

31.2.6 Enable/disable sending client's version information to RADIUS server function

Set the support configuration to send the version information of the client to the RADIUS server function, the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enable sending client version information to the RADIUS server function	radius attribute client-version	Send version information to server is disabled by default
Disable sending client version information to the RADIUS server.	undo radius attribute client-version	

[Example]

! Enable sending client version information to RADIUS servers

[GPON-aaa] radius attribute client-version

31.2.7 Enable/disable billing

After authentication, you can request relevant billing operations through radius accounting. this function is enabled by default. the relevant configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	

Enter AAA view	aaa	
Enable billing	radius accounting	Billing is enabled by default
Disable billing	undo radius accounting	

[Example]

! Turn off billing

[GPON-aaa] undo radius accounting

31.2.8 Enable/disable billing message unresponsive cut-off user function

After enabling billing, if there is no response to the billing message, the system cuts off user authentication, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enable billing message no response to cut off user function	radius server-disconnect drop 1x	Billing unresponsive cut off user function is enabled by default
Disable the billing message no response cut off user function	undo radius server-disconnect drop 1x	

[Example]

! Disable the billing message no response cut off user function

[GPON-aaa]undo radius server-disconnect drop 1x

31.2.9 Enable/disable port 802.1P priority extension attributes

The RADIUS server can extend the attribute name in the RADIUS message to perform some user characteristic operations. The device can enable the port priority extension attribute through radius 8021p enable, after this function is enabled, if the user passes the authentication, it will modify the priority of the port where the user is located, and this function is carried out by default through the attribute number 77 in the VendorSpecific attribute name. This function is carried out by default through the attribute number 77 in the VendorSpecific attribute, and the attribute number can be modified by using radius config-attribute, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enable the Port Priority Extension attribute	radius 8021p enable	Disable the port priority attribute by default
Disable the port priority extension attribute	undo radius 8021p	

[Example]

! Enable the port 802.1P priority extension attribute

[GPON-aaa] radius 8021p enable

31.2.10 Enable/disable port PVID extended attributes

The RADIUS server can extend the attribute name in the RADIUS message to perform some user characteristic operations. the device can enable the port PVID extension attribute through radius vlan enable. after this function is enabled, if the user authentication passes, it will modify the PVID of the port where the user is located. this function is fixed through the Tunnel-Pvt-Group This function is fixed by the Tunnel-Pvt-Group-ID attribute name, and the value of this attribute is required to be a string, through which the name descriptor of the VLAN is looked up to match the VLAN value, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enable the port PVID extended attribute	radius vlan enable	Disable the port PVID attribute by default
Disable the port PVID extended attribute	undo radius vlan	

[Example]

! Enable the port PVID extended attribute

[GPON-aaa] radius vlan enable

31.2.11 Enable/disable the port MAC address number limit extended attribute

The RADIUS server can perform some user-specific operations through the attribute name extension in the RADIUS message. The device can enable the port MAC address number limit extension attribute through the command, and after this function is enabled, if a user passes the authentication, it will modify the limit of the number of MAC addresses to be learned on the port where the user is located. This function is carried out by default through the attribute number 50 in the VendorSpecific attribute name, and the attribute number can be modified by using radius config-attribute, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enable the port MAC address number limit extended attribute	radius mac-address-number enable	Default Disable Port MAC Address Number Limit Attribute
Disable the port MAC address number limit extended attribute	undo radius mac-address-number	

[Example]

! Enable the port MAC address number limit extended attribute

[GPON-aaa] radius mac-address-number enable

31.2.12 Enable/disable port bandwidth control extended attributes

The RADIUS server can perform some user characteristic operations through the attribute name extension in the RADIUS message. the device can enable the port bandwidth control extension attribute through the command. uplink bandwidth control is performed by default through the attribute number 75 in the VendorSpecific attribute name, and the attribute number can be modified by using radius config-attribute. Downstream bandwidth control is performed by default through the 76 attribute number in the VendorSpecific attribute name, and the attribute number can be modified by using radius config-attribute. When this feature is enabled, the bandwidth control of the port where the user is located will be modified if the

user passes the authentication. The default bandwidth control unit value is kbps, which can be modified by radius config-attribute access-bandwidth unit, the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enable port bandwidth control extended attributes	radius bandwidth-limit enable	Disable port bandwidth control extended attributes by default
Disable the port bandwidth control extended attribute	undo radius bandwidth-limit	

[Example]

! Enable port bandwidth control extended attributes

[GPON-aaa] radius bandwidth-limit enable

31.2.13 Modify the extended attribute number

The RADIUS server can perform some user characteristic operations through the attribute name extension in the RADIUS message. the device can modify the corresponding extended attribute number through commands. the relevant configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Modify the port bandwidth control extended attribute number	radius config-attribute access-bandwidth { downlink | uplink } *vendor-type*	vendor-type indicates the extended attribute number, which can be configured in the range of 1-500, and the default value is described in Participating in the Extended Attribute Description above.
Modify the port bandwidth control unit value	radius config-attribute access-bandwidth unit { bps | kbps }	The default value is kbps
Modify the DSCP extended attribute number	radius config-attribute dscp *vendor-type*	
Modify the port MAC address number limit extended attribute number	radius config-attribute mac-address-number *vendor-type*	

[Example]

! Configure the downlink port bandwidth control extended attribute number to 100

[GPON-aaa] radius config-attribute access-bandwidth downlink 100

! Configure the port MAC address number limit extended attribute number to 200

[GPON-aaa] radius config-attribute mac-address-number 200

31.2.14 Configuring the default domain name

The system supports the configuration of the default domain name. When the user name does not carry a domain name during authentication, the system will treat the message as an illegal message and not process it when the default domain name is not configured. After configuring the default domain name, the system will add @ and the default domain name to the user name without a domain name to participate in authentication. When configuring the default domain, you must specify an existing domain, otherwise it will not succeed, the relevant configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Configuring the default domain name	default domain-name enable *domain-name*	You need to create a domain before you can set this domain name as the default domain name, the default domain name is not configured by default
Do not configure a default domain name	default domain-name disable	

[Example]

! Configure the default domain name test

[GPON-aaa] default domain-name enable test

31.3 RADIUS server configuration

31.3.1 RADIUS Server Configuration Task List

The RADIUS server holds the identity information of legitimate users, etc. When a user authenticates, the system forwards the user's identity information to the RADIUS server and forwards the authentication result information from the RADIUS server to the user. Users accessing the system can access the resources in the LAN only if they are authenticated by the RADIUS server. a list of the main configuration tasks of the RADIUS server is shown below.

Configuration tasks	clarification	Detailed Configuration
Create and enter the RADIUS server view	compulsory	31.3.2
Configure the IP address and authentication port of the master/slave authentication server	compulsory	31.3.3
Configure the IP address and authentication port of the master/slave billing server	compulsory	31.3.4
Configure the shared key between the device and the current RADIUS authentication server	compulsory	31.3.5
Configure a shared key between the system and the current RADIUS billing server	compulsory	31.3.6
Configure the NAS_IPAddress value sent to the RADIUS server	selectable	31.3.7
Configure the system to pass messages to the RADIUS server with or without a domain name.	selectable	31.3.8
Configuring Real-Time Billing for RADIUS Servers	selectable	31.3.9
Display RADIUS server configuration information	selectable	31.3.10

31.3.2 Create and enter the RADIUS server view

In AAA view, use the radius host command to enter the RADIUS server view. If this RADIUS server does not exist, create this RADIUS server automatically first and enter the server view. the relevant configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Create and enter the RADIUS server view	radius host *radius-name*	The value of the RADIUS server scheme name is in the range of 1 to 32 characters, case insensitive and Cannot contain spaces
Deleting a RADIUS server	undo radius host [*radius -name*]	

[Example]

! Enter the RADIUS server test

[GPON-aaa]radius host test

[gpon-aaa-radius-test]

31.3.3 Configure the IP address and authentication port of the master/slave authentication server

Under RADIUS server view, you can configure the IP address and authentication port of the master/slave authentication server, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enter the RADIUS server view	radius host *radius-name*	
Configure the IP address and authentication port of the primary authentication server	primary-auth-ip auth-ip-address auth-port	
Deleting the Primary Authentication Server Configuration	undo primary-auth-ip	
Configure the IP address and authentication port of the slave authentication server	second-auth-ip auth-ip-address auth-port	
Delete the slave authentication server configuration	undo second-auth-ip	

[Example]

! Configure the IP address of the RADIUS test master authentication server as 192.168.1.100 and the authentication port number as 1812

[GPON-aaa-radius-test]primary-auth-ip 192.168.1.100 1812

31.3.4 Configure the IP address and authentication port of the master/slave billing server

Under RADIUS server view, you can configure the IP address and authentication port of the master/slave billing server, and the related configuration commands are as follows.

manipulate	command	clarification

Go to System View	system-view	
Enter AAA view	aaa	
Enter the RADIUS server view	radius host *radius-name*	
Configure the IP address and authentication port of the primary authentication server	primary-acct-ip acct-ip-address auth-port	The billing server and the authentication server can be the same IP address, which means that the authentication and billing operations are performed on the same server.
Deleting the Primary Authentication Server Configuration	undo primary-acct-ip	
Configure the IP address and authentication port of the slave authentication server	second-acct-ip acct-ip-address acct-port	
Delete the slave authentication server configuration	undo second-acct-ip	

[Example]

! Configure the IP address of the RADIUS test master billing server to 192.168.1.100 and the authentication port number to 1813

[GPON-aaa-radius-test]primary-auth-ip 192.168.1.100 1813

31.3.5 Configure the shared key between the device and the RADIUS authentication server

The system supports setting the shared key with the current RADIUS authentication server. the key between the device and the RADIUS authentication server needs to be matched in order to carry out authentication processing. the relevant configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enter the RADIUS server view	radius host *radius-name*	
Configure key sharing with the authentication server	auth-secret-key *secret-key*	
Remove the shared key with the authentication server	undo auth-secret-key	

[Example]

Set the shared key between the device and the RADIUS authentication server test to 123456! Set the shared key between the device and the RADIUS authentication server test to 123456.

[GPON-aaa-radius-test] auth-secret-key 123456

31.3.6 Configure a shared key between the device and the RADIUS billing server

The system supports setting the shared key with the current RADIUS billing server. the key between the device and the RADIUS billing server needs to be matched for billing processing. the relevant configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	

Enter AAA view	aaa	
Enter the RADIUS server view	radius host *radius-name*	
Configure key sharing with the billing server	acct-secret-key *secret-key*	
Remove shared keys with the billing server	undo acct-secret-key	

[Example]

! Set the shared key between the device and the RADIUS billing server, test, to 123456.

[GPON-aaa-radius-test] acct-secret-key 123456

31.3.7 Configure the NAS_IPAddress value sent to the RADIUS server

The system supports configuring the value of nas-ipaddress to be sent to the RADIUS server, if not configured then the Layer 3 interface IP address of the device is used, the relevant configuration is as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enter the RADIUS server view	radius host *radius-name*	
Configure the NAS IP address to be sent to the RADIUS server	nas-ipaddress *ip-address*	
Delete the NAS IP address sent to the RADIUS server	undo nas-ipaddress	

[Example]

! Configure the NAS IP address sent to the RADIUS server test to be 192.168.1.100

[GPON-aaa-radius-test]nas-ipaddress 192.168.1.100

31.3.8 Configure the system to pass messages to the RADIUS server with or without a domain name.

The system supports configuring whether the user name should be with domain name when passing messages to the current RADIUS server. with-domain is with domain name and without-domain is without domain name. the relevant configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enter the RADIUS server view	radius host *radius-name*	
Configure the system to pass messages to the RADIUS server with the domain name of the user.	username-format with-domain	Default configuration with domain name
Configure the system to pass messages to the RADIUS server with a username	username-format without-domain	

without a domain name.		

[Example]

Configure the user name to be sent to the RADIUS server test without the domain name! Configure the username to be sent to the RADIUS server test delivery message without the domain name.

[GPON-aaa-radius-test] username-format without-domain

31.3.9 Configuring Real-Time Billing for RADIUS Servers

The system supports configuring the real-time accounting function for the RADIUS server with the realtime-account command under the RADIUS server view. the real-time accounting function is turned on by default, and the real-time accounting message sending interval is 12 minutes. the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Enter the RADIUS server view	radius host *radius-name*	
Enable real-time billing for RADIUS servers	realtime-account interval	Real-time billing is turned on by default
Configuring the RADIUS Server Real-Time Billing Message Transmission Interval	realtime-account interval interval	Interval indicates the real-time billing message sending interval, the configuration range is 1-255 minutes, and the default configuration is 12 minutes. Configuring the real-time billing interval command also turns on the real-time billing function.
Disable real-time billing for RADIUS servers	undo realtime-account	

[Example]

! Configure the RADIUS server test real-time billing function, the real-time billing message sending interval is 15 minutes

[GPON-aaa-radius-test] realtime-account interval 15

31.3.10 Display RADIUS server configuration information

RADIUS server-related configuration information can be displayed under any attempt.

manipulate	command	clarification
Display RADIUS server configuration information	display radius host [*radius-name*]	When no RADIUS server name is specified, all RADIUS server configuration information is displayed.
Display client version information sent to the RADIUS server configuration	display radius attribute	
Display the RADIUS server extended attribute number to modify the configuration	display radius config-attribute	

[Example]

! Show all RADIUS server configurations

[GPON] display radius host

31.4 domain configuration

31.4.1 Domain Configuration Task List

Clients need to provide a user name and password during authentication, the user name generally includes the user ISP information, domain and ISP one-to-one correspondence, the domain of the most important information is the domain of the user to which a RADIUS server authentication and billing. The list of main configuration tasks for the domain is as follows.

Configuration tasks	clarification	Detailed Configuration
Create and enter the domain view	compulsory	31.4.2
Configuring Domain Binding RADIUS Servers	compulsory	31.4.3
Configure the maximum number of users allowed to authenticate through the domain	selectable	31.4.4
Activate/deactivate domains	compulsory	31.4.5
Displaying Domain Configuration Information	selectable	31.4.6

▪

31.4.2 Create and enter the domain view

In AAA view, you can enter the domain view with the domain command. If the domain does not exist, the domain is automatically created first and you enter the domain view, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Create and enter the domain view	domain domain-name	The value of the field is in the range of 1 to 24 characters, case insensitive and cannot contain spaces.
Deleting a Domain Configuration	undo domain *domain-name*	

[Example]

! Create and enter the domain test.com

[GPON-aaa]domain test.com

[GPON-aaa-domain-test.com]

31.4.3 Configuring Domain Binding RADIUS Servers

Use the radius host command to select a RADIUS server for the current domain. The administrator specifies an existing RADIUS server to be configured as the RADIUS server for the current domain and enters domain view with the following configuration commands.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Go to the domain view	domain domain-name	

Configuring Domain Binding RADIUS Servers	radius host binding *radius-name*	You need to create the RADIUS server first and then configure the binding.
Removing Domain Bindings Configuring a RADIUS Server	undo radius host binding	

[Example]

! Bind RADIUS server test to domain test.com

[GPON-aaa-domain-test.com]radius host binding test

31.4.4 Configure the maximum number of users allowed to authenticate through the domain

Use the access-limit command to configure the maximum number of users allowed to authenticate through the current domain. the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Go to the domain view	domain domain-name	
Configure the maximum number of users allowed to authenticate through the domain	access-limit enable *max-num*	The maximum number of users is configured in the range of 1-640. the default configuration is unlimited.
Remove the maximum number of users allowed to authenticate through a domain configuration	access-limit disable	

[Example]

! Configure the maximum number of users allowed to authenticate through the test.com domain to 200

[GPON-aaa-domain-test.com] access-limit enable 200

31.4.5 Activate/deactivate domains

After you configure a domain, you need to activate the domain to take effect. The default domain is in the disabled state after configuration, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter AAA view	aaa	
Go to the domain view	domain domain-name	
activation domain	state active	The default domain is disabled
Disable Domain	state block	

[Example]

! Activate the domain test.com

[GPON-aaa-domain-test.com] state active

31.4.6 Displaying Domain Configuration Information

Domain configuration information can be displayed at any attempt.

manipulate	command	clarification
Displaying Domain Configuration Information	display domain [*domain-name*]	When no domain name is specified, all domain configuration information is displayed

[Example]

! Display Domain Configuration Information

```
[GPON] display domain
```

31.5 802.1X Configuration

31.5.1 802.1X Configuration Task List

The list of 802.1X configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable 802.1X authentication function	compulsory	31.5.2
Configure the port to send 802.1X watchdog messages	selectable	31.5.3
Set the protocol type between the device and the RADIUS server	selectable	31.5.4
Configuring the Reauthentication Function	selectable	31.5.5
Configure the control mode of an 802.1X port	selectable	31.5.6
Configure the maximum number of users allowed to authenticate on a port	selectable	31.5.7
Delete the specified online user	selectable	31.5.8
Configuring Heartbeat Detection	selectable	31.5.9
Configuring the Silent Function	selectable	31.5.10
Configuring the Guest VLAN Function	selectable	31.5.11
Configure host mode under port-based authentication	selectable	31.5.12
Configuring EAPOL Message Passthrough	selectable	31.5.13
Display 802.1X configuration information	selectable	31.5.14

31.5.2 Enable/disable 802.1X authentication function

The dot1x method command is used to start the 802.1X authentication function. Only after starting this function can the previous domain and RADIUS server configurations take effect, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enable 802.1X authentication function	dot1x method { macbased | portbased }	
Disable 802.1X authentication	undo dot1x	

[Example]

! Start the 802.1X authentication function of the device and configure it as MAC address-based authentication method

```
[GPON]dot1x method macbased
```

31.5.3 Configure the port to send 802.1X watchdog messages

Configure whether to send 1x watchdog messages on a port, and if so, configure the sending period. 1x watchdog messages are not sent by default, and the default is to send them once in 60 seconds after opening, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Global Configuration of the Send Watchtower Messages Function	dot1x daemon [interface ethernet *interface-list*]	When no port is specified, it indicates that all ports are configured. Global configuration indicates bulk configuration of all ports.
Disable sending watchdog messages	undo dot1x daemon [interface ethernet *interface-list*]	
Configure the watchdog message sending period globally	dot1x daemon time *time* [interface ethernet *interface-list*]	Send interval configuration range is 10-600S, the default configuration is 60S
Restore the default watchdog message delivery period	undo dot1x daemon time [interface ethernet *interface-list*]	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the port 802.1X watchdog message sending	dot1x daemon	
Disable port 802.1X watchdog message sending	undo dot1x daemon	
Configure the port 802.1X watchdog message sending period	dot1x daemon time *time*	
Disable port 802.1X watchdog message sending	undo dot1x daemon	

[Example]

! Turn on the Ethernet port 1 watchdog function and configure the send period to 30 seconds

```
[GPON-ethernet-0/0/1]dot1x daemon time 30
```

31.5.4 Configure the protocol type between the device and the RADIUS server

The system supports setting the protocol type between the device and the RADIUS server. Setting the eap-finish type, the device can convert the 802.1X authentication messages sent by the user encapsulated in EAP frames into data frames encapsulated in the standard RADIUS protocol before forwarding them to the RADIUS server. After the eap-transfer command is set, the device can forward the 802.1X authentication messages encapsulated in EAP frames sent by users to the RADIUS server directly without any processing. By default, the system uses eap-finish to forward user authentication messages, and the related configuration commands are as follows.

manipulate	command	clarification

Go to System View	system-view	
Configuring Finish Mode	dot1x eap-finish	Defaults to finish mode
Configure transfer mode	dot1x eap-transfer	

[Example]

! Setting up communication between the system and the RADIUS server via the standard RADIUS protocol

[GPON] dot1x eap-finish

31.5.5 Configuring the Reauthentication Function

The system supports setting the immediate re-authentication and periodic re-authentication functions of the port. Setting immediate re-authentication means that the user is manually triggered to re-authenticate once. Periodic re-authentication means that the client user is re-authenticated periodically, and the related configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configuring Immediate Reauthentication	dot1x re-authenticate [interface ethernet *interface-list*]	When the port number is not specified, it means that all ports are immediately re-authenticated.
Open Cycle Recertification	dot1x re-authentication [interface ethernet *interface-list*]	When the port number is not specified, it means that all ports are enabled for periodic re-authentication.
Off-cycle recertification	undo dot1x re-authentication [interface ethernet *interface-list*]	
Configuring the Reauthentication Period	dot1x timeout re-authperiod *period* [interface ethernet *interface-list*]	When the port number is not specified, it means configure the re-authentication period of all ports, the configuration range is 1-3600S, and the default re-authentication period is 3600S.
Restore the default re-authentication cycle	undo dot1x timeout re-authperiod [interface ethernet *interface-list*]	

[Example]

! Enable device cycle re-authentication, re-authentication cycle configuration not 1200S

[GPON]dot1x re-authentication

[GPON]dot1x timeout re-authperiod 1200

31.5.6 Configure the control mode of an 802.1X port

After turning on the 802.1X authentication function, all the ports of the system are in the state of requiring authentication by default, but the uplink ports and the ports connecting to the server should not require authentication, and three authentication modes can be set for the ports using dot1x port-control:

Forceauthorized, indicates a force-authorized authentication type, which does not require authentication to communicate;

Forceunauthorized, denotes a forced unauthorized authentication type, which cannot be communicated with or without authentication;

Auto mode, which indicates that the port needs to be authenticated before it can communicate. The port defaults to Auto

authentication mode, and the related configurations are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configure the port as a forced authorization authentication type port	dot1x port-controlforceauthorized [interface ethernet *interface-list*]	When no port number is specified, it means configure all ports
Configure the port as a forced unauthorized authentication port	dot1x port-control forceunauthorized [interface ethernet *interface-list*]	
Configured as an auto authentication port	dot1x port-control auto [interface ethernet *interface-list*]	
Restore the port default authorization authentication configuration	undo dot1x port-control [interface ethernet *interface-list*]	Port defaults to auto type authentication port

[Example]

! Ethernet port 1 is connected to the uplink server device, configure Ethernet port 1 as a mandatory authorization authentication port

```
[GPON] dot1x port-control forceauthorized interface ethernet 0/0/1
```

31.5.7 Configure the maximum number of users allowed to authenticate on a port

The system supports limiting the number of users allowed to pass 802.1X authentication, and supports configuring the maximum number of users under global and port views. Global configuration means configuring the maximum number of users for all ports in bulk, and the configuration is based on the last configured number of users, and the related configurations are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configure the maximum number of users globally	dot1x max-user *user-num* [interface ethernet *interface-list*]	When no port is specified, it means to configure all ports. The maximum number of users is configured in the range of 1-100, and the default configuration is 60.
Restore the default maximum number of users	undo dot1x max-user [interface ethernet *interface-list*]	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Port Configuration Maximum Number of Users	dot1x max-user *user-num*	The maximum number of users is configured in the range of 1-100, and the default configuration is 60
Restore the port's default maximum number of users	undo dot1x max-user	

[Example]

! Configure the number of authenticated users allowed on all Ethernet ports to 50

```
[GPON] dot1x max-user 50
```

31.5.8 Delete the specified online user

The system supports the deletion of specified online users by user name and MAC address, and the related configurations are as follows.

manipulate	command	clarification
Go to System View	system-view	
Delete online users based on MAC address	dot1x user cutmac-address *mac-address*	
Delete online users based on username	dot1x user cut username *username*	

[Example]

! 删除用户名为abcd@test.com的在线用户

[GPON]dot1x user cut username abcd@test.com

31.5.9 Configuring Heartbeat Detection

The system supports setting to turn on the heartbeat detection function for online 802.1X clients and configuring the heartbeat detection interval, and the related configurations are as follows.

manipulate	command	clarification
Go to System View	system-view	
Turn on heartbeat detection	dot1x detect [interface ethernet *interface-list*]	When the port number is not specified, it means that all ports are configured. The default is to disable heartbeat detection for all ports.
Disable heartbeat detection	undo dot1x detect [interface ethernet *interface-list*]	
Configuring the Heartbeat Detection Interval	dot1x detect interval *interval*	Heartbeat detection interval configuration range is 1-3600S, default configuration is 25S
Restore the default heartbeat detection interval	undo dot1x detect interval	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Turn on heartbeat detection	dot1x detect	
Disable heartbeat detection	undo dot1x detect	

[Example]

! Turn on heartbeat detection on Ethernet port 2 and configure the heartbeat detection period to 60 seconds

[GPON]dot1x detect interface ethernet 0/0/2

[GPON]dot1x detect interval 60

31.5.10 Configuring the Silent Function

The system supports the configuration of the silent function. After the silent function is enabled, if the user fails to authenticate, then the user will not be able to authenticate again during the silent time, and the related configurations are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Silent Function	dot1x quiet-period-value *quiet-period-value*	Silence time configuration range is 0-600S, the default is 0S that does not open the silence function
Turning off the silent function	undo dot1x quiet-period-value	

[Example]

! Start the silent function and configure the silent time to 10 seconds

```
[GPON] dot1x quiet-period-value 10
```

31.5.11 Configuring the Guest VLAN Function

The port's Guest VLAN takes effect only when portbased authentication is enabled. After the port is configured with the Guest VLAN, the port joins to this VLAN in an untagged manner, and at this time, the user can and only can access the network resources of this VLAN. Once the user is successfully authenticated, the port automatically reverts to the previously configured VLAN, and if the authentication server issues a valid If the authentication server issues a valid VLAN, the port is automatically added to the issued VLAN, and the port is restored to the Guest VLAN after the user goes offline. To ensure that the various functions can be used normally, assign different VLAN IDs to the Config VLAN, radius-issued VLAN, and Guest VLAN, etc., and the relevant configurations are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configure guest vlan	dot1x guest-vlan *vlan-id* [interface ethernet *interface-list*]	
Delete guest vlan	undo dot1x guest-vlan [interface ethernet *interface-list*]	

[Example]

! Configuring Guest VLAN 100

```
[GPON] dot1x guest-vlan 100
```

31.5.12 Configure host mode under port-based authentication

The host mode configuration takes effect only when portbased authentication is enabled. Host mode is automatically disabled if the port is set to macbased authentication when the host mode is configured as single-host. Host mode includes the following two modes:

1) multi-hosts: multi-hosts mode, when a user on this port passes the authentication, other users on this port can access the network without authentication;

2) single-host: single-host mode, only one authenticated user is allowed to access the network on this port, and other users cannot access the network or be authenticated again.

The relevant configuration commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configured for single host mode	dot1x portbased host-modesingle-host [interface ethernet *interface-list*]	
Configuring for Multi-Host Mode	dot1x portbased host-modemulti-hosts [interface ethernet *interface-list*]	

Restore port default host mode	undo dot1x portbased host-mode [interface ethernet *interface-list*]	Multi-host mode by default

[Example]

! Configure Ethernet port 1 host mode as single host mode

[GPON] dot1x portbased host-mode single-host interface ethernet 0/0/1

31.5.13 Configuring EAPOL Message Passthrough

When the port turns off 802.1x authentication, it is required to be able to pass through the 802.1x EAPOL message of the user, and the device acts as a relay, so that the user can carry out 802.1x authentication in the upper layer device. This function can only handle the EAPOL messages on the CPU, for the messages not on the CPU by the hardware itself, not subject to this configuration.EAPOL message passthrough port and its uplink port can only be configured on the port that turns off the 802.1x authentication function, and the port that opens the 802.1x authentication can not be configured with the passthrough function, the relevant configurations are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enable EAPOL message passthrough for the port	dot1x eapol-relay [interface ethernet *interface-list*]	When the port number is not specified, it means that all ports are configured. By default, all ports disable the EAPOL message passthrough function.
Disable EAPOL message passthrough on the port	undo dot1x eapol-relay [interface ethernet *interface-list*]	
Configuring the uplink port for EAPOL message passthroughs	dot1x eapol-relay uplink [interface ethernet *interface-list*]	
Deleting the uplink port for EAPOL message passthroughs	undo dot1x eapol-relay uplink [interface ethernet *interface-list*]	

[Example]

! Configure Ethernet port 1 to enable EAPOL message passthrough

[GPON] dot1x eapol-relay interface ethernet 0/0/1

31.5.14 Monitoring and Maintenance of 802.1X

You can view 802.1X related configuration and operation information under any attempt.

manipulate	command	clarification
Viewing 802.1X configuration information	display dot1x [interface ethernet *interface-list*]	The display includes configuration information such as 802.1X authentication type, port mode, re-authentication configuration, and maximum number of authenticated users. When no port is specified, it means that all ports are displayed.
Display Watchtower Message Function Configuration	display dot1x daemon [interface ethernet *interface-list*]	

Show Heartbeat Detection Function Configuration	display dot1x detect [interface ethernet *interface-list*]	
Show EAPOL Message Passthrough Function Configuration	display dot1x eapol-relay [interface ethernet *interface-list*]	
Show Guest VLAN Configuration	display dot1x guest-vlan [interface ethernet *interface-list*]	
Display port authentication status	display dot1x port-auth	Display whether the port has passed the authentication, through the authentication for open, not through the authentication for close
Display Silent Function Configuration	display dot1x quiet-period-value	
Display 802.1X authenticated user information	display dot1x session [interface ethernet *interface-list* | mac-address *mac-address*]	

[Example]

! View 802.1X configuration information

[GPON]display dot1x

Chapter 32 LLDP Configuration

32.1 Introduction to the LLDP Protocol

LLDP (Link Layer Discovery Protocol), is a Layer 2 discovery protocol defined by IEEE 802.1AB. By adopting LLDP technology, the network management system can quickly grasp the Layer 2 network topology information and topology change information when the network scale is rapidly expanding.

LLDP provides a standard link layer discovery method, which can organize the main capabilities, management address, device identification, interface identification and other information of the local device into different TLVs (Type/Length/Value) and encapsulate them in LLDPDU (Link Layer Discovery Protocol Data Unit) for distribution to directly connected neighbors. Unit (Link Layer Discovery Protocol Data Unit) is released to the neighbor directly connected to itself, and the neighbor receives this information and saves it in the form of standard MIB (Management Information Base) for the network management system to query and judge the communication status of the link.

32.2 LLDP Function Configuration

32.2.1 LLDP Feature Configuration Task List

The configuration tasks take effect only after the global LLDP switch is turned on. Before you turn on the global LLDP switch, you can configure the global LLDP and individual port-related parameters, which remain after the global LLDP switch is turned off, and take effect when the global LLDP switch is turned on.The list of major LLDP configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable LLDP function	compulsory	32.2.2
Configuring Hello-time for LLDP	selectable	32.2.3
Configuring Hold-time for LLDP	selectable	32.2.4
Configure the LLDP Chassis-id	selectable	32.2.5
Configure the port LLDP message sending and receiving mode	selectable	32.2.6
Configure the management IP address interface for LLDP messages	selectable	32.2.7
Display LLDP information	selectable	32.2.8

▪

32.2.2 Enable/disable global LLDP function

Please configure the LLDP function switch under the system view. The LLDP function can take effect only after the global function is turned on:

manipulate	command	clarification
Go to System View	system-view	
Enable LLDP function	lldp	The system disables lldp by default
Disable LLDP function	undo lldp	

[Example]

! Enable global LLDP function

[GPON]lldp

32.2.3 Configuring Hello-time for LLDP

The system can configure the time interval for sending LLDP protocol messages each time. do the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Configuring Hello-time for LLDP	lldp hello-time *seconds*	Hello-time configuration range is 5-32768S, default is 30S
Restore the default LLDP Hello-time	undo lldp hello-time	

[Example]

! Configure LLDP hello-time to 60 seconds

[GPON]lldp hello-time60

32.2.4 Configuring Hold-time for LLDP

The system can configure the LLDP survival time granularity. you can determine the survival time of the neighbor table entries by the survival time granularity and the hello-time time. the product of hello-time and hold-time indicates the survival time of the neighbor table entries. do the following configurations in global configuration mode.

manipulate	command	clarification
Go to System View	system-view	
Configuring Hold-time for LLDP	lldp hold-time *seconds*	Hold-time configuration range is 2-10S, default is 4S
Restore the Hold-time of the default LLDP	undo lldp hold-time	

[Example]

! Configure the LLDP hold-time to 5

[GPON]lldp hold-time 5

32.2.5 Configure the LLDP Chassis-id

The system can configure LLDP Chassis-id, which identifies the device chassis ID. the device chassis ID TLV is a fixed TLV that identifies the chassis that contains the IEEE 802 LAN workstations that are associated with the LLDP sending agent. There are various ways to identify the airframe, and the airframe ID subtype is used to indicate the type of components involved in the airframe ID domain. Each LLDP message contains one and only one Body ID TLV, and the value of the Body ID field shall remain the same for all LLDP messages while the connection remains normal.

The body ID subtype of this device is 5, which identifies the Network Address, and the system supports the configuration of Chassis-ID, which is configured as the IP address. when Chassis-ID is not configured, in order to prevent the existence of Chassis-ID conflicts in the network, the system will default to using the last four MAC digits of the device's MAC address as the Chassis ID. related configurations The commands are as follows.

manipulate	command	clarification
Go to System View	system-view	
Configure the Chassis-ID for LLDP	lldp chassis-id *ip-address*	
Restore the Chassis-ID of the default LLDP	undo lldp chassis-id	

[Example]

! Configure the LLDP Chassis-ID to 192.168.1.100

[GPON] lldp chassis-id 192.168.1.100

32.2.6 Configure the port LLDP message sending and receiving mode

The port has three send and receive modes for LLDP message processing:

Rx mode: receive LLDP messages only

Tx mode: sends only LLDP messages

Rxtx mode: sending and receiving LLDP messages

In addition, it supports to shut down the port lldp function. After shutting down, the port no longer processes LLDP messages, and the related configurations are as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the port LLDP message sending and receiving mode	lldp { rx | rxtx | tx }	The port's default send/receive mode is rxtx
Disable port LLDP function	undo lldp	When you configure the lldp message sending and receiving mode, you also turn on the lldp message processing function of the port, so there is no command to turn on the lldp function under the port

[Example]

! Configure Ethernet port 0/0/1 to receive only LLDP messages

[GPON-ethernet-0/0/1]lldp rx

32.2.7 Configure the management IP address interface for LLDP messages

For Layer 2 devices, the device supports only one management IP address, so it is sufficient to use the local management IP address for the local device IP address in the LLDP message without special specification. For Layer 3 devices, because the device supports configuration of multiple Layer 3 interfaces, multiple IP addresses can be configured, so you need to specify the local IP address in the LLDP message, and after specifying the IP address interface, the device will use the Layer 3 interface main IP address to encapsulate the LLDP message and send the message to the opposite end of the device, and the related configuration is as follows.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the management IP address interface for LLDP messages	lldp management-address { vlan-interface | supervlan-interface } *vlan-id*	Specify the Layer 3 interface, if more than one IP is configured in the Layer 3 interface, the primary IP shall prevail.
Delete the management IP address interface configuration for LLDP messages	undo lldp management-address	

[Example]

! Configure the management IP address interface for LLDP messages on Ethernet port 0/0/1 as VLAN Layer 3 interface 100

[GPON-ethernet-0/0/1] lldp management-address vlan-interface 100

32.2.8 Display LLDP information

LLDP-related information can be displayed at any attempt.

manipulate	command	clarification
Display LLDP information	display lldp interface [ethernet *interface-list*]	Displayed information includes: LLDP switch information, LLDP global parameter configuration information, port send/receive packet statistics, port neighbor information, etc.

[Example]

! Display LLDP information for Ethernet port 1

```
[GPON]display lldp interface ethernet 0/0/1
```

Chapter 33 PPPoE Plus Configuration

33.1 Introduction to PPPoE Plus

PPPoE (Point to Point Protocol over Ethernet), Point to Point Protocol over Ethernet, is a network tunneling protocol that encapsulates the Point to Point Protocol (PPP) in the Ethernet (Ethernet) framework. Because the protocol integrates the PPPoE protocol, it realizes the authentication, encryption, and compression functions that traditional Ethernet cannot provide, and PPPoE can also be used in cable modems (Cable Modem) and digital subscriber lines (DSL) and other Ethernet protocols to provide access services to users of the protocol system.

PPPoE Plus, short for PPPoE Intermediate agent, is a device that connects directly to the end-user and adds the user's physical information (connected port, VLAN, and MAC address of the local device, etc.) to the Sub-Tag field of the PPPoE protocol message. The authentication server can read this information to know the specific location of the user in the network in order to manage, maintain and serve the user. The realization principle is similar to that of the DHCP Option82 scheme, and the PPPoE protocol message is expanded. The access device intercepts the protocol message in the PPPoE discovery phase, inserts the user's physical information in the uplink direction, and strips off the user's physical information in the downlink direction, and then forwards it.

33.2 PPPoE Plus Feature Configuration

33.2.1 PPPoE Plus Feature Configuration Task List

The list of major configuration tasks for PPPoE Plus is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable PPPoE Plus function	compulsory	33.2.2
Configuring the PPPoE Plus Message Format Type	selectable	33.2.3
Configuring the PPPoE Plus Message Format	selectable	33.2.4
Configuring the PPPoE Plus Message Separator	selectable	33.2.5
Configuring the PPPoE Plus Label Replacement Policy	selectable	33.2.6
Configure the PPPoE Plus port type	selectable	33.2.7
Configure a custom Circuit ID	selectable	33.2.8
Configuring the Discard PPPoE Messages Function	selectable	33.2.9
Show PPPoE Plus Configuration	selectable	33.2.10

▪

33.2.2 Enable/disable PPPoE Plus function

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Enable PPPoE Plus function	pppoeplus	The system disables the pppoe plus function by default
Disable the PPPoE Plus feature	undo pppoeplus	

[Example]

! Enable the device PPPoE Plus function

```
[GPON]pppoeplus
```

33.2.3 Configuring the PPPoE Plus Message Format Type

The types of PPPoE Plus message formats supported by the system are: Standard format, Huawei format, and customized format. The default type is standard, and the added label format is China Telecom standard; when the type is huawei, the added label contains hostname information, and the customized format allows you to flexibly select the message according to the user's needs. content, please make the following configurations under global view.

manipulate	command	clarification
Go to System View	system-view	
Configure the PPPoE Plus type as Huawei or Standard	pppoeplus type { standard | huawei }	The system defaults to the standard type
Configure circuit-id for custom type PPPoE Plus	pppoeplus type self-defined circuit-id [*user-defined-string*] [client-mac] [hostname] [port] [switch-mac] [vlan] [ont-id] [ont-mac] [ont-sn]	
Configure the remote-id for custom type PPPoE Plus	pppoeplus type self-defined remote-id [*user-defined-string*] [client-mac] [hostname] [switch-mac]	
Restore the default PPPoE Plus type	undo pppoeplus	

[Example]

! Enable PPPoE Plus type as Huawei

```
[GPON]pppoeplus type huawei
```

33.2.4 Configuring the PPPoE Plus Message Format

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Configure the PPPoE message format	pppoeplus format { binary | ascii }	The system defaults to binary format
Restore the default PPPoE message format	undo pppoeplus format	

[Example]

! Configure the PPPoE Plus message format as ascii

```
[GPON]pppoeplusformatascii
```

33.2.5 Configuring the PPPoE Plus Message Separator

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Configure the PPPoE message format	pppoeplus delimiter { colon | dot | slash | space }	The system defaults to space
Restore the default PPPoE message separators	undo pppoeplus delimiter	

[Example]

! Configure the PPPoE Plus message separator to dot

[GPON]pppoeplusdelimiter dot

33.2.6 Configuring the PPPoE Plus Label Replacement Policy

The system supports configuring policies for handling PPPoE Plus messages received by the port, including discarding PPPoE Plus messages, keeping the original PPPoE Plus field, replacing the original PPPoE Plus field with the device's Tag, and transmitting PPPoE Plus messages, so please make the following configurations under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring the PPPoE Plus Label Replacement Policy	pppoeplus strategy { drop | keep | replace | transmit }	The default policy is transmit
Restore the default PPPoE Plus label replacement policy	undo pppoeplus strategy	

[Example]

! Configure the PPPoE Plus label replacement policy for Ethernet port 1 as keep

[GPON-ethernet-0/0/1]pppoeplus strategy keep

 Description:

When a port operates in transmit mode, the port receives a PPPoE packet and does not perform any software processing on the packet, but treats it as a normal Layer 2 packet and forwards it as a flooded packet within the VLAN to other ports, including Trust and Untrust ports.Trust and Untrust ports are defined in the description in 35.2.5.

33.2.7 Configure the PPPoE Plus port type

PPPoE port types include two types, Untrust ports and Trust ports. When a port works in untrust mode, if it receives a PPPoE message, it will only forward it to the Trust port. The system defaults all ports to be untrust ports, please do the following configuration under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the trust port type	pppoeplus trust	The system defaults to the untrust port
Close trust port type	undo pppoeplus trust	

[Example]

! Enabling Ethernet Port 1 as a PPPoE Plus Trust Port

[GPON-ethernet-0/0/1]pppoeplus trust

33.2.8 Configure a custom Circuit ID

The system supports the configuration of custom Circuit IDs. perform the following configurations in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num} | *interface-name* }	
Configuring a Custom Circuit ID	pppoeplus circuit-id *user-defined-string*	Custom characters can be configured in lengths ranging from 1-63
Remove custom Circuit IDs	undo pppoeplus circuit-id	

[Example]

! Enable the Circuit ID of Ethernet port 1 to be test

[GPON-ethernet-0/0/1]pppoeplus circuit-id test

 Description:

The system does not support customized Remote ID, Remote ID defaults to switch-mac

33.2.9 Configuring the Discard PPPoE Messages Function

The system supports the configuration of discarding PADI and PADO packets. When configured to discard packets, the port will discard the packets after receiving the corresponding packets, and the main function of this feature is to prevent PPPoE packets from entering the device from illegal ports, which will have an impact on the device. For example, the upstream PPPoE Trust port of the device, in general, only receives PADO or PADS messages sent by the PPPoE server, if the upstream port receives a PADI message at this time, it can be assumed that the message belongs to the illegal entry into the device, and you can configure the upstream Trust port to discard the PADI message to avoid the device from being affected by the impact of the illegal PADI message, perform the following configurations under port view. port view to perform the following configuration.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring the Discard PADI Messages Function	pppoeplus drop padi	
Remove the function of dropping PADI messages	undo pppoeplus drop padi	
Configuring the Discard PADO Message Function	pppoeplus drop pado	
Remove the function of dropping PADO messages	undo pppoeplus drop pado	

[Example]

! Enable Ethernet port 1 to drop the PADI function

[GPON-ethernet-0/0/1]pppoeplus trust

[GPON-ethernet-0/0/1] pppoeplus drop padi

 Description:

- Only Trust ports support configuration of the drop padi feature; untrust ports do not support configuration of drop padi;
- Only Untrust ports support configuration of the drop pado feature; trust ports do not support configuration of drop pado;

33.2.10 Show PPPoE Plus Configuration

You can view PPPoE Plus related configuration, including PPPoE message format type configuration, port type configuration, label replacement policy and other information under any attempt.

manipulate	command	clarification
Display PPPoE Plus configuration information	display pppoeplus interface [ethernet *interface-list*]	When no port number is specified, PPPoE plus configuration information for all ports is displayed

[Example]

! Display PPPoE Plus configuration information for Ethernet port 1

```
[GPON]display pppoeplus interface ethernet 0/0/1
```

Chapter 34 CFM Configuration

34.1 CFM Protocol Introduction

34.1.1 CFM Protocol Introduction

CFD stands for Connectivity Fault Detection, defined by the IEEE 802.1ag standard. It is an end-to-end VLAN-based OAM (Operations, Administration and Maintenance) mechanism on Layer 2 links, which is mainly used for detecting link connectivity, confirming faults and determining the location of faults in Layer 2 networks. The main functions include continuity detection, loopback, link tracing, alarm indication, and remote fault alarm.

34.1.2 CFM Basic Concepts

1. Maintenance domain MD

The Maintenance Domain (MD) specifies the network covered by connectivity error detection, and its boundaries are defined by a series of maintenance endpoints configured on ports. The Maintenance Domain is identified by a "Maintenance Domain Name". In order to accurately locate the point of failure, the concept of levels (hierarchies) is introduced in the maintenance domain. Maintenance domains are divided into eight levels, represented by integers 0-7, the larger the number, the higher the level, the larger the scope of the maintenance domain. Different maintenance domains can be adjacent or nested, but not cross, and nesting can only be nested from the high-level maintenance domain to the low-level maintenance domain, that is, the low-level maintenance domain must be included in the high-level maintenance domain.

2. Maintenance set MA

Multiple Maintenance Associations (MAs) can be configured within a maintenance domain, each of which is a collection of maintenance points within the maintenance domain. A maintenance association is identified by "maintenance domain name + maintenance association name". The maintenance set serves a VLAN, and the messages sent by the maintenance points in the maintenance set are tagged with the VLAN, while the maintenance points in the maintenance set can receive messages from other maintenance points in the maintenance set.

3. Maintenance point MP

Maintenance Point (MP) is configured on a port and belongs to a maintenance set, which can be categorized into Maintenance association End Point (MEP) and Maintenance association Intermediate Point (MIP). It can be categorized into Maintenance association End Point (MEP) and Maintenance association Intermediate Point (MIP). The Maintenance End Point MEP is identified by the MEP ID integer, which defines the scope and boundary of the maintenance domain. The MA and MD to which the maintenance endpoint belongs determine the VLAN attributes and level of messages sent from the maintenance endpoint. The maintenance intermediate point MIP is located inside the maintenance domain and cannot actively issue CFD protocol messages, but can process and respond to CFM protocol messages. The MA set and MD to which the maintenance intermediate point belongs determine the VLAN attributes and level of messages received by this maintenance intermediate point.

4. Maintenance of endpoint lists

The maintenance endpoint list is a collection of local maintenance endpoints allowed to be configured and remote maintenance endpoints to be monitored within the same maintenance set, which limits the selection range of maintenance endpoints within the maintenance set: all maintenance endpoints within the same maintenance set on different devices should be included in this list and the MEP IDs do not repeat each other. If a maintenance endpoint receives a CCM (Continuity Check Message) message from a remote device with a maintenance endpoint that is not in the list of maintenance endpoints in the same maintenance set, the message is discarded.

34.1.3 Introduction to CFM Functions

The effective application of connectivity error detection is based on proper network deployment and configuration. It is realized between the configured maintenance points and the main functions include:

- Continuity Check function (CC)

- Loopback function (LB)
- Linktrace function (LT)

1. Continuity detection function CC

The continuity detection function is used to detect the connectivity status between maintenance endpoints. Failure of connectivity can be caused by device failure or configuration error. This function is realized by the maintenance endpoint periodically sending a CCM message, which is a multicast message, and the other maintenance endpoints in the same maintenance set receive the message and thus know the status of the remote end. If the maintenance endpoint does not receive a CCM message from the remote maintenance endpoint within three times the CCM message sending period, it considers that there is a problem with the link and outputs a log report. When multiple maintenance endpoints in the maintenance domain are sending CCM messages, multi-point to multi-point link detection is realized.

2. Loopback function LB

The loopback function is similar to the ping function at the IP layer, which is used to verify the connection status between the local device and the remote device. This function is realized by sending LBM (Loopback Message) from the maintenance endpoint to the remote maintenance endpoint and checking the link status according to whether it can receive LBR (Loopback Reply) from the other end.LBM and LBR are unicast messages.

3. Link Trace Function LT

The link trace function is used to determine the path from the source to the target maintenance endpoint, which is realized by the following way: the source sends LTM (Linktrace Message) to the target maintenance endpoint, and the target maintenance endpoint and the maintenance intermediate point passed by the LTM will send LTR (Linktrace Reply) to the source according to the received LTR to determine the path to the target maintenance endpoint. When the target maintenance endpoint and the maintenance intermediate point through which the LTM passes receive this message, they will send LTR (Linktrace Reply) to the source, and the source determines the path to the target maintenance endpoint according to the LTR received.

34.2 CFM Functional Configuration

34.2.1 CFM Functional Configuration Task List

When enabling the CFM function you have to configure the domain before configuring other parameters. the list of main CFM configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Create/Delete Maintenance Domain MD	compulsory	34.2.2
Configuring Maintenance Domain MD Parameters	compulsory	34.2.3
Create/Delete Maintenance Set MA	compulsory	34.2.4
Configuring Maintenance Set MA Parameters	compulsory	34.2.5
Create/delete maintenance endpoint MEPs	compulsory	34.2.6
Create/Delete Remote Maintenance Endpoint RMEPs	compulsory	34.2.7
Create/Delete Maintenance Intermediate Point MIP	compulsory	34.2.8
CFM loopback detection	selectable	34.2.9
CFM Link Tracing	selectable	34.2.10
Monitoring and Maintenance of CFM	selectable	34.2.11

-

34.2.2 Create/Delete Maintenance Domain MD

In order to perform OAM management for operation-level Ethernet, you can divide the network into different maintenance

domains according to the requirements, and perform independent management and maintenance for each maintenance domain separately. different maintenance domains can be nested but not overlapped, and you can only configure up to 8 MDs for one device. please configure it under the system view.

manipulate	command	clarification
Go to System View	system-view	
Create an MD domain and go to the MD view	cfm md md-index	When there is no MD configuration, this command automatically creates an MD and enters MD domain view
Delete the MD domain	undo cfm md *md-index*	

[Example]

! Create an MD with index 1 and go to the MD view

[GPON]cfm md 1

34.2.3 Configuring Maintenance Domain MD Parameters

In order to distinguish between MDs, you can specify a different domain name for each MD. The domain name consists of two parts: the name format and the name content, and the domain name should preferably be unique across the network. In order to indicate the nesting relationship between MDs, you must also specify the level of the MDs, and only MDs with a large level can nest MDs with a small level. please configure it under cfm md view.

manipulate	command	clarification
Go to System View	system-view	
Go to the MD view	cfm md md-index	
Configure the airspace name MD	cfm md format none level *md-level*	When the configuration is not none, it means that the domain name of this MD is not specified
Configure the domain name and level of the MA and activate that MA	cfm md format { dns-name | mac-uint | string } name *md-name* level *md-level*	

[Parameter Description]

none: Indicates that the domain name of the MD is not specified.

dns-name: The domain name consists of a string and a 2-byte unsigned decimal integer value, e.g.: test-1

mac-uint: The domain name consists of the MAC address and a 2-byte unsigned decimal integer value, for example. 00:e1:4b:15:e5:1c-1

string: The domain name is a normal string, e.g.: test

md-name: MD name content, must be consistent with the name format

md-level: MD level, in the range 0-7

[Example]

! Specify the domain name of md 1 as test-3 and the level 3

[GPON-cfm-md-1]cfm md format dns-name name test-3 level 3

34.2.4 Create/Delete Maintenance Set MA

Multiple service instances can be configured in an MD according to the requirements. a service instance is a maintenance

set MA. the CFM performs connectivity fault detection for each MA separately. A maximum of 48 MAs can be configured in each MD and a device can be configured with a maximum of 48 MAs. please configure it under cfm md view.

manipulate	command	clarification
Go to System View	system-view	
Go to the MD view	cfm md md-index	
Create an MA set and go to the MA view	cfm ma ma-index	When no MA is configured, this command automatically creates an MD and enters MA view
Deleting the MA Set Configuration	undo cfm ma *ma-index*	

[Example]

! Configure the MA with index 1 within MD 1 and enter the MA view

[GPON-cfm-md-1]cfm ma 1

34.2.5 Configuring Maintenance Set MA Parameters

In order to distinguish the MAs in each MD, you can assign a different instance name to each MA. The instance name consists of two parts: the name format and the name content, and the domain name plus the instance name of this MA must be guaranteed to be unique in the whole network. Please configure it under cfm ma view.

manipulate	command	clarification
Go to System View	system-view	
Go to the MD view	cfm md md-index	
Go to the MA view	cfm ma ma-index	
Configure the instance name and associated VLAN of the MA and activate this MA	cfm ma format { primary-vid | string | uint16 | vpn-id } name *ma-name* primary-vlan *vlan-id*	
Configure the intra-MA CCM message sending interval	cfm cc interval { 1 | 10 | 60 | 600 }	Unit is second, default is 1S
Restore the default CCM message sending interval	undo cfm cc interval	

[Parameter Description]

primary-vid: The instance name is a VLAN ID that can be specified as the primary associated VLAN for the MA, in the range 1-4094

string:The instance name is a normal string, e.g.: test

uint16: instance name is a 2-byte unsigned decimal integer value, e.g.: 65535

vpn-id: The instance name consists of a 3-byte OUI and a 4-byte unsigned shaped value in hexadecimal, e.g.:00E14B00112233

ma-name: MA name content, must be consistent with the name format

vlan-id: Primary VLAN associated with the MA, in the range 1-4094

[Example]

! Specify the instance name of ma 1 of md 1 as test and the associated VLAN as 3

[GPON-cfm-md-1-ma-1]cfm ma format string name test primary-vlan 3

! Specify the ma 10ccm send interval for md 1 as 10s

[GPON-cfm-md-1-ma-1]cfm cc interval 10

34.2.6 Create/delete maintenance endpoint MEPs

The points in an MD that participate in OAM computation are called maintenance point MPs, and MPs are categorized into MEPs and MIPs based on their location; MEPs are boundary points of MDs and are capable of initiating and terminating OAM frames used for fault management and performance monitoring, and MIPs are capable of responding to only certain OAM frames, but do not initiate OAM frames. Throughout the MA, MEPs other than local are locally called RMEPs (Remote Maintenance End Points). A maximum of 255 MPs (including MEP/MIP/RMEP) can be configured in each MA. a device can be configured with a maximum of 255 MPs. please configure it under cfm ma view.

manipulate	command	clarification
Go to System View	system-view	
Go to the MD view	cfm md md-index	
Go to the MA view	cfm ma ma-index	
Create the MEP and specify the direction, associated VLAN, and associated port of the MEP	cfm mep *mep-id* direction { up | down } [primary-vlan *vlan-id*] interface ethernet *interface-num*	
Delete MEP Configuration	undo cfm mep *mep-id*	
Enable MEP management state	cfm mep *mep-id* state { enable | disable }	
Enable the CCM message sending function of the MEP	cfm mep *mep-id* cc { enable | disable }	
Configure the MEP to send CCM/LTM priority	cfm mep mep-id priority priority-id	Priority range 0-7, default value 0
Restore the priority of the MEP to send CCM/LTs	undo cfm mep *mep-id* priority	

[Parameter Description]

mep-id: mep identifier, all mep identifiers cannot be duplicated in an MA, range 1-8191

mep in the up:up direction, which must be connected to other MPs through a port other than this one

down: mep in the down direction that connects directly to other MPs through the port it is on

vlan-id: mep-associated VLAN, if no VLAN is specified, the primary associated VLAN of the MA in which the mep is located is directly used.

interface-num: port on which the mep is located, in the range of all available ports on the device

Note that you need to configure configure primary-vlan before you can configure MEP, please refer to 34.2.5 for primary-vlan related configuration.

[Example]

! Create mep in md 1 ma 1 with id 1 direction down port 1

```
[GPON-cfm-md-1-ma-1]cfm mep 1 direction down interface ethernet 0/0/1
```

34.2.7 Create/Delete Remote Maintenance Endpoint RMEPs

Please perform RMEP configuration under cfm ma view.

manipulate	command	clarification
Go to System View	system-view	
Go to the MD view	cfm md md-index	
Go to the MA view	cfm ma ma-index	

Creates an RMEP and specifies the associated MEPs	cfm rmep rmep-id mep mep-id	
Delete RMEP	undo cfm rmep *rmep-id*	

[Parameter Description]

rmep-id: rmep identifier, specifies the identifier of the mep other than the local mep in the MA where it is located, range 1-8191

mep-id: mep identifier, specified as the identifier of the local mep in the host MA, in the range 1-8191

[Example]

! Create rmep with id 2 in md 1 ma 1 and associate to mep 1

```
[GPON-cfm-md-1-ma-1]cfm rmep 2 mep 1
```

34.2.8 Create/Delete Maintenance Intermediate Point MIP

Please perform MIP configuration under cfm ma view.

manipulate	command	clarification
Go to System View	system-view	
Go to MD view	cfm md md-index	
Go to the MA view	cfm ma ma-index	
Create a MIP and specify the associated port	cfm mip *mip-id* interface ethernet *interface-num*	
Delete MIP	undo cfm mip *mip-id*	

[Parameter Description]

mip-id: mip identifier, specified as the identifier of the local mip in the host MA, in the range of 1-8191

interface-num: port on which the mip is located, in the range of all available ports on the device

[Example]

! Create mip with id 1 port 1 in md 1 ma 1

```
[GPON-cfm-md-1-ma-1]cfm mip 1 interface ethernet 0/0/1
```

34.2.9 CFM loopback detection

The cfm loopback function is mainly used to check whether the network connection and the destination mac address are reachable. Please do the following in cfm ma configuration mode.

manipulate	command	clarification
Go to System View	system-view	
Go to the MD view	cfm md md-index	
Go to the MA view	cfm ma ma-index	
CFM loopback detection	cfm loopback mep *mep-id* { dst-mac *mac-address* | dst-mep *rmep-id* } [priority *pri-id* | count *pkt-num* | length *data-len* | data *pkt-data*]	

[Parameter Description]

mep-id: mep identifier, specified as the mep that performed the cfm loopback operation, in the range 1-8191

mac-address: destination MAC address, specified as the MAC address of the remote mep or mip

rmep-id: target mep identifier, specified as the remote mep, range 1-8191

pri-id: Priority for sending loopback messages, range is 0-7, default value is 0

pkt-num: number of ringback messages sent, range is 1-1024, default value is 5

data-len: The length of the transmit ring return, the range is 1-1500 bytes, the default value is 0.

pkt-data: data content of the send ring return, length 1-400 characters, default value is empty

Note: You need to configure the MEP before you can perform this operation.

[Example]

! Detect whether mep 1 to mep 2 is reachable in md 1 ma 1

[GPON-cfm-md-1-ma-1]cfm loopback mep 1 dst-mep 2

! Detecting if mep 1 to 00:E1:4B:15:E5:1C is reachable in md 1 ma 1

[GPON-cfm-md-1-ma-1]cfm loopback mep 1 dst-mac00:E1:4B:15:E5:1C

34.2.10 CFM Link Tracing

The cfm linktrace function is mainly used for link tracing and checking network connections. Please do the following in cfm ma view.

manipulate	command	clarification
Go to System View	system-view	
Go to the MD view	cfm md md-index	
Go to the MA view	cfm ma ma-index	
CFM Link Tracing	cfm linktrace mep *mep-id* { dst-mac *mac-address* | dst-mep *rmep-id* } [timeout *pkt-time* | ttl *pkt-ttl* | flag { use-mpdb | unuse-mpdb }]	

[Parameter Description]

mep-id: mep identifier, specified as the mep that performed the cfm link trace operation, in the range 1-8191

mac-address: destination MAC address, specified as the MAC address of the remote mep or mip

rmep-id: target mep identifier, specified as the remote mep, range 1-8191

pkt-time: timeout for waiting for a response after sending a message, range is 3-60s, default value is 5s

pkt-ttl: Initial ttl value for sending message, range is 1-255, default value is 64

use-mpdb: Forwarding message identifier, indicates the use of CCM database for forwarding messages, first look up the MAC address table, and then look up the CCM database if it cannot be found.

unuse-mpdb: Forwarding message identifier, indicates that the CCM database will not be used for the forwarding operation of the message, and will only look up the

MAC address table

Note: You need to configure the MEP before you can perform this operation.

[Example]

! View the network connection between mep 1 to mep 2 in md 1 ma 1

[GPON-cfm-md-1-ma-1]cfm linktrace mep 1 dst-mep 2

! Viewing network connections from mep 1 to 00:E1:4B:15:E5:1C in md 1 ma 1

[GPON-cfm-md-10-ma-10]cfm linktrace mep 1 dst-mac00:E1:4B:15:E5:1C

34.2.11 Monitoring and Maintenance of CFM

CFM-related configuration and maintenance information can be viewed under any attempt.

manipulate	command	clarification

Display maintenance domain MD information	display cfm md [*md-index*]	The display includes: MD name, MD level, and MD activation status. If index is not specified, all MDs are displayed.
Display Maintenance Set MA information	display cfm ma	The display includes: the MD where the MA is located, the MA name, the primary VLAN associated with the MA, the CCM transmission interval of the MA, the MA activation status
Display local maintenance point MP (MEP/MIP/RMEP) information	display cfm mp local	The display includes: MD and MA where the MP is located, MP identification, MP type, MP direction, MP associated port, MP management enable status, MP CCM transmit enable status, and the priority used by the MP to send messages.
Display remote maintenance point MP information	display cfm mp remote	The display includes the MD and MA where the rmep is located, the rmep identifier, the rmep's associated mep, the rmep's MAC address, the rmep's incoming port, and the rmep's aging time
Displaying CCM Statistics	display cfm cc	The display reads: number of messages sent ccm
Clearing CCM Statistics	clear cfm cc	
Displaying CCM database information	display cfm cc database	Displayed: mac address, vlan-id, incoming port
Clearing CCM database information	clear cfm cc database	
Displaying CFM Fault Alarm Messages	display cfm errors	The display shows: the MD and MA where the faulty maintenance point is located, the faulty maintenance point identification, the type of the faulty maintenance point, the mac address of the faulty maintenance point, and the cause of the fault

[Example]

! Display all maintenance association information

[GPON]display cfm md

[GPON]display cfm ma

! Displays information about all local maintenance points

[GPON] display cfm mp local

! Displays information about all maintenance points at the remote end

[GPON] display cfm mp remote

! Display CCM message statistics

[GPON]display cfm cc

! Clear CCM message statistics

[GPON]clear cfm cc

! Display all maintenance point database information

[GPON] display cfm cc database

! Display all fault messages

[GPON] display cfm errors

Chapter 35 EFM Configuration

35.1 Introduction to the EFM Protocol

35.1.1 Introduction to the EFM Protocol

EFM (Ethernet of first mile), defined by the IEEE 802.3ah standard, is mainly used to solve the OAM problem of the "last mile" Ethernet connection, which is used to monitor the link connection status between two directly connected devices, test the link performance, and manage and maintain the point-to-point Ethernet link. It is used to monitor the link status between two directly connected devices, test the link performance, and manage and maintain the point-to-point Ethernet link.

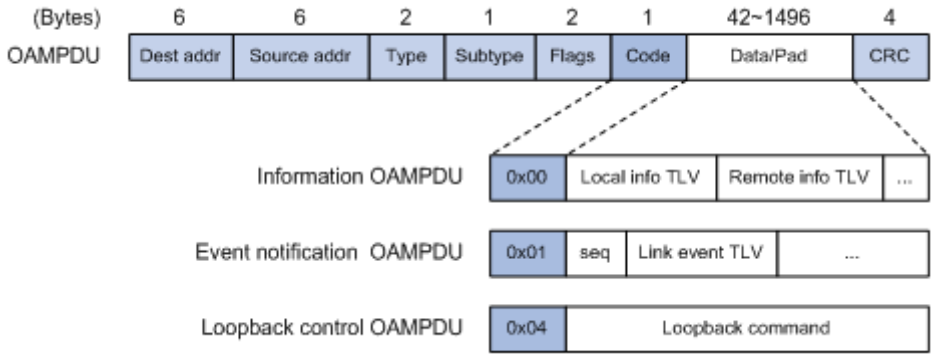
EFM contains five main functions: OAM node discovery function, remote fault notification function, OAM remote loopback function, OAM link monitoring function, and remote MIB variable access function.

35.1.2 EFM Basic Concepts

1. EFM protocol messages

EFM OAM works at the data link layer, and its protocol messages are called OAMPDUs (OAM Protocol Data Units).EFM OAM is to report the link status through the timed interaction of OAMPDUs between devices, so that network administrators can manage the network effectively.

The OAMPDU message format is shown below:



The meaning of OAMPDU important fields is shown in the table below:

field	hidden meaning
Dest addr	Destination MAC address, for the slow protocol multicast address: 01:80:C2:00:00:02. The characteristic of the slow protocol message is that it cannot be forwarded by the bridge, so regardless of whether the OAM function is available or whether the OAM function is activated or not, the EFM OAM message cannot be forwarded across multiple hops
Source addr	Source MAC address, the MAC address of the sender's interface
Type	Protocol type for 0x8809
Subtype	Protocol subtype for 0x03
Flags	Flag field containing status information about the EFM OAM entity
Code	Message encoding, different values indicate different types of OAMPDUs, common OAMPDUs are shown in Table 35-2

Common OAMPDUs are listed below:

Code value	message type	hidden meaning	corresponds English -ity, -ism, -ization

0x00	Information OAMPDU	The message OAMPDU, also known as a heartbeat message	Used to send status information (including local, remote, and customized information) of an OAM entity to a remote OAM entity to maintain Ethernet OAM connectivity
0x01	Event Notification OAMPDU	Event Notification OAMPDU	Typically used for link monitoring to alert on faults occurring on the link connecting the local and remote OAM entities
0x04	Loopback Control OAMPDU	Loopback control OAMPDU	Mainly used for remote loopback control, used to control the OAM loopback state of the remote device, the message with the information to enable or de-enable the loopback function, according to the information to enable or disable the remote loopback function

2. Connectivity model

There are two types of EFM OAM connection modes: active mode and passive mode.An EFM OAM connection can only be initiated by an OAM entity in active mode, while an OAM entity in passive mode can only wait for a connection request from a remote OAM entity. An EFM OAM connection cannot be established between two OAM entities that are also in passive mode. The following are the EFM processing capabilities of the device in active and passive modes:

processing capability	active mode	passive mode
Initializing the EFM OAM Discovery Process	can	may not
Response to the EFM OAM Discovery initialization process	can	can
Send Information OAMPDU	can	can
Send Event Notification OAMPDU	can	can
Sending Information OAMPDUs that do not carry TLVs	can	can
Send Loopback Control OAMPDU	can	may not
Response to Loopback Control OAMPDUs	Yes, but requires the remote end to be in active mode	can

3. Link events

The link events defined in the EFM OAM are divided into two categories: general link events for link performance monitoring and emergency link events for remote fault detection, and contain the types shown in the following table:

General Link Events:

Event Type	Event Description
Error Symbol Event (Errored Symbol Event)	A set number of signals are received as the detection window, and an error signal event is generated if the number of error signals detected within the window reaches or exceeds the detection threshold.
Error Frame Event (Errored Frame Event)	A set time is used as the detection window, and an error frame event is generated if the number of detected error frames within the window reaches or exceeds the detection threshold.
Errored Frame Period Event (EFPE)	A set number of frames are received as the detection window, and if the number of error frames detected during the window reaches or exceeds the detection threshold, an error frame cycle event is generated.
Errored Frame Seconds Event (Errored Frame Seconds Event)	A set time is used as the detection window, and an error frame second event is generated if the number of error frame seconds (at least one error frame is detected in a given second, and that second is called an error frame second) detected during the window reaches or exceeds the detection threshold.

Emergency Link Incident:

Event Type	Event Description	OAMPDU Transmission Frequency
Link Fault	Loss of remote link signal	Sends once per second
Dying Gasp	Unpredictable state occurrences, such as power interruptions	uninterrupted transmission
Critical Event	Uncertainty about the occurrence of an emergency	uninterrupted transmission

35.1.3 EFM Operational Mechanism

1. EFM OAM connection establishment

The realization of EFM OAM functionality is based on EFM OAM connectivity, and the process of establishing EFM OAM connectivity is also known as the Discovery phase, i.e., the process by which the local OAM entity discovers the remote OAM entity and establishes a stable dialogue with it.

When the EFM OAM function is enabled on an interface of the device, an EFM OAM connection is initiated from that interface to the remote end if the EFM OAM operating mode of that interface is active. During the process of establishing an EFM OAM connection, the connected OAM entities communicate their respective EFM OAM configuration information through interactive Information OAMPDUs. When the OAM entity receives the configuration parameters from the remote end, it decides whether to establish an EFM OAM connection. If the EFM OAM configurations of both sides match, the EFM OAM connection is established.After the EFM OAM connection is established, the OAM entities at both ends send Information OAMPDUs periodically to check whether the connection is normal. If one OAM entity does not receive an Information OAMPDU from the remote end within the connection timeout period, the EFM OAM connection is considered broken.

2. Link performance monitoring

When one end OAM entity monitors a general link event, it will send Event Notification OAMPDU to its remote OAM entity for notification, and at the same time, it will record the monitoring information in the log and report it to the network management system; when the remote OAM entity receives the information, it will also record it in the log and report it to the network management system. In this way, the administrator can dynamically grasp the status of the network by observing the log information.

3. Remote fault detection

When an emergency link event occurs on the device and causes traffic interruption, the OAM entity at the fault end notifies the fault information (that is, the type of emergency link event) to the remote OAM entity through the Flag field in the Information OAMPDU, and at the same time enters the fault information into the logs and reports it to the network management system; after the remote OAM entity receives the information, it also enters it into the logs and reports it to the network management The remote OAM entity receives the information and also logs it and reports it to the network management system. In this way, the administrator can dynamically understand the link status by observing the log information and handle the corresponding errors in time.

4. Remote loopback

The far-end loopback function means that when an OAM entity in active mode sends all other messages except OAMPDUs to the far-end, the far-end receives the messages and does not forward them according to their destination addresses, but returns them to the home end in the original way. It can be used to locate link faults and detect link quality: by observing the return of non-OAMPDU messages, network administrators can judge link performance (including packet loss rate, delay, jitter, etc.).

35.2 EFM Functional Configuration

35.2.1 EFM Function Configuration Task List

The point-to-point Ethernet link between two points can be managed and maintained after the EFM function is enabled. the

list of main EFM configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable EFM function	compulsory	35.2.2
Configure the port's EFM operating mode	compulsory	35.2.3
Configuring the EFM Discovery Cycle	selectable	35.2.4
Configure the timeout for EFM discovery	selectable	35.2.5
Configuring the EFM Response Timeout	selectable	35.2.6
Configuring Link Monitor Event Parameters	selectable	35.2.7
Enable/disable remote failure indication	selectable	35.2.8
Enable/disable the link monitoring function	selectable	35.2.9
Enable/disable remote MIB variable fetch function	selectable	35.2.10
Enable/disable remote loopback function	selectable	35.2.11
Enable/disable remote loopback	selectable	35.2.12
Configure whether to process remote loopback request messages	selectable	35.2.13
EFM Monitoring and Maintenance	selectable	35.2.14

-

35.2.2 Enable/disable EFM function

Please perform EFM switch configuration in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable EFM function	efm	EFM is disabled by default
Disabling the EFM function	undo efm	

[Example]

! Enabling EFM on Ethernet Port 1

[GPON-ethernet-0/0/1]efm

35.2.3 Configure the port's EFM operating mode

Please configure the EFM operating mode in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring the EFM Operating Mode	efm mode { passive | active }	Active mode by default
Disabling the EFM function	undo efm	

[Parameter Description]

passive: passive mode

active: active mode

[Example]

! Configure the EFM operating mode of Ethernet port 1 to passive mode

[GPON-ethernet-0/0/1]efm mode passive

35.2.4 Configuring the EFM Discovery Cycle

Configure the discovery period of EFM, during which at least one OAMPDU information message must be sent. Please configure it in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring the EFM Discovery Cycle	efm pdu-timeout *time-out*	The default discovery period is 1S
Restore the default EFM discovery cycle time configuration	undo efm pdu-timeout	

[Parameter Description]

time-out: EFM discovery period in seconds, the range is 1-60s, the default value is 1s, and the value cannot be greater than 1/3 of the EFM discovery timeout.

[Example]

! Configure the EFM discovery period for Ethernet port 1 to 5 seconds

[GPON-ethernet-0/0/1]efm pdu-timeout 5

35.2.5 Configure the timeout for EFM discovery

Configure the timeout period for EFM discovery, which will restart the EFM discovery process when the timeout period expires. Please configure it in port configuration mode.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring the EFM Discovery Timeout	efm link-timeout *time-out*	The default timeout is 5S
Restore the default EFM discovery timeout period	undo efm link-timeout	

[Parameter Description]

time-out: timeout for EFM discovery, in seconds, in the range of 3-300s, the default value is 5s, and the value cannot be less than three times the EFM discovery period.

[Example]

! Configure the timeout for EFM discovery on Ethernet port 1 to 20 seconds

[GPON-ethernet-0/0/1]efm link-timeout 20

35.2.6 Configuring the EFM Response Timeout

Configure the timeout time for the remote end to respond to OAMPDU request messages, and discard the OAMPDU response messages received after the timeout if the response is timeout. Please configure it under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the remote end's response timeout for OAMPDUs	efm remote-response-timeout *time-out*	The default response timeout is 2S
Restore the default remote response timeout for OAMPDUs	undo efm remote-response-timeout	

[Parameter Description]

time-out: response timeout in seconds, range is 1-10s, default value is 2s.

[Example]

! Configure the timeout for Ethernet large port 1 to respond to remote OAMPDU packets to 5 seconds

```
[GPON-ethernet-0/0/1]efm remote-response-timeout 5
```

35.2.7 Configuring Link Monitor Event Parameters

Please perform the following link monitoring event parameter configuration in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring the window parameter for the errored-symbol-period event	efm link-monitor errored-symbol-period window high *win-hi-value* low *win-lo-value*	window：表示接收的symbol数（长度为8字节），范围：1-0xffffffffffffffff，缺省为10000，win-hi-value和win-lo-value分别表示高4字节和低4字节
Configuring the threshold parameter for errored-symbol-period events	efm link-monitor errored-symbol-period threshold high *th-hi-value* low *th-lo-value*	threshold：表示接收的错误symbol数（长度为8字节），范围：1-0xffffffffffffffff，缺省值为1，th-hi-value和th-lo-value分别表示高4字节和低4字节
Configuring the window parameter for the errored-frame event	efm link-monitor errored-frame window *win-value*	win-value: indicates the receive time, range: 10-600ms, default is 100ms
Configuring the threshold parameter for errored-frame events	efm link-monitor errored-frame threshold *th-value*	th-value: indicates the number of received error frames, range: 1-0xffffffff, default value is 1
Configuring the window parameter for the errored-frame-period event	efm link-monitor errored-frame-period window *win-value*	win-value: Indicates the number of frames received, range: 1-0xffffffff, default is 10000
Configuring the threshold parameter for the errored-	efm link-monitor errored-frame-period threshold *th-value*	th-value: indicates the number of received error frames, range: 1-0xffffffff, default value is 1

frame-period event		
Configuring the window parameter for the errored-frame-seconds event	efm link-monitor errored-frame-seconds window *win-value*	win-value: indicates the receive time, range: 100-9000ms, default is 100ms
Configuring the threshold parameter for the errored-frame-seconds event	efm link-monitor errored-frame-seconds threshold *th-value*	th-value: indicates the number of seconds of error received, range: 1-900, default value is 1
Restore the link monitoring event window parameter to its default value	undo efm link-monitor { errored-symbol-period | errored-frame | errored-frame-period | errored-frame-seconds } window	
Restore the link monitoring event threshold parameter to the default value	undo efm link-monitor { errored-symbol-period | errored-frame | errored-frame-period | errored-frame-seconds } threshold	

[Parameter Description]

The relevant parameter descriptions are described in the description section of the table above.

[Example]

! Configure the window parameter of the errored-frame event on Ethernet port 1 to 200

```
[GPON-ethernet-0/0/1]efm link-monitor errored-frame window 200
```

35.2.8 Enable/disable remote failure indication

Configure whether the EFM Remote Failure Indication function of the port is enabled or not. which is used to monitor whether an EFM emergency connection event occurs on the device. Please perform the following configurations under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable remote failure indication	efm remote-failure { link-fault | dying-gasp | critical-event }	By default, this feature is turned off
Disable remote failure indication	undo efm remote-failure { link-fault | dying-gasp | critical-event }	

[Parameter Description]

link-fault: indicates that a fault was detected in the local receive direction

dying-gasp: no detection method defined yet

critical-event: no detection method defined yet

[Example]

! Enable the link-fault function on Ethernet port 1

```
[GPON-ethernet-0/0/1]efm remote-failure link-fault
```

35.2.9 Enable/disable the link monitoring function

Configure whether the EFM link monitoring function of the port is enabled or not, which is used to monitor the link status in real time and generate an EFM general event when the link is abnormal. Please perform the following configurations under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable link monitoring	efm link-monitor { errored-symbol-period | errored-frame | errored-frame-period | errored-frame-seconds }	Enable link monitoring by default
Disable link monitoring	undo efm link-monitor { errored-symbol-period | errored-frame | errored-frame-period | errored-frame-seconds }	

[Parameter Description]

errored-symbol-period: number of errored symbols in the last N symbols exceeds the threshold

errored-frames: number of errored frames over a certain period of time exceeds the threshold

errored-frame-period: number of errored frames in the last N frames exceeds the threshold

errored-frame-seconds:Number of errored seconds (at least one errored frame in a second) in the last M seconds exceeds the threshold

[Example]

! Enable errored-frame monitoring on Ethernet port 1

```
[GPON-ethernet-0/0/1]efm link-monitor errored-frame
```

35.2.10 Enable/disable remote MIB variable fetch function

Configure whether the EFM remote MIB variable acquisition function of the port is enabled or not, which is used to query the remote MIB variable value. Please perform the following configurations under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable remote MIB variable fetching	efmvariable-retrieval	Default function on
Disable remote MIB variable acquisition	undo efmvariable-retrieval	

[Example]

! Disable remote MIB variable acquisition on Ethernet port 1

```
[GPON-ethernet-0/0/1]undo efm variable-retrieval
```

35.2.11 Enable/disable remote loopback function

Configure whether the EFM remote loopback function of the port is enabled, which is used to detect whether the link state is normal. Please perform the following configurations under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	

Enable Remote Loopback	efm remote-loopback	Default function off
Disable Remote Loopback	undo efm remote-loopback	

[Example]

! Enable remote loopback on Ethernet port 1

[GPON-ethernet-0/0/1]undo efm remote-loopback

35.2.12 Enable/disable remote loopback

To enable/disable the remote loopback function of the corresponding port of the remote device, perform the following configuration under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable/disable remote loopback function	efm remote-loopback { start | stop }	

[Parameter Description]

start: Enable remote loopback, after executing start, the port starts remote loopback.

stop: stop remote loopback, after executing stop, the port stops remote loopback.

[Example]

! Enable remote loopback on Ethernet port 1

[GPON-ethernet-0/0/1]efm remote-loopback start

35.2.13 Configure the processing policy for remote loopback request messages

Configure whether the port handles (ignores/processes) incoming far-end loopback request OAMPDUs. perform the following configuration under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configure the processing policy for remote loopback request messages	efm remote-loopback { ignore | process }	The default processing strategy is ignore

[Parameter Description]

ignore: ignore processing

process: processing

[Example]

! Configure the Ethernet port 1 far-end loopback request message processing policy to Process

[GPON-ethernet-0/0/1]efm remote-loopback process

35.2.14 EFM Monitoring and Maintenance

EFM configuration and operation information can be displayed at any attempt.

manipulate	command	clarification
Display EFM protocol operation information	display efm status interface [ethernet *interface-num*]	When the port number is not specified, the EFM operation information of all ports is displayed, and the display includes: EFM on status, EFM operation mode, remote failure indication function on status, link monitoring function on status, and parameter configuration of link monitoring events.
Display EFM summary information	display efm summary	The display includes: remote MAC address, remote OUI, local EFM operating mode, local EFM capability, local remote loopback status
Displaying EFM Discovery Information	display efm discovery interface [ethernet *interface-num]*	The display includes: local EFM operating mode, local EFM capability, maximum OAMPDU length supported by the local end, local port operation status, local port loopback status, current status of the local EFM discovery state machine, local OAMPDU revision value, remote MAC address, remote Vendor identification, remote OUI, remote OAMPDU revision value, far-end EFM operating mode, far-end EFM capability, maximum OAMPDU length supported by the far-end
Displaying EFM Statistics	display efm statistics interface [ethernet *interface-num*]	The display includes the number of OAMPDUs received and sent at the local end, the number of remote failure indication events generated at the local and remote ends, and the number of general link monitoring events generated at the local and remote ends.
Clearing EFM Statistics	clear efm statisticsinterface [ethernet *interface-num*]	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Remote MIB variable lookup for a port	display efm port *interface-list* remote-mib { phyadminstate | autonegadminstate }	Viewed in port attempt mode. phyadminstate: the enable state of the port. autonegadminstate: self-negotiation enable state of the port.
Global remote MIB variable lookup	display efm remote-mib { fecability | fecmode }	Viewed in port attempt mode. fecability: FEC (Forward Error Correction) capability. fecmode: FEC (Forward Error Correction) mode.

[Example

! Display the protocol running status of all ports

[GPON]display efm status interface

! Display EFM summary information

[GPON]display efm summary

! Display EFM discovery information for all ports

[GPON]display efm discovery interface

! Display EFM statistics for all ports

[GPON]display efm statistics interface

! Displays the enable status of Ethernet port 1

[GPON-ethernet-0/0/1]display efm port 1 remote-mibhyadminstate

Chapter 36 ERRP Configuration

36.1 Introduction to the ERRP Protocol

36.1.1 Introduction to the ERRP Protocol

ERRP (Ethernet Redundant Ring Protocol) The ERRP protocol is a link-layer protocol specifically applied to Ethernet rings that prevents broadcast storms on the ring and features fast convergence of link downtime.

In Layer 2 networks, the Spanning Tree (STP) protocol is generally used to protect the topology of the network. The STP protocol family has been standardized by the IEEE, and the main protocols include STP, RSTP, and MSTP. STP was originally invented to avoid the formation of loops in the network, which could lead to unavailability of the network due to broadcast storms, but it does not impose very high requirements on the convergence time of the network when there is a change in the topology. convergence time when there is a topology change in the network, but STP does not impose high requirements on the service convergence time. STP protocol is used as topology protection network, service convergence time in tens of seconds of order of magnitude, RSTP STP protocol has been improved, service convergence time can be controlled in seconds, and the MSTP protocol is mainly a multi-instantiation of the RSTP supplement, service convergence time is basically the same as RSTP.

With the rapid development of Ethernet technology in enterprise LAN networks and carrier metro networks, especially under the trend of convergence of data, voice, video and other services to IP, enhancing Ethernet reliability, shortening the network failure convergence time, and providing a satisfactory user experience for voice services, video and other services have become a basic requirement, both for the carrier's customers and the majority of enterprise users.

In order to shorten the convergence time and eliminate the effect of network size, the ERRP protocol was created.ERRP is a link-layer protocol specialized for Ethernet rings that prevents broadcast storms caused by data loops in an Ethernet ring. When a link on an Ethernet ring is broken, a backup link can be quickly enabled to restore the communication path between nodes on the ring. Compared with STP protocol, ERRP protocol is characterized by fast topology convergence (less than 50ms) and the convergence time is independent of the number of nodes on the ring.

36.1.2 ERRP Basic Concepts

1. ERRP Domain (ERRP)

An ERRP domain is identified by an ID represented by an integer. A group of devices configured with the same domain ID and control VLAN and interconnected constitute an ERRP domain.

2. ERRP Ring (ERRP Ring)

An ERRP ring corresponds to a physical ring-connected Ethernet topology. Each ERRP domain consists of multiple ERRP rings connected to each other, with one ring being the primary ring and the others being subrings. Of course, an ERRP domain can also contain only one ERRP ring. In the case of a single ring, the ERRP ring can be either a primary ring or a subring, with the same effect on the application. the role of the ERRP ring is determined by user configuration.

3. ERRP control VLAN

Each ERRP domain has two control VLANs, called the master control VLAN and the subcontrol VLAN. protocol messages for the master ring are propagated in the master control VLAN, and protocol messages for the subring are propagated in the subcontrol VLAN.

4. Master nodes

The master node is the main decision and control node on the ERRP ring. There must and can only be one master node on each ERRP ring.

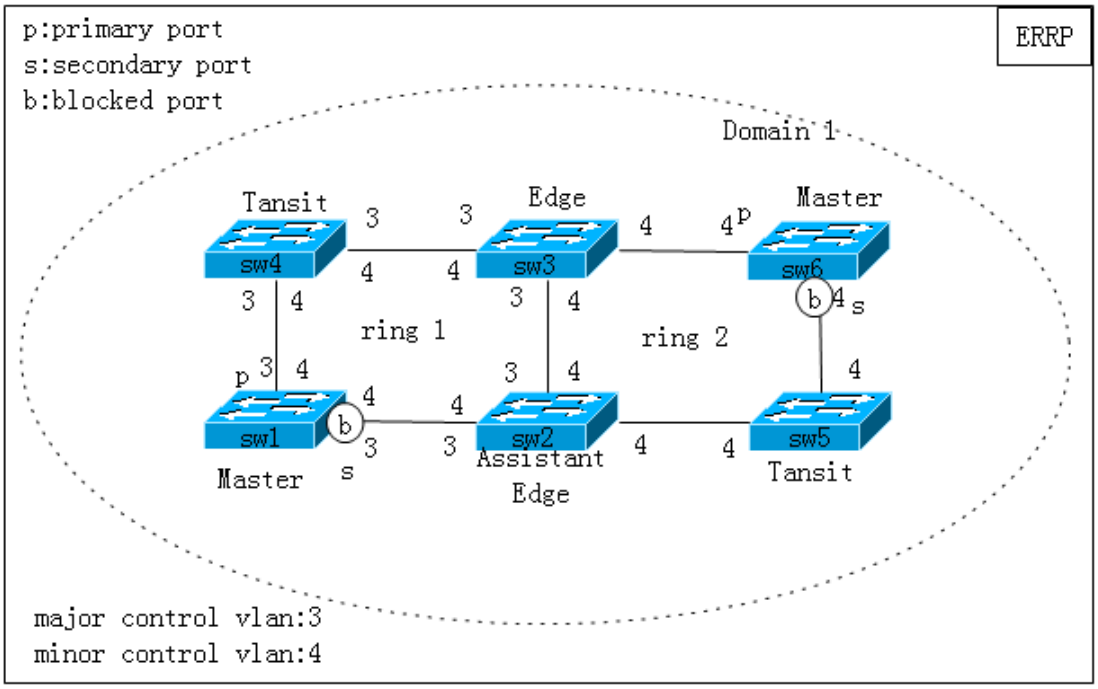
5. Transmission nodes (Tansit)

All nodes on the ring other than the master node can be called transmission nodes (edge nodes and auxiliary edge nodes are actually special transmission nodes). An ERRP ring can have multiple transmission nodes or no transmission nodes.

6. Edge nodes and auxiliary edge nodes

When two rings intersect there must be two intersection points. Similarly, the subring and the main ring will have two intersections, and one of the switches at these two intersections is called an edge node and the other is called an auxiliary edge node. There is no special requirement for which device to be configured as an edge node or auxiliary edge node, as long as the configuration can distinguish between the two nodes.

As shown in the following figure Domain 1 is an ERRP domain, and all devices from S1~S6 belong to Domain 1. The master control VLAN and subcontrol VLAN of Domain 1 are VLAN3 and VLAN4, respectively, and the domain contains two ERRP rings, Ring 1 and Ring 2, respectively. the master node of the master ring is S1, and the master node of the subring is S6. S2 , S3, and S4 are the transmission nodes of the primary ring, and S5 is the transmission node of the subring. The edge nodes and auxiliary edge nodes of the subring are S3 and S2, respectively.



36.1.3 ERRP Protocol Principles

The basic working principle of ERRP is that multiple devices are connected in series to form a ring to provide link redundancy, a master device is responsible for detecting/maintaining the health of the ring, the master device provides redundant ports, and when the ring fails, the master device releases the redundant ports to keep the service flowing. Due to its simplicity and small computation, it converges faster than STP protocol.

1. ERRP protocol basics

--All nodes on each domain are configured with the same ERRP domain ID and control VLANs

--Each domain has two control VLANs, the primary control VLAN and the subcontrol VLANs

--Master ring protocol messages are propagated in the master control VLAN and subring protocol messages are propagated in the subcontrol VLANs

--ERRP ports on the primary ring point join both the primary control VLAN and the subcontrol VLAN, and ERRP ports on the subring join the subcontrol VLANs

--Protocol messages of the subring are treated as data messages in the main ring, and synchronized blocking/releasing with data messages is achieved.

2. Polling mechanism

The Polling mechanism is a mechanism for the master node of an ERRP ring to actively detect the health status of the ring

network. The master node periodically sends HELLO messages from its master port, which are propagated through each transmission node on the ring in turn. If the master node can receive its own HELLO message from the secondary port, it indicates that the ring link is complete; otherwise, if the HELLO message cannot be received within the specified time, it is considered that the ring network has a link failure.

A master node in the Fault state receives a HELLO message from the secondary port from itself, immediately migrates to the Health state, blocks the secondary port and refreshes the FDB, and also sends a COMPLETE_FLUSH_FDB message from the master port to notify all transport nodes of the release of the temporary blocking port and the refreshing of the FDB.

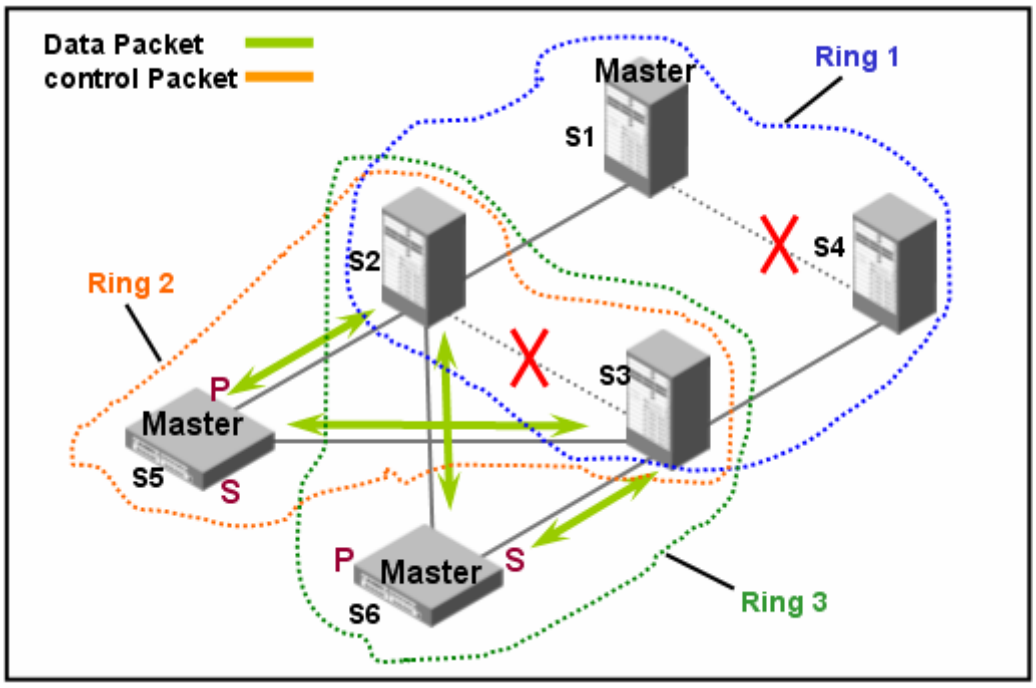
3. Link state change notification mechanism

The link state change notification mechanism provides a faster mechanism for handling topology changes in the ring network than the Polling mechanism, which is initiated by the transport node. The transport node is always monitoring its port link state, and once the state changes, it notifies the master node of the change by sending a notification message, and then the master node decides how to handle it. The transport node will send a LINK-UP message from the paired ERRP port to the ring when it detects a port UP, and a LINK-DOWN message if it detects a port DOWN.

4. Mechanism for checking the channel status of subring protocol messages on the primary ring

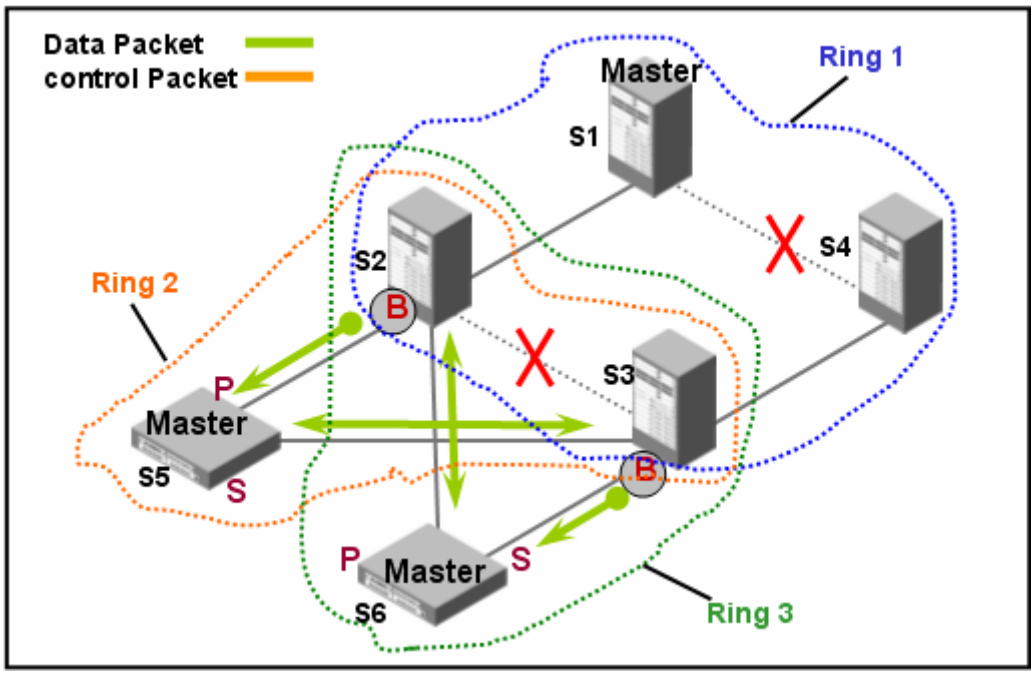
This mechanism is applied in the networking of multiple subrings intersecting the primary ring. The protocol messages of the subring need to be propagated between the edge nodes and the edge ports of the auxiliary edge nodes through the channel provided by the primary ring, as if the whole primary ring is a node on the subring. When the link of the primary ring fails and the channel of the subring protocol message between the edge node and the auxiliary edge node is interrupted (the common link with the subring in the primary ring fails and more than one non-common link fails), the master node of the subring will not be able to receive the Hello message it sends out, and so the Fail timer times out, and the master node of the subring migrates to the Fault state, releasing the secondary port.

For ordinary networking, the above scheme ensures that broadcast loops will not be formed and that the backup links play their proper roles. However, the actual network is often a dual-attribution network, as shown in the figure below, the two subrings Ring2 and Ring3 of the dual-attribution are connected to each other with the help of the edge node, which itself forms a ring, and when the main ring Ring1 fails, the secondary ports of the master nodes of all the subrings are released, and the broadcast loops are bound to be formed between the subrings (as shown by the arrows).



In order to eliminate this defect, a subring protocol message channel state detection mechanism is introduced on the primary ring, which needs to be accomplished by the edge nodes and auxiliary edge nodes in cooperation with the aim of

blocking the edge ports of the edge nodes before the subring primary node subports are released, so as to avoid the formation of data loops between the subrings. The effect of the mechanism after the failure of the primary ring is shown in the following figure.



One of the limitations of this mechanism in application is that it has to block the edge port of the edge node before the subring master node secondary port timeout is released. the edge node is the initiator and decision maker of the mechanism, the auxiliary edge node channel state listener, and is responsible for notifying the edge node of the channel state change in a timely manner.

36.2 ERRP Function Configuration

36.2.1 ERRP Feature Configuration Task List

Each configuration parameter is valid only when the ERRP protocol is on and the ring is activated. When the protocol is off or the ring is de-activated, the configuration information remains and takes effect the next time the ERRP protocol is turned on or the ring is activated.

Configuration tasks	clarification	Detailed Configuration
Enable/disable ERRP function	compulsory	36.2.2
Configuring ERRP Timer Parameters	selectable	36.2.3
Create and enter ERRP domain view	compulsory	36.2.4
Configure the operating mode of the ERRP domain	selectable	36.2.5
Configuring Control VLANs for ERRP Domains	compulsory	36.2.6
Create/delete ERRP rings and nodes within rings	compulsory	36.2.7
Activation/de-activation of ERRP rings	compulsory	36.2.8
Configuring ERRP to Trigger Multicast Query Message Delivery	selectable	36.2.9
Configuring ERRP Topology Collection	selectable	36.2.10
Display ERRP configuration information	selectable	36.2.11

36.2.2 Enable/disable ERRP function

Please perform ERRP protocol on/off configuration under system view.

manipulate	command	clarification
Go to System View	system-view	
Enable ERRP function	errp	Disable errp by default
Disabling the ERRP function	undo errp	

[Example]

! Enable ERRP function

[GPON]errp

36.2.3 Configuring ERRP Timer Parameters

Please configure it in system view.

manipulate	command	clarification
Go to System View	system-view	
Configure the ERRP message timeout	errp fail-timer *timer-value*	The message timeout parameter configuration range is 3-30S, the default is 6S, the value must be greater than or equal to 3 times the message sending interval
Restore the default ERRP message timeout period	undo errp fail-timer	
Configure the ERRP message sending interval	errp hello-timer *timer-value*	Send interval configuration range is 1-10S, the default is 1S, the value must be less than or equal to 1/3 of the message timeout time
Restore the default ERRP message sending interval	undo errp hello-timer	

[Example]

! Configure the ERRP protocol to send messages at an interval of 2 seconds

[GPON]errp hello-timer 2

36.2.4 Create and enter ERRP domain view

Please configure the following under system view.

manipulate	command	clarification
Go to System View	system-view	
Create and enter ERRP domain view	errp domain *domain-id*	When no domain is created, the system automatically creates the domain. Domain ID is the domain identifier, configured as an integer in the range of 0-15
Delete ERRP domain	undo errp domain [*domain-id*]	

[Example]

! Create and enter ERRP domain 0 view

[GPON]errpdomain 0

[GPON-errp-domain-0]

36.2.5 Configure the operating mode of the ERRP domain

In order to be able to interface with devices from other vendors, you can add working mode configuration items in the ERRP domain. Multiple ERRP domains can be configured on the same device, and each domain can be configured with different working modes. Please do the following configuration under the ERRP domain view.

manipulate	command	clarification
Go to System View	system-view	
Enter ERRP domain view	errp domain *domain-id*	
Configure the ERRP domain operating mode	workmode { standard | huawei | eips-subring }	

[Parameter Description]

standard: The protocol message uses the standard destination MAC address and message format in RFC3619, default is standard mode.

huawei: The protocol message uses Huawei's private destination MAC address and message format, which can be interfaced with Huawei's RRPP function.

eips-subring: protocol messages use Maipu protocol messages that can be interfaced with the Maipu protocol.

[Example]

! Configure the operating mode of ERRP domain 0 as standard

```
[GPON-errp-domain-0]workmode standard
```

36.2.6 Configuring Control VLANs for ERRP Domains

Please configure the following under ERRP domain view.

manipulate	command	clarification
Go to System View	system-view	
Enter ERRP domain view	errp domain *domain-id*	
Configuring Control VLANs for ERRP Domains	control-vlan *vlan-id*	Control VLAN identifier for the ERRP domain, an integer value from 1 to 4093
Delete the control VLAN for an ERRP domain	undo control-vlan	

[Parameter Description]

vlan-id: control VLAN identifier of the ERRP domain, takes an integer value of 1-4093.

Configuration Notes:

Control VLANs are relative to data VLANs; data VLANs are used to transmit data packets, and control VLANs are used to pass only ERRP protocol packets. Each ERRP domain has two control VLANs, called the master control VLAN and the subcontrol VLAN. protocol messages for the master ring are propagated in the master control VLAN, and protocol messages for the subring are propagated in the subcontrol VLAN. You only need to specify the master control VLAN when configuring it, and use the VLAN that is 1 greater than the master control VLAN ID value as the subcontrol VLAN.

On each device, only the ports that access the Ethernet ring (i.e., ERRP ports) belong to the control VLAN, and other ports cannot join the control VLAN. the ERRP ports of the primary ring belong to both the primary control VLAN and the subcontrol VLAN; the ERRP ports of the subring belong only to the subcontrol VLAN; and the data VLANs can contain ERRP ports as well as non ERRP ports. The primary ring is regarded as a logical node of the subring, and the protocol messages of the subring are transmitted through the primary ring and treated as data messages in the primary ring; the protocol messages of the primary ring are propagated only inside the primary ring and do not enter the subring. In order to

avoid conflict between the control VLAN and VLANs used for other purposes, the control VLAN must be configured as a VLAN ID that does not currently exist, and if the VLAN ID is configured as a control VLAN, then you cannot create that VLAN, and ERRP ports will be added automatically when configuring the control VLAN. To ensure that ERRP functions properly, the MAC address learning mode must be configured as IVL.

[Example]

! Configure the control VLAN for ERRP domain 0 to 25

[GPON-errp-domain-0]control-vlan 25

! Delete the control VLAN for ERRP domain 0. If there are still rings in the ERRP domain that are active then the control VLAN is not allowed to be deleted

[GPON-errp-domain-0]undo control-vlan

36.2.7 Create/delete ERRP rings and nodes within rings

Please configure the following under ERRP domain view.

manipulate	command	clarification
Go to System View	system-view	
Enter ERRP domain view	errp domain *domain-id*	
Creating a master node	ring *ring-id* role master primary-port *pri-port* secondary-port *sec-port* level *level*	
Creating a Transport Node	ring *ring-id* role transit primary-port *pri-port* secondary-port *sec-port* level *level*	
Creating Edge Nodes	ring *ring-id* role edge common-port *common-port* edge-port *edge-port*	
Creating auxiliary edge nodes	Ring *ring-id* role assistant-edgecommon-port *common-port* edge-port *edge-port*	
Delete ERRP ring	undo ring [*ring-id*]	

[Parameter Description]

ring-id: ring identifier with value 0-15

pri-port: port descriptor, e.g. ethernet 0/1

sec-port: port descriptor, e.g. ethernet 0/1

common-port: port descriptor, e.g. ethernet 0/1

sec-port: port descriptor, e.g. ethernet 0/1

level: the level of the ring, with 0 being the main ring and 1 being the subring.

[Example]

! Configure ERRP domain 0 with id 0 for the master ring, node mode as master, master port 1, slave port 2

[GPON-errp-domain-0]ring 0 role master primary-port ethernet 0/0/1 secondary-port ethernet 0/0/2 level 0

36.2.8 Activation/de-activation of ERRP rings

The ERRP ring will not take effect until it is activated. please configure the following in ERRP domain mode.

manipulate	command	clarification
Go to System View	system-view	
Enter ERRP domain view	errp domain *domain-id*	

Activation/de-activation of ERRP rings	ring *ring-id* { enable | disable }	

[Parameter Description]

ring-id: ring identifier

enable: activates a ring

diable: de-activate a ring

[Example]

! Activate ERRP domain 0 ring 0

[GPON-errp-domain-0]ring 0 enable

36.2.9 Configuring ERRP to Trigger Multicast Query Message Delivery

This function is used to cooperate with IGMP SNOOPING to immediately notify the IGMP querier to resend the IGMP general query message when the topology of the ERRP ring is changed, so that the IGMP SNOOPING multicast database can be updated in time. The master node turns on the Query-Solicit function by default, and other nodes turn off the Query-Solicit function by default. Please configure the following in ERRP domain mode.

manipulate	command	clarification
Go to System View	system-view	
Enter ERRP domain view	errp domain *domain-id*	
Enable trigger multicast query message sending	ring *ring-id* query-solicit	
Disable triggering multicast query message sending	undo ring *ring-id* query-solicit	

[Example]

! Enabling Query-Solicit for ERRP Domain 0 Ring 0

[GPON-errp-domain-0]ring 0 query-solicit

36.2.10 Configuring ERRP Topology Collection

This function is used to collect topology information within the ERRP domain. the topology information includes port and node connectivity relationships. Please configure the following in ERRP domain mode.

manipulate	command	clarification
Go to System View	system-view	
Enter ERRP domain view	errp domain *domain-id*	
Enable topology collection	topo-collect	
Turning off topology collection	undo topo-collect	

[Example]

! Enable topology information collection for ERRP domain 0 ring 0

[GPON-errp-domain-0] topo-collect

36.2.11 Display ERRP configuration information

ERRP domain and ring information can be displayed at any attempt.

manipulate	command	clarification
Display ERRP domain and ring information	display errp [domain *domain-id* [ring *ring-id*]]	When no domain or ring parameters are entered, indicates that all domain and ring information is displayed
Display ERRP control VLAN information	display errp control-vlan [*vlan-id*]	
Display ERRP topology collection information	display errp topology [domain *domain-id* [ring *ring-id*] | summary [domain *domain-id* [ring *ring-id*]]	

[Example]

! Display information about ring 1 in ERRP domain 0

[GPON]display errp domain 0 ring 1

Chapter 37 FlexLink Configuration

37.1 Introduction to FlexLink

37.1.1 Introduction to FlexLink

FlexLink is a Layer 2 link backup protocol. FlexLink consists of a pair of ports (which can be physical ports or aggregation ports), when one port forwards data the other port is in a backup standby state, when the main link fails, the backup port starts forwarding data. When the primary link fails, the backup port starts forwarding data. After the failed port recovers, the state changes to backup, and if the preemption mechanism is set, the master port recovers, and the state changes to forwarding data after the warning preemption delay. flexLink port preemption mechanism can be configured to use bandwidth and delay as the preemption mechanism, and the one that has the highest priority will be the master port. The device generates trap alarms when the primary and backup links fail.

37.1.2 FlexLink Basic Concepts

1. FlexLink group

A Flex Link group is also known as a flexible link group. A FlexLink group contains two member ports, one of which is designated as the master port (Master Port) and the other is designated as the backup port (Slave Port), and a port can only belong to one FlexLink group. Under normal circumstances, only one port (Master Port or Backup Port) is in the forwarding (ACTIVE) state, and the other port is blocked and in the standby (STANDBY) state. When a link failure occurs on the port in the forwarding state, such as the port state going DOWN, Ethernet OAM link failure, etc., the FlexLink group will automatically block the forwarding port and switch the port that was in the standby state to the forwarding state.

2. Master Port

A master port is a port role for a FlexLink group that is specified on the command line. the master port of a FlexLink group can be an Ethernet port or an aggregation group port.

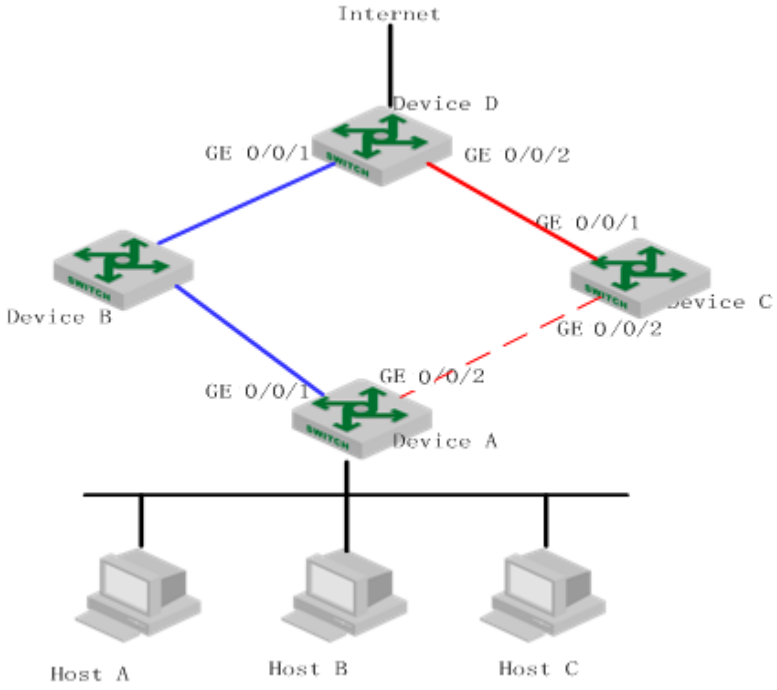
3. Backup Port (Slave Port)

A backup port is another port role for a FlexLink group specified on the command line. the backup port for a FlexLink group can be an Ethernet port or an aggregation group. the link on which the backup port resides is called the "backup link. The link on which the backup port resides is called the "backup link".

4. Flush messages

When a link switchover occurs in a FlexLink group, the original MAC forwarding table entries are no longer applicable to the new topology network and the MAC address forwarding table entries need to be updated for the entire network. the FlexLink notifies the other devices of the MAC table entries refreshing operation by means of the Flush message.

37.1.3 FlexLink Basic Principles



Taking the above figure as an example, the working principle of FlexLink is introduced according to the link normal working mechanism, link fault processing mechanism, and link recovery processing mechanism.

1. Link normalization mechanisms

Port 0/0/1 of Device A is the primary port and port 0/0/2 is the backup port. When both uplinks are normal, the primary port 0/0/1 is in forwarding state and the link it is on is the primary link, and the backup port is in standby state and the link it is on is the backup link. Data is transmitted along the link indicated by the blue line, and there are no loops in the network to avoid broadcast storms.

2. Link troubleshooting mechanisms

When the primary link of Device A fails, the primary port 0/0/1 switches to the standby state and the backup port 0/0/2 switches to the forwarding state. At this time, because the MAC address forwarding table entries on the devices in the network may have been incorrect, Device A notifies the other devices to update the MAC table entries by sending Flush messages. This approach requires that the upstream devices Device B, Device C, and Device D all support the FlexLink function and all recognize the Flush message.

In order to realize fast link switching, it is necessary to enable the Flush message sending function on Device A, and to enable the receiving and processing of Flush messages on all the ports of the upstream device that are on the dual uplink network.

After a link switchover occurs on Device A, it sends a Flush message from the new primary link, that is, it sends a Flush message from port 0/0/2. When Device C, the upstream device, receives the Flush message, it processes the Flush message and sends down the MAC address in the message to port 0/0/2 of Device C.

Thereafter, if Device D receives a data packet whose destination device is Host A, Host B, or Host C, Device D will forward it through Layer 2 broadcasting.Device C looks up the MAC address table after receiving it, and forwards it to Device A from port 0/0/2, and then finally forwards it to Host A, Host B from Device A, Host A, Host B, and Host C.

The mechanism of notifying the device of the update through the Flush message does not need to wait until the table entries are aged before updating, and can greatly reduce the time required for updating the table entries. In general, the entire switching process of the link can be completed in milliseconds, and there is basically no traffic loss.

3. Link recovery processing mechanisms

FlexLink supports three modes: preemption mode, non-preemption mode and bandwidth preemption mode. The link recovery mechanism is different in different modes:

If the FlexLink is configured in preemption mode, when the primary link failure is recovered, the primary port will be preempted into the forwarding state, and the backup port will go into standby state.

If FlexLink is configured in non-preemptive mode, the backup port will continue to be in the forwarding state and the primary port will continue to be in the standby state when the primary link failure is recovered, so that the traffic can be kept stable.

If FlexLink is configured in bandwidth preemption mode, when the primary link failure is recovered, if the bandwidth of the backup port is higher, the backup port will continue to be in the forwarding state and the primary port will continue to be in the standby state. If the bandwidth of the primary port is higher, the primary port is preempted into the forwarding state and the backup port goes into the standby state.

37.2 FlexLink Function Configuration

37.2.1 FlexLink Function Configuration Task List

The list of FlexLink function configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Creating/Deleting FlexLink Groups	compulsory	37.2.2
Add/Remove FlexLink Master Ports	compulsory	37.2.3
Add/Remove FlexLink Slave Ports	selectable	37.2.4
Configuring the FlexLink Group Preemption Method	selectable	37.2.5
Configuring the FlexLink Group Preemption Delay Time	selectable	37.2.6
Configuring the FlexLink Flush Function	selectable	37.2.7
Display FLexlink configuration information	selectable	37.2.8

37.2.2 Creating/Deleting FlexLink Groups

Please create or delete FlexLink groups in System View.

manipulate	command	clarification
Go to System View	system-view	
Creating a Flexlink Group	flex-link-group *groupid*	The groupid can be configured from 0-127.
Delete Flexlink Group	undo flex-link-group	

[Example]

! Configure Flexlink group 0

```
[GPON]flex-link-group 0
```

37.2.3 Add/Remove Flexlink Master Ports

Please add or remove Flexlink Master ports under Flexlink group view.

manipulate	command	clarification
Go to System View	system-view	
Enter the Flexlink group view	flex-link-group *groupid*	
Adding a Flexlink Group Master Ethernet	port ethernet *interface-num*	

Port	master	
Adding a Flexlink Group Master Aggregation Group Port	port channel-group *channel-group-id* master	channel-group-id is the aggregation group ID, in the range 0-31
Delete Flexlink Group Master Port	undo port master	

[Example]

Add Ethernet port 1 as the Master port of FlexLink group 0! Add Ethernet port 1 as the Master port of FlexLink group 0.

[GPON-flex-link-group-0] port ethernet 0/0/1 master

37.2.4 Add/Remove Flexlink Slave Ports

Please add or remove Flexlink Slave ports under Flexlink group view.

manipulate	command	clarification
Go to System View	system-view	
Enter the Flexlink group view	flex-link-group *groupid*	
Adding a Flexlink Group Master Ethernet Port	port ethernet *interface-num* slave	
Adding a Flexlink Group Master Aggregation Group Port	port channel-group *channel-group-id* slave	channel-group-id is the aggregation group ID, in the range 0-31
Delete Flexlink Group Master Port	undo port slave	

[Example]

Add Ethernet port 2 as the Slave port of FlexLink group 0! Add Ethernet port 2 as Slave port of FlexLink group 0!

[GPON-flex-link-group-0]port ethernet 0/0/2 slave

Description:

- The device supports configuration of multiple Flexlink groups, and ports cannot exist in different Flexlink groups;
- In the Flexlink group, to configure both Master and Slave ports, you must wire down the STP function of the ports, otherwise the configuration fails;

37.2.5 Configuring the FlexLink Group Preemption Method

Please configure the FlexLink group preemption method under the Flexlink group view.

manipulate	command	clarification
Go to System View	system-view	
Enter the Flexlink group view	flex-link-group *groupid*	
Configuring the FlexLink Group Preemption Method	preemption mode { forced | bandwidth | off }	Defaults to off non-preemptive mode
Restore the default preemption method for FlexLink groups	undo preemption mode	

[Parameter Description]

Forced: forced preemption method

Bandwidth: according to the bandwidth preemption method

Off: Non-compulsory preemption approach

[Example]

! Configure the priority preemption method for FlexLink group 0 as Forced

[GPON-flex-link-group-0] preemption mode forced

37.2.6 Configuring the FlexLink Group Preemption Delay Time

Please perform FlexLink group preemption delay time configuration under Flexlink group view.

manipulate	command	clarification
Go to System View	system-view	
Enter the Flexlink group view	flex-link-group *groupid*	
Configuring the FlexLink Group Preemption Delay Time	preemption delay *delay-time*	delay-time, delay time, the configuration range is 1-60 seconds, the default is 45 seconds
Restore the default preemption delay time for FlexLink groups	undo preemption delay	

[Parameter Description]

Delay-time: delay time, the configuration range is 1-60 seconds, the default is 45 seconds: forced preemption mode Delay-time needs to be configured when the preemption method is forced or bandwidth to take effect.

[Example]

! Configure the preemption delay time for FlexLink group 0 to 30 seconds

[GPON-flex-link-group-0] preemption delay 30

37.2.7 Configuring the FlexLink Flush Function

When the forwarding port is down, the backup port will change to the forwarding state. In order to accelerate the convergence of the device, you can turn on the Flexlink flush function. When the backup port turns into forwarding state after the flush send function is turned on, it will send out the mac address learned from other ports of the exchange. The device that receives the flush message will forward the message, and if you turn on the flush receive function, it will update the local mac address according to the received message, so as to achieve the effect of fast convergence of services.

The Flush function is based on global control and all Flexlink groups use the same Flush configuration. please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Enable FlexLink Flush sending	flex-link flush transmit	Disable sending Flush messages by default
Disable FlexLink Flush sending	undo flex-link flush transmit	
Enable FlexLink Flush reception	flex-link flush receive	Disable receiving Flush messages by default
Turning off FlexLink Flush reception	undo flex-link flush receive	

[Example]

! Enable the device to receive and send FlexLink Flush messages

[GPON] flex-link flush receive

[GPON] flex-link flush transmit

37.2.8 Display FlexLink configuration information

FlexLink configuration information can be viewed under any attempt.

manipulate	command	clarification
Displaying FlexLink Group Configuration Information	display flex-link-group [*group-id*]	The display internally includes: FlexLink group's Master port, Slave port, Active port, priority preemption mode, preemption delay time, etc. When group-id is not specified, all Flexlink group configuration information is displayed.
Displaying FlexLink Flush Configuration Information	display flex-link flush statistics	

[Example]

! Display all FlexLink group configuration information

```
[GPON]display flex-link-group
```

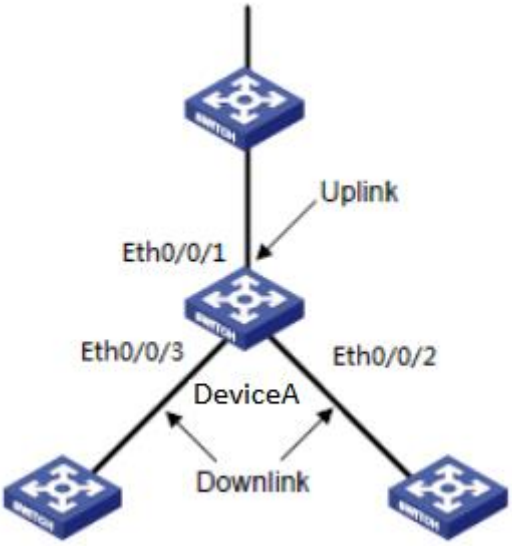
Chapter 38 Monitorlink Configuration

38.1 About Monitorlink

38.1.1 About Monitorlink

MonitorLink is a port linkage solution introduced to supplement Flexlink, which is used to monitor the uplink and perfect the backup role of Flexlink. monitorLink can trigger the up/down change of the downlink according to the uplink up/down status change, thus triggering the switching of the backup link of the downstream device.

A MonitorLink group consists of an uplink port and one or more downlink ports. When the link on which the uplink port is located fails, MonitorLink forcibly shuts down all downlink ports in the group; when the link on which the uplink port is located returns to normal, it reopens all downlink ports in the group.



In the above figure, for example, the MonitorLink group configured on Device A consists of one uplink port (Ethernet0/0/1) and two downlink ports (Ethernet0/0/2 and Ethernet0/0/3). Each member port can be an Ethernet port or a port link aggregation group.

38.1.2 Monitorlink Basic Concepts

1. Monitorlink group

Monitorlink groups are also called Monitor Link groups, and each group consists of both uplinks and downlinks, with member roles determined by user configuration. Among them, there can be multiple member ports in both uplink and downlink, but each member can only belong to one Monitor Link group. The member ports can be Ethernet ports or aggregation interfaces.

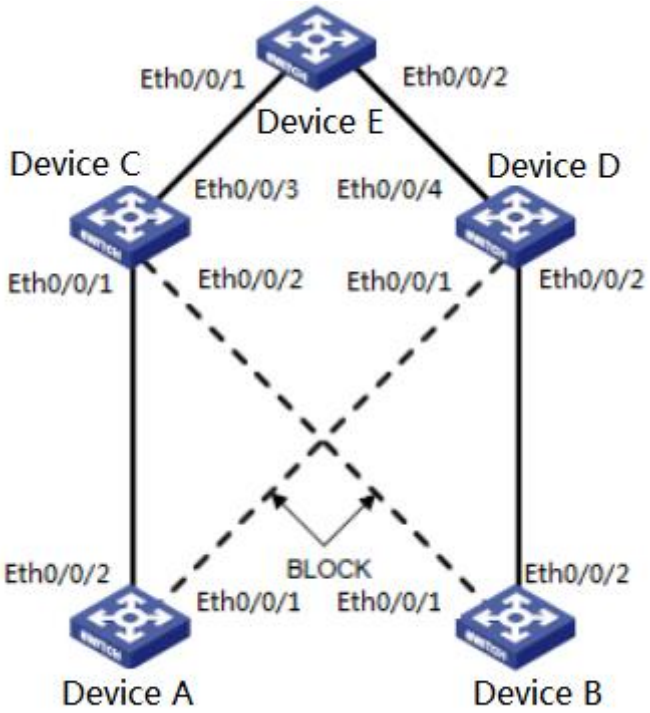
2. Uplinks

The uplink (uplink) is the monitored link in the MonitorLink group. When there is no uplink member in the MonitorLink group or all uplink member ports are down, the MonitorLink group is in the down state. And when just one uplink member in the MonitorLink group is up, the MonitorLink group is in the up state.

3. Downlink

The downlink is the controlled link in the MonitorLink group. When the up/down state of the MonitorLink group changes, the MonitorLink changes the state of the downlink member ports accordingly to keep them consistent with the MonitorLink group state.

38.1.3 Monitorlink Basic Principles



As shown in the figure above, the working principle of MonitorLink is introduced.Device C and Device D are connected to the upstream device Device E. A MonitorLink group is configured on Device C, with port Ethernet0/0/3 as the upstream port and ports Ethernet0/0/1 and Ethernet0/0/2 as the downstream ports.Configure the Flexlink group on Device A with port Ethernet0/0/2 as the Master port and port Ethernet0/0/1 as the Slave port.

1) If the Monitorlink group is not configured on Device C, when the link where uplink port Ethernet0/0/3 is located in Device C fails, Device A, which is configured with the Flexlink group, will not experience a link switchover within the Flexlink group because the link where its primary port Ethernet0/0/2 is located has not failed. Flexlink group link switching does not occur at this time. However, in fact, the traffic on Device A can no longer be uplinked to Device E through the link on port Ethernet0/0/2.

2) If a Monitorlink group is configured on Device C, and the Monitorlink group discovers that there is a link failure on its uplink port Ethernet0/0/3, it will shut down all the downlink ports in the group, so port Ethernet0/0/1 on Device C will be blocked. At this time, the Flexlink group on Device A discovers that a link failure has occurred on its master port Ethernet0/0/2, and the slave port Ethernet0/0/1 will immediately switch to the forwarding state, thus switching the traffic to the backup link.

38.2 Monitorlink Function Configuration

38.2.1 Monitorlink Function Configuration Task List

The list of Monitorlink feature configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Configure the Monitorlink group for the port	compulsory	38.2.2
Configuring Monitorlink Groups for Aggregation Groups	selectable	38.2.3

Display Monitor Link information	selectable	38.2.4

38.2.2 Configure the Monitorlink group function of a port

Please configure the Monitorlink group function of the port in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring Uplink Ports for Monitorlink Groups	port monitor-link-group *monitor-link-group-id* uplink	monitor-link-group-id is configured in the range of 0-4
Configuring Monitorlink Group Downlink Ports	port monitor-link-group *monitor-link-group-id* downlink	
Delete the port Monitorlink group configuration	undo port monitor-link-group *monitor-link-group-id*	

[Example]

! Configure Ethernet port 1 as the uplink port for Monitorlink group 1.

[GPON-ethernet-0/0/1]port monitor-link-group 0 uplink

! Configure Ethernet port 2 as the downlink port for Monitorlink group 1.

[GPON-ethernet-0/0/2]port monitor-link-group 0 downlink

38.2.3 Configuring Monitorlink Group Functions for Aggregation Groups

Please configure the Monitorlink group function of the aggregation group under system view.

manipulate	command	clarification
Go to System View	system-view	
Configure the aggregation port as a Uplink port of the Monitorlink group	channel-group *channel-group-id* monitor-link-group *monitor-link-group-id* uplink	channel-group-id is the aggregation group ID in the range 0-31. monitor-link-group-id is the Monitorlink group ID in the range 0-4.
Configure the aggregation port as the Downlink port of the Monitorlink group	channel-group *channel-group-id* monitor-link-group *monitor-link-group-id* downlink	
Delete aggregation group Monitorlink group configuration	undo channel-group *channel-group-id* monitor-link-group *monitor-link-group-id*	

[Example]

! Configure aggregation group 1 as a Uplink port for Monitorlink group 1

[GPON]channel-group 1 monitor-link-group 1 uplink

38.2.4 Display Monitorlink configuration information

Configuration information for Monitorlink can be viewed under any attempt.

manipulate	command	clarification
Display Monitorlink configuration information	display monitor-link-group [*monitor-link-group-id*]	When monitor-link-group-id is not specified, all Monitorlink group configuration information is displayed.

[Example]

! Displays configuration information for Monitorlink group 1

[GPON] display monitor-link-group 1

Chapter 39 Static Route Configuration

39.1 Introduction to Static Routing

This device is based on ASIC technology, and the system internally maintains a Layer 3 forwarding routing table. The routing table is used to indicate the next-hop address and related information to a certain destination address, and these routes can be dynamically learned by the routing protocol or manually added statically. Static routes are routes that are manually specified to a certain address or a certain segment of an address.

39.2 Static Routing Feature Configuration

39.2.1 Static Route Configuration Task List

The list of static routing feature configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Add/delete static routing table entries	compulsory	39.2.2
Display routing table information	selectable	39.2.3

39.2.2 Add/delete static routing table entries

You can configure and delete static route table entries under system view with the following configuration commands.

manipulate	command	clarification
Go to System View	system-view	
Adding a Static Routing Table Entry	ip route ip-address mask next-hop-address	
Delete static routing table entries	undo ip route ip-address mask [next-hop-address]	
Delete all static routing table entries	undo ip route static all	

[Parameter Description]

IP-address: the address of the destination segment of the static route to be added

Mask: Mask of the destination address

next-hop-address: next-hop IP address of the static route

[Example]

! The following command adds a segment route to 192.168.1.0/24 with a next hop address of 10.10.10.254

```
[GPON]ip route 192.168.1.0 255.255.255.0 10.10.10.254
```

! Delete all static routing table entries

```
[GPON]undo ip route static all
```


Description:

- The next-hop IP address must be on the same network segment as the device's Layer 3 interface for the configuration to succeed;
- If the destination address and mask are all zeros, the route added is the default route;
- If the mask is configured as all 255, the added route is a host route;

39.2.3 Display routing table information

Routing table entry information in the device can be displayed at any attempt.

manipulate	command	clarification
Display all routing table information	display ip route	
Displays specified routing table information	display ip route *ip-address* [*mask*]	
Display all static routing table information	display ip route static	

[Example]

! Display all routing table information

[GPON]display ip route

Chapter 40 RIP configuration

40.1 Introduction to RIP

RIP (Routing Information Protocol) is a relatively simple Interior Gateway Protocol (IGP), mainly used in smaller networks, such as campus networks and regional networks with simpler structures. For more complex environments and large networks, RIP is generally not used, because the implementation of RIP is relatively simple, in the configuration and maintenance of management is far easier than OSPF and IS-IS, so there is still a wide range of applications in the actual network.

40.1.1 Basic Concepts of RIP

RIP is a protocol based on the Distance-Vector (D-V) algorithm, which exchanges routing information through UDP messages, using port number 520. it exchanges routing information through UDP (User Datagram Protocol) datagrams, and sends out update messages every 30 seconds. If the local router does not receive a route update message from the router at the opposite end after 180 seconds, the local router marks all route information from the router at the opposite end as unreachable; if a route information is marked as unreachable and an update message from the router at the opposite end is still not received within 120 seconds after the information has been marked as unreachable, the local router deletes the route from the routing table maintained by it.

RIP uses Hop Count as a measure of the distance to reach the letter-host, i.e., the destination, called the Routing Metric. In RIP, a router's hop count to a network directly connected to it is 0, the hop count to a network reachable through a router is 1, and so on. In order to limit the convergence time, RIP specifies that the Metric is an integer between 0 and 15, and hops greater than or equal to 16 are defined as infinity, i.e., the destination network or host is unreachable.

There are two versions of RIP, RIP-1 and RIP-2 (RIP-2 supports plaintext authentication).

To improve performance and prevent routing loops, RIP supports Split Horizon and Poison Reverse.

40.1.2 RIP's routing database

Each router running RIP manages a routing database that contains route entries to all reachable destinations in the network that contain the following information:

1) Destination address: the IP address of the host or network;

2) Next hop address: the address of the next router to pass through in order to reach the destination;

3) Output interface: indicates the interface from which the message will be forwarded out;

4) Metric value: the overhead for this router to reach the destination, an integer between 0 and 16;

5) Timer: the time elapsed since the routing entry was last modified. the timer is reset to 0 each time the routing entry is modified.

40.1.3 RIP startup and operation process

The entire process of starting and running the RIP is as follows:

1) After a router starts RIP, it sends a request message to the RIP neighboring routers. When the neighboring RIP routers receive the request message, they respond to the request and send back a response message containing local routing table information;

2) The router receives the response message, updates the local routing table, and at the same time sends a triggered update message to the neighboring routers to notify the routing update information. After receiving the triggered update message, neighboring routers send triggered update messages to their respective neighboring routers. After a series of trigger update broadcasts, each router gets and keeps the latest routing information;

3) RIP sends local routing tables to neighboring routers every 30 seconds by default. Neighboring routers running the RIP protocol maintain the local routes after receiving the message, select an optimal route, and then send update information to their respective neighboring networks so that the updated routes can eventually be globally valid. At the same time, RIP uses an aging mechanism to age the timeout routes to ensure that the routes are real-time and effective.

40.1.4 Protocol Versions of RIP

RIP has two protocol versions: RIP-1 and RIP-2.

RIP-1 is a Classful Routing Protocol, which only supports broadcasting of protocol messages.RIP-1 protocol messages cannot carry mask information, and it can only recognize the routes of natural network segments such as classes A, B, and C. Therefore, RIP-1 does not support Discontiguous Subnet. Therefore, RIP-1 does not support Discontiguous Subnet.)

RIP-2 is a Classless Routing Protocol (CRP) and has the following advantages over RIP-1:

1) Supports route marking, and the routes can be flexibly controlled according to the route marking in the routing policy;

2) The message carries mask information and supports route aggregation and CIDR (Classless Inter-Domain Routing);

3) Supports specifying the next hop, so that the optimal next hop address can be selected on the broadcast network;

4) Support multicast routing to send update messages to reduce resource consumption.

 Description:

RIP-2 has two message delivery methods: broadcast and multicast. by default. the multicast method will be used to send messages. the multicast address used is 224.0.0.9. when the interface is running the RIP-2 broadcast method, it can also receive RIP-1 messages.

40.2 RIP Feature Configuration

40.2.1 RIP Feature Configuration Task List

In each configuration task, RIP must be enabled before other functional features can be configured. The configuration of functional features related to Layer 3 interfaces is not restricted by whether RIP is enabled or not. Note that after you turn off RIP, the original Layer 3 interface parameters remain and take effect the next time you start RIP.

The list of RIP configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable RIP function	compulsory	40.2.2
Specifies that the IP interface is running the RIP protocol	compulsory	40.2.3
Specifies the RIP version of the interface	selectable	40.2.4
Configure RIP message authentication	selectable	40.2.5
Configuration level segmentation and toxicity reversal	selectable	40.2.6
Configuring a Publication Aggregation Route	selectable	40.2.7
Configuring Additional Routing Rights	selectable	40.2.8
Configuring Default Route Weights	selectable	40.2.9
Configuring RIP Routing Administrative Distance	selectable	40.2.10
Configuring Route Filtering	selectable	40.2.11
Configure the introduction of external routes	selectable	40.2.12
Configuring Default Route Redistribution	selectable	40.2.13
Configure the specified interface to block RIP packets	selectable	40.2.14
Configuring RIP Timer Parameters	selectable	40.2.15
Create/delete RIP keychain keychain	selectable	40.2.16
Create/delete RIP keychain keychain-key	selectable	40.2.17
Configure the key keychain-key related parameters of the RIP keychain	selectable	40.2.18

RIP Monitoring and Maintenance	selectable	40.2.19

40.2.2 Enable/disable the RIP function

By default, the device disables the RIP function. please configure it in system view.

manipulate	command	clarification
Go to System View	system-view	
Initiate RIP protocol	router rip	
Disabling the RIP protocol	undo router rip	

[Example]

! Start the RIP protocol

[GPON]router rip

40.2.3 Specifies that the IP interface is running the RIP protocol

By default, when the RIP function is turned on, no Layer 3 interface on the device runs the RIP protocol, and this interface sends and receives RIP messages only if it is specified to run the RIP protocol on a certain IP segment. please configure it under the RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Specifies that the IP interface is running the RIP protocol	network ip-address	ip-address is the device Layer 3 interface IP address
Eliminate IP interfaces running the RIP protocol	undo network *ip-address*	

[Example]

! Specify the interface IP address 192.168.1.100 to run the RIP protocol

[GPON-router-rip]network 192.168.1.100

40.2.4 Specifies the RIP version for the interface

The system supports configuring the RIP version of an interface under RIP view, and this command is equivalent to performing the RIP version configuration of all interfaces in bulk. In addition, the system supports specifying the RIP version of an interface individually under VLAN interface or Supervlan interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Configuring the RIP Version	version{ 1 | 2 }	The default RIP version is Version 2
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	

Configure the interface to receive RIP protocol message types	ip rip receive version { 1 | 2 [bcast | mcast] }	Default Receive Protocol MessageVersion 2 mcast
Restore the interface's default permission to receive RIP protocol packets	undo ip rip receive version	
Configure the interface to send RIP protocol message types	ip rip send version{ 1 | 2 [bcast | mcast] }	Default Send Protocol MessageVersion 2 mcast
Restore the interface to send RIP protocol messages by default	undo ip rip send version	

[Parameter Description]

bcast: the RIP Version 2 version of the message, sends a broadcast message

mcast: RIP Version 2 of the message version, sends multicast messages

The message transmission method of RIP-1 is broadcast. there are two message transmission methods in RIP-2: broadcast and multicast. by default, multicast will be used to send messages. the multicast address in RIP-2 is 224.0.0.9.

The advantage of sending messages in multicast is that those hosts in the same network that are not running RIP can avoid receiving broadcast messages from RIP. In addition, sending messages in multicast allows hosts running RIP-1 to avoid incorrectly receiving and processing RIP-2 routes with subnet masks. When an interface is running RIP-2 and broadcasting, it is also compatible with receiving broadcast messages from RIP-1.

[Example]

! Specifies that VLAN interface 100 is running RIP Version 2 and receives and sends broadcast RIP packets.

```
[GPON-vlanInterface-100] ip rip receive version 2 bcast
[GPON-vlanInterface-100] ip rip send version 2 bcast
```

40.2.5 Configuring RIP Message Authentication

RIP-1 does not support message authentication. When the interface is running RIP-2, you can configure whether to perform message authentication. The authentication method is Text authentication or MD5 authentication. please configure it under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring MD5 Authentication for RIP Messages	ip rip authentication modemd5 key-chain *key-string*	The interface does not enable RIP message authentication by default. The key-string can be configured up to 32 characters.
Configuring RIP Message Text Authentication	ip rip authentication mode text passwd *passwd*	passwd can be configured up to 16 characters long.
Remove the RIP message authentication function	undo ip rip authentication	

[Example]

! Configure RIP message authentication on VLAN interface 100 as MD5 authentication with the key value test

```
[GPON-vlanInterface-100]ip rip authentication mode md5 key-chain test
```

40.2.6 Configuration level segmentation and toxicity reversal

Horizontal segmentation means: a route learned by a device on a certain interface is not sent out again from that interface, so that routing loops can be avoided. Horizontal segmentation also includes horizontal segmentation with toxicity reversal, when a routing path collapses, the earliest device to broadcast this route will continue to keep the original route in the message, but specify that the route is infinitely long. In some special cases, it is necessary to disable horizontal segmentation to sacrifice efficiency for proper route propagation.

Both horizontal segmentation and toxic reversal horizontal segmentation prevent the creation of routing loops, while toxic reversal horizontal segmentation is superior in that it immediately breaks the routing loops that have been created. The disadvantage is that it increases the amount of routing information in the network. Therefore, RFCs consider horizontal segmentation to be a must for RIP and toxic reversal horizontal segmentation to be a should. By default interfaces have horizontal segmentation turned on and toxicity reversal turned off.

Please perform the following configurations under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring Horizontal Segmentation	ip rip split-horizon	This feature is enabled by default
Configuration of horizontal segmentation with toxicity reversal	ip rip split-horizon poisoned-reverse	This feature is disabled by default
Turn off the horizontal split function	undo ip rip split-horizon	
Turn off the toxicity reversal function	undo ip rip split-horizon poisoned-reverse	

[Example]

! Enable horizontal segmentation and toxicity reversal for VLAN interface 100

[GPON-vlanInterface-1]ip rip split-horizon

[GPON-vlanInterface-1]ip rip split-horizon poisoned-reverse

40.2.7 Configuring a Publication Aggregation Route

Route aggregation is the process by which routes from different subnets within the same natural segment are aggregated into a single naturally masked route for outbound (other segments) transmission. Route aggregation reduces the amount of routing information in the routing table and also reduces the amount of exchange information.

For example, assuming that there are three subnet-contiguous routes, 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24, in the routing table, the device only needs to be configured to publish an aggregated route, 192.168.0.0/16, which is aggregated into a single route, 192.168.0.0/16, for outbound delivery.

Please make the following configurations under RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Configure to publish an aggregation	aggregate-address ip-address/mask-length	
Delete an aggregation function	undo aggregate-address ip-address/mask-length	

[Parameter Description]

ip-address/mask-length: IP address and mask length parameters, for example 192.168.0.0/16

[Example]

! Post a RIP aggregation route with a 192.168.0.0 segment and a 16-bit mask!

[GPON-router-rip]aggregate-address 192.168.1.0/16

40.2.8 Configuring Additional Routes Rights

The device supports setting the interface to add an additional Routing Metric to a route when it sends and receives RIP datagrams. The additional Routing Metric does not directly change the routing metric of a route in the routing table, but adds a specified metric when the interface receives or sends a route. Please perform the following configuration under RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Configure additional routing rights for incoming interfaces	offset-list { *ip-acl-name* | *ip-acl-number* } in *metric* [{ vlan-interface | supervlan-interface } *vlan-id*]	Metric values are configured in the range 0-16. When no Layer 3 interface is specified, it means that it is applied to all Layer 3 interfaces
Delete additional routing rights for incoming interfaces	undo offset-list { *ip-acl-name* | *ip-acl-number* } in *metric* [{ vlan-interface | supervlan-interface } *vlan-id*]	
Configure additional routing rights for outgoing interfaces	offset-list { *ip-acl-name* | *ip-acl-number* } out *metric* [{ vlan-interface | supervlan-interface } *vlan-id*]	Metric values are configured in the range 0-16. When no Layer 3 interface is specified, it means that it is applied to all Layer 3 interfaces
Delete additional routing rights for outgoing interfaces	undo offset-list { *ip-acl-name* | *ip-acl-number* } out *metric* [{ vlan-interface | supervlan-interface } *vlan-id*]	

[Parameter Description]

ip-acl-name|ip-acl-number: references the IP-ACL of the matching routing table entry;

metric: Configured route append value, configured in the range of 0-16;

vlan-interface |supervlan-interfac: Layer 3 interface used to configure additional routing rights;

[Example]

! Configure the routing table entry 192.168.1.0/24 to add a metric value of 5 when coming in from VLAN interface 100

[GPON-router-rip]ip acl 1 permit 192.168.1.0 0.0.0.255

[GPON-router-rip]offset-list 1 in 5 vlan-interface 100

40.2.9 Configuring Default Route Weights

The device supports configuring the default route weights for introduced routes. perform the following configurations in RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Configuring Default Route Weights	default-metric *metric*	The default metric value is 1, and the configuration range is 1-16
Restoring the Default Routing Rights Configuration	undo default-metric	

[Parameter Description]

metric: Routing weight, configured in the range of 1-16;

[Example]

! Configure the default route weight as 5

```
[GPON-router-rip] default-metric 5
```

40.2.10 Configuring RIP Routing Administrative Distance

The device supports configuring the routing administrative distance of the RIP protocol. Route administrative distance is used to select routes when there are two routes of different routing protocols to reach the same destination address. the smaller the administrative distance of a routing protocol is, the more reliable the route obtained by the protocol is. the default route administrative distance of RIP is 120, and the default route administrative distance of OSPF is 110, so that the routes learned by OSPF have a higher priority. Perform the following configuration in RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Configuring RIP Routing Administrative Distance	distance distance [[ip-address/mask-length] [ip-acl-name|ip-acl-number]]	Default distance value is 120, configuration range is 1-255
Restore the default RIP routing administrative distance	undo distance [distanceip-address / mask-length [ip-acl-name | ip-acl-number]]	

[Parameter Description]

distance: routing administrative distance, configured in the range of 1-255;

ip-address/mask-length: prefix address (dotted decimal) and mask length, such as 192.168.1.0/24;

ip-acl-name|ip-acl-number: references the IP-ACL of the matching routing table entry;

Only routes that meet the ip-address/mask-length or ip-acl-name|ip-acl-number conditions set the corresponding distance.

[Example]

! Configure the RIP routing administrative distance to 150

```
[GPON-router-rip] distance 150
```

40.2.11 Configuring Route Filtering

The device supports configuring application access lists and prefix lists to filter routes. perform the following configuration in RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Configure the incoming interface to apply route filtering	distribute-list { *ip-acl-name* | *ip-acl-number* | prefix *prefix-list* } in [{ vlan-interface | supervlan-interface } *vlan-id*]	When no Layer 3 interface is specified, it means that it is applied to all Layer 3 interfaces
Delete the inbound interface to apply route filtering	undo *distribute-list* { *ip-acl-name* | *ip-acl-number* | prefix *prefix-list* } in [{ vlan-interface | supervlan-interface } *vlan-id*]	
Configure the outgoing interface to apply route filtering	distribute-list { *ip-acl-name* | *ip-acl-number* | prefix *prefix-list* } out [{ vlan-interface | supervlan-interface } *vlan-id*]	
Remove the outgoing interface to apply route filtering	undo distribute-list { *ip-acl-name* | *ip-acl-number* | prefix *prefix-list* } out [{ vlan-interface | supervlan-interface } *vlan-id*]	

[Parameter Description]

ip-acl-name|ip-acl-number: references the IP-ACL of the matching routing table entry;

prefix-list: IP segment configuration

[Example]

! Configure filtering of routes on the 192.168.1.0/24 network segment

```
[GPON-router-rip]ip acl 1 deny 192.168.1.0 0.0.0.255
[GPON-router-rip]distribute-list 1 in
```

40.2.12 Configure the introduction of external routes

RIP allows users to introduce routing information from other protocols into RIP.

The routing protocols or types that can be introduced by RIP in the device include: Connected, Static, OSPF, and ISIS.

Please perform the following configuration in RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Configure the introduction of external routes	redistribute { babel | bgp | connected | isis | kernel | ospf | rip | static } metric *metric* route-map *route-map*	
Remove the introduction of external routes	undo redistribute { babel | bgp | connected | isis | kernel | ospf | rip | static }	

[Parameter Description]

babel: introduced from the Babel route;

bgp: introduced from BGP routing;

conneted: introduced from a directly connected route;

isis: introduced from the ISIS route;

kernel: introduced from the core route;
ospf: introduced from OSPF routing;
rip: introduced from RIP routing;
static: introduced from static routes;
metric: the route weight assigned to the introduced route, ranging from 0-16;
route-map: pointer to the route map used to introduce routes, configurable up to 32 characters;
[Example]
! Configure the introduction of OSPF routes with route weights of 5

[GPON-router-rip]redistribute ospf metric 5

40.2.13 Configuring Default Route Redistribution

The device allows network 0.0.0.0 to be redistributed into RIP, i.e., the device inserts the default route with destination 0.0.0.0 into the RIP route database and advertises the route in the same way as it advertises any other route, which is turned off by default. Please perform the following configuration under RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Configuring Route Redistribution	default-information originate	
Delete route republishing	undo default-information originate	

[Example]
! Configuring the Default Route Redistribution Feature

[GPON-router-rip]default-information originate

40.2.14 Configure the specified interface to block RIP packets

The device supports configuration to block RIP broadcasts on specified Layer 3 interfaces, which can be achieved through passive-interface, which means "passive interface", and with this command, updates to specific routing protocols will not be sent out of this interface. Passive-interface This method can be used to control the flow of routing updates and avoid unnecessary wastage of link resources. Please configure it under RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Specifies that the interface blocks RIP packets	passive-interface { default | vlan-interface *vlanid* | supervlan-interface *vlanid* }	
Cancel interface blocking of RIP packets	undo key passive-interface { default | vlan-interface *vlanid* | supervlan-interface *vlanid* }	

[Parameter Description]
default: Specifies that all Layer 3 interfaces on the device are set to "passive interface" mode;
vlan-interface: Specifies a VLAN interface as "passive interface" mode;
supervlan-interface: Specifies a Supervlan interface as "passive interface" mode;
[Example]
Configure VLAN interface 100 as a "passive interface" mode! Configure VLAN interface 100 for "passive interface" mode

[GPON-router-rip]passive-interface vlan-interface 100


Description:

When modifying from default configuration to vlan-interface or supervlan-interface, you need to cancel default configuration first. When switching from vlan-interface or supervlan-interface to default configuration, you can switch directly.

40.2.15 Configuring RIP Timer Parameters

The device supports configuring the time for RIP timer update, timeout, and garbage collection. By default, the system broadcasts RIP update messages every 30 seconds. When an update message for a route routing protocol command cannot be received after 180 seconds, the route is considered invalid, but the route can still exist in the routing table for 120 seconds, and then the routing table is deleted after 120 seconds. Please configure it under RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Configuring RIP Timer Parameters	timers basic update timeout garbage	
Delete RIP timer parameters	undo timers basic	

[Parameter Description]

update: RIP routing message update time, the configuration range is 5-2147483647 seconds, the default is 30 seconds;

timeout: RIP routing timeout, the configuration range is 5-2147483647 seconds, the default is 180 seconds;

garbage: RIP route garbage collection time, the configuration range is 5-2147483647 seconds, the default is 120 seconds;

[Example]

! Configure RIP route update time to 60 seconds, timeout time to 360 seconds, and garbage collection time to 240 seconds

[GPON-router-rip] timers basic 60 360 240

40.2.16 Create/delete RIP keychain keychain

The device supports configuration of RIP key chains. perform the following configuration under RIP view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Create and enter the keychain keychain view	key chain key-chain-name	If no keychain exists, this command automatically creates a keychain and enters the keychain view.
Remove the keychain configuration	undo key chain *key-chain-name*	

[Parameter Description]

key-chain-name: Key chain name, up to 32 configurable characters;

[Example]

! Create and enter keychaintest

[GPON-router-rip] key chain test

40.2.17 Create/delete RIP keychain keychain-key

After creating a RIP key chain, you can configure the key ID in RIP key chain view.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Go to the keychain keychain view	key chain key-chain-name	
Enter key ID keychain-key view.	key key-number	When the key ID does not exist, this command automatically creates the key ID and enters key ID keychain-key view.
Delete Key ID	undo key key-number	

[Parameter Description]

key-number: key ID, configurable range is 0-2147483647;

[Example]

! Configure the key ID of the keychain test to 12345678

```
[GPON-router-keychain]key 12345678
```

40.2.18 Configure the parameters related to the keychain-key of the RIP keychain

After you create the RIP key chain keychain-key, you can configure the related key parameters.

manipulate	command	clarification
Go to System View	system-view	
Enter RIP view	router rip	
Go to the keychain keychain view	key chain key-chain-name	
Enter key ID keychain-key view.	key key-number	
Configure the password used by the key	key-string *string*	
Remove keyed passwords	undo key-string	
Configure the legal time for key acceptance	accept-lifetime *start-time* { *end-time* | duration *seconds* | infinite }	
Delete the legal time accepted by the key	undo accept-lifetime	
Configure the time when the key is sent	send-lifetime *start-time* { *end-time* | duration *seconds* | infinite}	
Delete the time of sending the key	undo send-lifetime	

[Parameter Description]

string: indicates the configuration key, the maximum configuration can be 16 characters

start-time: start time in HH:MM:SS day Month Year format;

end-time: end time, in the format HH:MM:SS day Month Year;

duration: indicates the total time from the start time to the end time in seconds, with a configuration range of 1-2147483646;

infinite: indicates an infinite time, i.e., it can be effective from the start time onwards;

[Example]

! Configure the password for key ID 12345678 to abcd

```
[GPON-router-keychain]key 12345678
```

[GPON-router-keychain-key]key-string abcd

40.2.19 Monitoring and Maintenance of RIP

RIP-related configuration information can be displayed in any view.

manipulate	command	clarification
Display all routing table information	display ip route	
Display RIP information	display ip route rip	
Display RIP configuration information for an interface	display ip rip interface [loopback-interface { 0 | 1 } | vlan-interface *vlanid* | supervlan-interface *vlanid*]	When no interface is specified, RIP configuration information for all interfaces is displayed
Display RIP status information	display ip rip status	

[Example]

! Display RIP routing table information

[GPON]display ip route rip

! Display RIP status information

[GPON]display ip rip status

! Display RIP configuration information for all interfaces

[GPON]display ip rip interface

Chapter 41 OSPF Configuration

41.1 Introduction to OSPF

OSPF, which stands for Open Shortest Path First, is an internal routing protocol developed by the IETF organization that is based on link state and shortest path first techniques. On IP networks, it dynamically discovers and propagates routes by collecting and transmitting link state from autonomous systems.The OSPF protocol supports interface-based message authentication to ensure the security of routing calculations.The OSPF protocol uses IP multicast to send and receive messages.

OSPF has the following characteristics:

1) Wide range of adaptability, supporting networks of various sizes, up to hundreds of routers;

2) Fast convergence, sending update messages immediately after a topology change in the network so that changes are quickly synchronized in the autonomous system;

3) Support authentication and interface-based message authentication to ensure the security of message interaction and routing calculation;

4) Supports routing hierarchy, using four different types of routes, in order of priority: intra-area routes, inter-area routes, first type of external routes, and second type of external routes;

5) Area segmentation, which allows the network of an autonomous system to be divided into areas to be managed, and the routing information transmitted between areas is further abstracted, thus reducing the occupied network bandwidth;

6) No self-loop, OSPF uses the shortest path tree algorithm to calculate routes based on the collected link states, which guarantees that no self-loop routes will be generated from the algorithm itself;

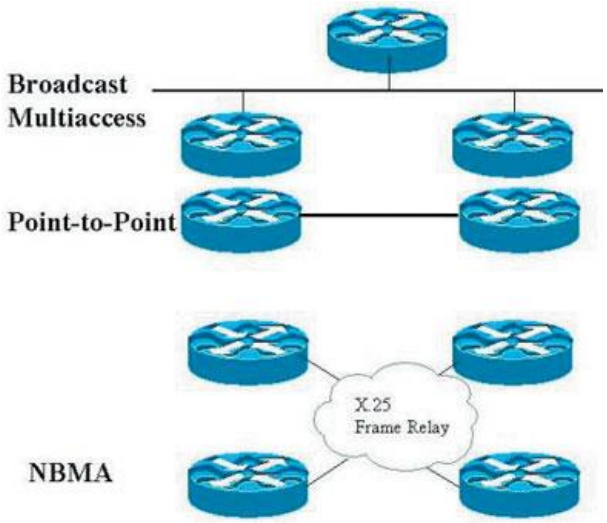
7) Multicast sending, which sends protocol messages at multicast addresses on certain types of links to reduce interference with other devices;

8) Supports Equivalent Routing, supports multiple equivalent routes to the same destination address;

41.1.1 Basic concepts of OSPF

1. OSPF network types

Depending on the physical network to which the router is connected, OSPF classifies the network into four types: BroadcastMultiAccess, NoneBroadcastMultiAccess, Point-to-Point, P2P, Point-to-MultiPoint, and Point-to-MultiPoint. Point-to-MultiPoint (P2MP). Broadcast Multi-Access networks such as: Ethernet, TokenRing, FDDI, NBMA networks such as: FrameRelay, X.25, SMDS, Point-to-Point networks such as: PPP, HDLC.



2. Autonomous System (AS)

An autonomous system is a group of routers that exchange routing information using the same routing protocol, abbreviated AS.

3. OSPF routing process

The OSPF protocol route calculation process is roughly as follows:

1) Each OSPF router generates LSAs (Link State Advertisements,) based on its surrounding network topology.
(link state announcements) and sends the LSAs to other OSPF routers in the network via update messages;

2) Each OSPF router collects the LSAs notified by other routers, and all the LSAs are put together to form the LSDB (Link State Database). the LSA is a description of the network topology around the router, and the LSDB is a description of the network topology of the whole autonomous system;

3) The OSPF router converts the LSDB into a directed graph with routing weights, which is a true reflection of the entire network topology. The directed graph obtained by each router in the network is identical;

4) Each router computes a shortest path tree rooted at itself based on the directed graph using the SPF algorithm, which gives the routes to the nodes in the autonomous system.

4. Router ID number

The RID (Router ID, Router ID) must exist if the router is to run the OSPF protocol.

RIDs can uniquely identify a router in an autonomous system.RIDs can be manually configured or automatically generated.

If no RID is specified by command, a RID is automatically generated in the following order:

1) If the current device is configured with a Loopback interface, the IP address with the largest IP address value on all Loopback interfaces will be selected as the RID;

2) If the current device does not have a Loopback interface configured, the IP address with the largest value among all configured IP addresses on the interface with a valid link is selected as the RID;

5. Designated router (DR) and backup designated router (BDR)

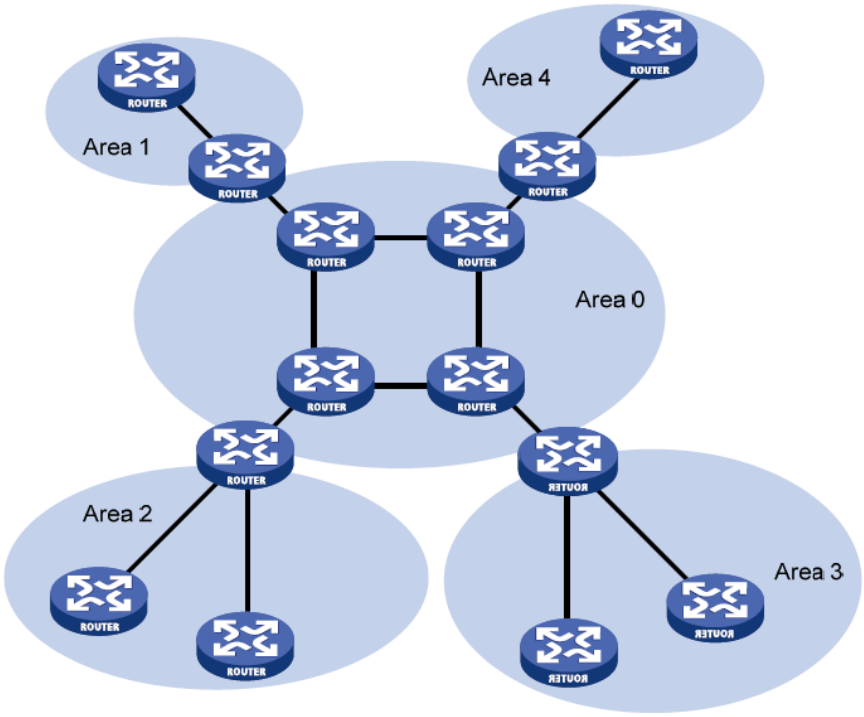
Multiple routers may exist on a multi-access network, and to avoid the large overhead associated with establishing full adjacency between routers, OSPF requires that a DR (Designated Router) be elected in the area. Each router establishes a full-adjacency relationship with it. the DR is responsible for collecting all link-state information and distributing it to other routers. The election of a DR also elects a BDR (Backup DesignatedRouter), which assumes the duties of the DR in the event of a DR failure.

Point-to-point type of network does not require DR as there are only two nodes, which are completely adjacent to each other. Protocol Components The OSPF protocol consists of Hello protocol, switching protocol, and diffusion protocol.

6. OSPF regionalization

OSPF protocol introduces the concept of "hierarchical routing", the network will be divided into a "trunk" connected to a group of independent parts, these independent parts are called "area" (Area), "trunk" part is called "trunk area" (Area 0). Each area is like a separate network, and the OSPF router in that area only keeps link state for that area. Each router's link-state database can be kept reasonably large, and the route calculation time and number of messages will not be too large.

The OSPF regions are divided as shown below:



7. OSPF router types

OSPF routers can be categorized into the following four groups depending on their location in the AS:

1) Intra-area Router (Internal Router)

All interfaces of this class of router belong to the same OSPF area.

2) Area Border Router ABR (Area Border Router)

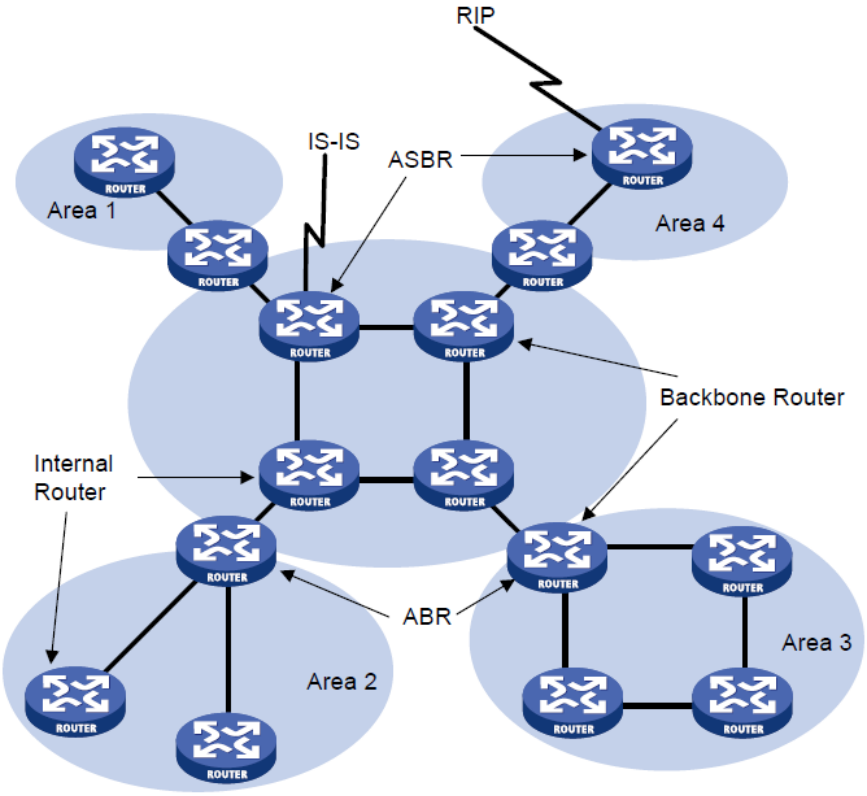
This type of router can belong to more than two areas at the same time, but one of them must be a backbone area (see the next subsection for a description of backbone areas.) The ABR is used to connect a backbone area to a non-backbone area, and it can be either physically or logically connected to the backbone area.

3) Backbone Router (Backbone Router)

Routers in this category have at least one interface that belongs to the backbone area. Therefore, all ABRs and internal routers located in Area0 are backbone routers.

4) Autonomous System Border Router ASBR

A router that exchanges routing information with other ASes is called an ASBR. an ASBR is not necessarily located at the boundary of an AS; it can be an in-area router or an ABR. an OSPF router becomes an ASBR as soon as it introduces information for external routes.



8. OSPF protocol messages

OSPF has five types of protocol messages:

1) Hello message: Hello is sent periodically to discover and maintain OSPF neighbor relationships. The main contents of the message include the timer value, DR (Designated Router), BDR (Backup DesignatedRouter) and its own OSPF neighbor information;

2) DD (Database Description) message: the message contains the summary information of each LSA in the local LSDB, which is used for database synchronization between the two routers;

3) LSR (Link State Request) message: the content of the message contains the summary information of the required LSA. After the two routers exchange DD messages with each other, the router sends LSR messages to request the missing LSAs in the local LSDB;

4) LSU (Link State Update) message: sends the LSA it needs to the other party;

5) LSAck (Link State Acknowledgment) message: used to acknowledge the received LSA. The content is the header of the LSA to be acknowledged (one message can acknowledge multiple LSAs);

9. Types of LSAs

The descriptions of link state information in OSPF are encapsulated in LSAs and published. the following types of LSAs are commonly used:

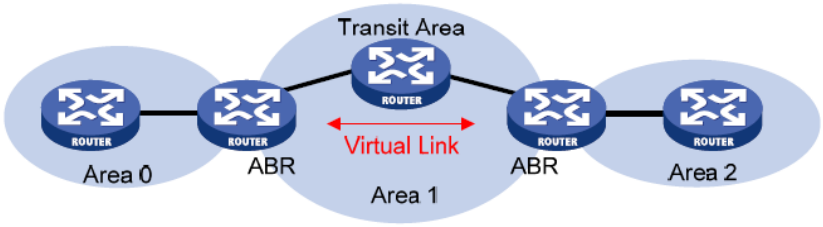
1) Router LSA (Type1): generated by each router, describes the link state and overhead of the router, and is propagated in the area from which it originates;

2) Network LSA (Type2): Generated by the DR, it describes the link status of all routers in this segment and is propagated in the area from which it originates;

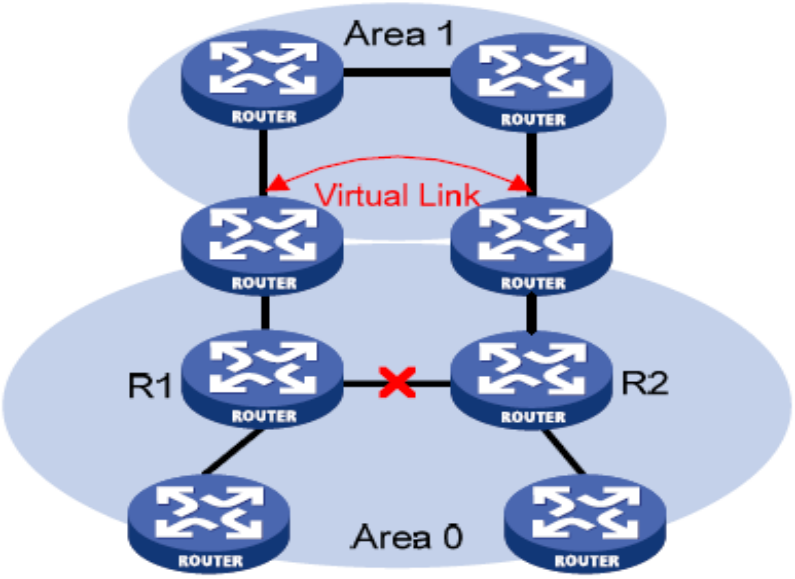
3) Network Summary LSA (Type3): Generated by ABR (Area Border Router), it describes the routes of a segment within an area and advertises them to other areas;

4) ASBR Summary LSA (Type4): Generated by ABR, it describes the routes to ASBR (Autonomous System Boundary Router) and notifies the relevant areas;

5) AS External LSA (Type5): generated by the ASBR, describes routes to the outside of the AS (Autonomous System), advertised to all areas (except Stub areas and NSSA areas);
6) NSSA External LSA (Type7): generated by an ASBR in the NSSA (Not-So-Stubby Area) area, describes routes to the outside of the AS and is propagated only within the NSSA area.
10. Neighbors and adjacencies
Neighbor and Adjacency are two different concepts in OSPF. an OSPF router starts up and sends a Hello message out through the OSPF interface. The OSPF router that receives the Hello message checks the parameters defined in the message and forms a neighbor relationship if both sides agree. Neighbors may not always form an adjacency relationship, depending on the network type. Only when both sides successfully exchange DD messages, exchange LSAs, and achieve LSDB synchronization can they form a real sense of neighbor relationship.
11. Backbone areas and virtual connections
1) Backbone Area (Backbone)
After OSPF delineates areas, not all areas are equally related. One of the areas is different, its Area ID is 0, usually called the backbone area. The backbone area is responsible for routing between areas, and routing information between non-backbone areas must be forwarded through the backbone area. OSPF has two rules for this:
-> All non-backbone areas must remain connected to the backbone;
-> The backbone region itself must also remain connected;
However, in practice, it may not be possible to meet this requirement due to the limitations of various conditions. This can be solved by configuring OSPF Virtual Link.
2) Virtual Link (VL)
A virtual connection is a logical connection channel between two ABRs through a non-backbone area. It must have ABRs at both ends and must be configured at both ends to take effect. The area that provides an internal non-backbone area route for both ends of the virtual connection is called the Transit Area.
In the following figure, there is no directly connected physical link between Area2 and the backbone area, but a virtual connection can be configured on the ABR to keep Area2 connected to the backbone area over a logical link.



In addition, another application of virtual connections is to provide redundant backup links, so that when the backbone area cannot remain connected due to a link failure, the logical connectivity of the backbone area can still be ensured through a virtual connection.
A virtual connection is equivalent to forming a point-to-point connection between two ABRs, so on this connection, as on a physical interface, you can configure the various parameters of the interface, such as the interval between sending Hello messages.



12. STUB region

Stub areas are specific areas where ABRs in the Stub area are not allowed to note Type5 LSAs. the size of the router's routing table as well as the amount of routing information delivered is greatly reduced in these areas.

To further reduce the size of the routing table and the amount of routing information passed to routers in a Stub area, the area can be configured as a Totally Stub area, where the ABRs in the area do not pass inter-area routing information and external routing information to this area.

The (Totally) Stub region is an optional configuration attribute, but not every region qualifies for configuration. Typically, (Totally) Stub regions are located at the boundaries of autonomous systems.

To ensure that routes to other areas of this autonomous system or outside the autonomous system remain reachable, the ABR in this area will generate a default route and advertise it to other non-ABR routers in the area. The following points should be noted when configuring (Totally) Stub areas:

1) Backbone areas cannot be configured as (Totally) Stub areas;

2) If an area is to be configured as a Stub area, all routers in the area must be configured with the stub command;

3) To configure an area as a Totally Stub area, all routers in the area must be configured with the stub command order, the ABR routers in this area need to be configured with the stub [no-summary] command;

4) (Totally) No ASBR can exist in the Stub area, i.e., routes from outside the autonomous system cannot be propagated in this area;

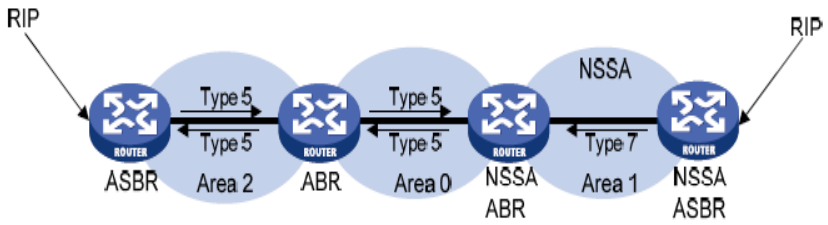
5) Virtual connections cannot cross (Totally) Stub areas;

13. NSSA region

The NSSA (Not-So-Stubby Area) area is a variant of the Stub area and has many similarities with the Stub area.The NSSA area also does not allow Type5 LSA injection, but it can allow Type7 LSA injection.Type7 LSAs are generated by the ASBR of the NSSA area and propagate within the NSSA area. When the Type7 LSA reaches the ABR of the NSSA, the ABR converts the Type7 LSA to Type5 LSA, which propagates to other regions.

As shown in the figure below, the autonomous system running the OSPF protocol consists of three areas: area 1, area 2, and area 0, and the other two autonomous systems run the RIP protocol. Area 1 is defined as an NSSA area, and the RIP routes received by Area 1 are propagated to NSSA ASBR, which generates Type7 LSAs to be propagated in Area 1, and when Type7 LSAs reach NSSA ABR, they are converted into Type5 LSAs to be propagated to Area 0 and Area 2.

On the other hand, RIP routes from an autonomous system running RIP propagate through the OSPF autonomous system by generating Type5 LSAs through the ASBR in area 2. However, Type5 LSAs do not reach Area 1 because Area 1 is an NSSA area. as with Stub areas, virtual connections cannot cross NSSA areas.



14. Route aggregation

Route aggregation is when an ABR or ASBR aggregates routing information with the same prefix to publish only one route to other areas.

After the AS is divided into different areas, each area is connected through an OSPF border router (ABR). Inter-area routing aggregation can be used to reduce routing information, reduce the size of the routing table, and improve the router's computing speed.

After calculating the intra-area routes for an area, the ABR aggregates multiple of these OSPF routes into a single one to be sent outside the area according to the aggregation-related settings.

For example, there are two network segments in a region as follows:

192.168.1.0 255.255.255.0

192.168.2.0 255.255.255.0

Can be aggregated into one segment: 192.168.0.0 255.255.0.0

Once an aggregated segment of a network is added to an area, all internal routes for IP addresses in that area that fall within this aggregated segment are no longer broadcast independently to other areas, but only broadcast summary information about the routes of the entire aggregated segment.

If the range of this segment is qualified with the keyword noadvertise, summary information about routes to this segment will not be broadcast. This network segment is described by way of an IP address/mask. Receiving aggregated network segments and qualifying this segment reduces the amount of inter-area routing information exchanged.

Note: Route aggregation is effective only when configured on the ABR.

41.1.2 Protocol flow of OSPF

The OSPF protocol processing flow consists of the following five main steps:

1. Step 1: Establish router adjacencies

Adjacency is a relationship that OSPF routers establish between selected neighboring routers for the purpose of exchanging routing information. A router first sends a Hello message with its own RID information. A neighboring router that receives this Hello message adds the RID information within this message to its own Hello message.

If a port on a router receives a Hello message containing its own RID information from another router, it determines whether it can establish an adjacency based on the type of network in which the port is located.

In a point-to-point network, the router will establish a direct neighbor relationship with the peer router, and the router will proceed directly to the third step of the operation: discovering other routers. In the case of a BroadcastMultiAccess network, the router will proceed to the election step.

2. Step 2: Election of the DR/BDR

Different types of networks elect DR and BDR in different ways.

BroadcastMultiAccess networks support multiple routers, in which case OSPF needs to be established as the central node for link state and LSA updates. The election is determined using the RID and Priority field values within the Hello message. The Priority field value is sized from 0 to 255, and the router with the highest priority becomes the DR. If the priority values are the same size, the router with the highest RID value is elected as the DR, and the router with the next highest priority is

elected as the BDR. Both the priority and ID values can be manually configured as needed.

3. Step 3: Discover the router

In this step, the router and the router first confirm the master-slave relationship using the RID information of the Hello message, and then the master-slave routers exchange part of the link state information with each other. Each router analyzes and compares the information, and if there is something new in the received information, the router will ask the other party to send the complete link state information. After this state is completed, a full adjacency (FullAdjacency) relationship is established between routers, while neighboring routers have their own independent and complete link state database.

Within the BroadcastMultiAccess network, the DR exchanges information with the BDR and simultaneously exchanges link status information with other routers within this subnet.

In a Point-to-Point or Point-to-MultiPoint network, link state information is exchanged between neighboring routers.

4. Step 4: Choose the appropriate router

When a router has a complete and independent link-state database, it uses the SPF algorithm to calculate and create a routing table. the OSPF router independently uses the SPF algorithm to calculate paths to each destination network based on the contents of the link-state database and stores the paths in the routing table.

OSPF calculates the destination path using a measure (Cost), and the shortest path is the one with the smallest Cost. When configuring an OSPF router, you can set the Cost of a link according to the actual situation, such as link bandwidth, delay, or economic costs.The smaller the Cost, the greater the likelihood that the link will be selected as a route.

5. Step 5: Maintain routing information

When the link state changes, OSPF informs the other routers on the network through the Flooding process.An OSPF router that receives a link state update message with the new information will update its own link state database and then recalculate the routing table using the SPF algorithm. During the recalculation process, the router continues to use the old routing table until SPF completes the new routing table calculation. The new link state information will be sent to other routers. It is important to note that OSPF routing information is automatically updated even if the link state has not changed, which is 30 minutes by default.

41.2 Configuration of OSPF

41.2.1 OSPF Configuration Task List

In each configuration task, you must start OSPF before you can configure other functional features. The configuration of features related to Layer 3 interfaces is not restricted by whether OSPF is enabled or not. Note that after shutting down OSPF, the original Layer 3 interface parameters remain and take effect the next time you start OSPF.

The list of OSPF configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable OSPF function	compulsory	41.2.2
Configure the RID number of the router	compulsory	41.2.3
Specify the IP interface to run the OSPF function	compulsory	41.2.4
Configure the authentication type of the zone	selectable	41.2.5
Configure the interface type	selectable	41.2.6
Configure the interface to ignore MTU checks	selectable	41.2.7
Configuring Interface Overhead	selectable	41.2.8
Setting the interface in DR priority	selectable	41.2.9

Set the interface Hello message sending interval	selectable	41.2.10
Setting the Failure Time Between Interface Neighboring Routers	selectable	41.2.11
Setting the interval for retransmission of LSAs by the interface's neighboring routers	selectable	41.2.12
Set the transmission delay time for LSU messages sent by the interface	selectable	41.2.13
Configuring Interface Message Authentication	selectable	41.2.14
Configuring the Interface BFD Monitoring Link Status Function	selectable	41.2.15
Configure the STUB area for OSPF	selectable	41.2.16
Configure the NSSA area for OSPF	selectable	41.2.17
Configuring OSPF Area Route Aggregation	selectable	41.2.18
Configuring OSPF Virtual Connections	selectable	41.2.19
Configure OSPF to introduce external routes	selectable	41.2.20
Configure OSPF to introduce default routes	selectable	41.2.21
Configuring OSPF to Introduce External Routes Default Spend	selectable	41.2.22
Configuring OSPF Route Filtering	selectable	41.2.23
Configuring OSPF Routing Administrative Distance	selectable	41.2.24
Configuring OSPF Neighbor Routers for Interconnected NBMA Networks	selectable	41.2.25
OSPF monitoring and maintenance	selectable	41.2.26

41.2.2 Enable/disable OSPF function

By default, the device disables the OSPF function. please configure it in system view.

manipulate	command	clarification
Go to System View	system-view	
Initiate RIP protocol	router ospf	
Disabling the RIP protocol	undo router ospf	

[Example]

! Start the OSPF protocol

[GPON]router ospf

41.2.3 Configure the RID of the router

The router ID is a 32-bit unsigned integer that uniquely identifies a router in the autonomous system, and the user must configure the router ID number. When manually configuring the router ID, you must ensure that no two routers in the autonomous system have the same ID. It is common practice to configure the router ID to match the IP address of one of the router's interfaces.

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Configuring the Router ID	router id *router-id*	
Cancel Router ID	undo router id	

[Example]

! Configure the router ID used by the device to run OSPF to 192.168.1.100

[GPON]router id 192.168.1.100

41.2.4 Specify that the IP interface is running the OSPF protocol

The OSPF task must also specify on which network segment it is to be applied after it is started and configure the region to which it belongs.

The OSPF protocol further divides the autonomous system into different areas (Areas), which are logical groups of routers. Some routers may belong to different areas (such routers are called Area Boundary Routers ABRs), while a network segment can only belong to one area, or each interface running the OSPF protocol must be specified to belong to a particular area, which is identified by an area number. Routing information is passed between different areas through ABRs. In addition, all routers within the same area should agree on the configuration of the parameters for that area. Therefore, when configuring routers within the same area, you should be aware that most configuration data should be considered uniformly on an area basis. Wrong configuration may result in neighboring routers not being able to pass information to each other, or even lead to the blocking of routing information or self-loop. Please perform the following configuration under OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Specifies that the interface runs the OSPF protocol and specifies the area code	network ipaddress wildcard-mask area area-id	Area-id can be configured as a decimal number with a configuration range of 0-4294967295. or in the form of an IP address.
Remove the interface from running the OSPF protocol	undo network ipaddress wildcard-mask area area-id	

[Example]

! Specifies that OSPF is running on the interface with IP address 192.168.1.100, specifying area 0

[GPON-router-ospf] network 192.168.1.1000.0.0.255 area 0

41.2.5 Configure the authentication type of the zone

The authentication type must be the same for all routers in an area (no authentication support, plaintext authentication support, MD5 ciphertext authentication support). please configure it under OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configure the authentication type of the zone	area *area-id* authentication [message-digest]	MD5 authentication is not enabled by default
Type of authentication for the de-regionization	undo area *area-id* authentication	

[Example]

! Configure the authentication method for OSPF area 0 as MD5 authentication

[GPON-router-ospf]area 0 authentication message-digest

41.2.6 Configure the interface type

The OSPF protocol calculates routes based on the topology of the networks neighboring this router. Each router describes the topology of its own neighboring networks and passes it on to all other routers.OSPF classifies networks into four types, depending on the physical network to which the router is connected: BroadcastMultiAccess, NoneBroadcastMultiAccess (NBMA), Point-to-Point (P2P), and Point-to-MultiPoint (P2MP):

1) BroadcastMultiAccess type: when the link layer protocol is Ethernet, FDDI, OSPF considers the network type to be BroadcastMultiAccess by default;

2) Non-Broadcast Multiple Access Type: when the link layer protocol is ATM, OSPF considers the network type to be NBMA by default;

3) Point-to-Multipoint type: no link layer protocol is considered a Point-to-Multipoint type by default. Point-to-Multipoint must be a mandatory change from another network type. The most common practice is to change a non-fully connected NBMA to a Point-to-Multipoint network;

4) Point-to-Point Type: when the link layer protocol is PPP, LAPB, or POS, OSPF considers the network type to be P2P by default;

NBMA networks are nonbroadcast, multipoint reachable networks, more typically ATM. the polling interval can be configured to specify the period of time that a router sends a polled Hello message before forming an adjacency with an adjacent router. On a broadcast network without multiple-access capability. the interface can be configured in the nonbroadcast mode. The interface can be configured as P2MP if it is not directly reachable between all routers in the NBMA network. The interface type can also be changed to point-to-point if the router has only one peer in the NBMA network.

The difference between NBMA and point-to-multipoint:

1) In the OSPF protocol NBMA refers to those fully connected, non-broadcast, multipoint reachable networks. Point-to-multipoint networks, on the other hand, do not necessarily need to be fully connected;

2) Election of DR & BDR is required on NBMA whereas there is no DR & BDR in point-to-multipoint network;

3) NBMA is a default network type, e.g., if the link layer protocol is ATM, OSPF will by default consider the network type of the interface to be NBMA (regardless of whether the network is fully connected or not). Point-to-multipoint is not the default network type; no link layer protocol is considered point-to-multipoint; point-to-multipoint must be forced to change by some other network type. The most common practice is to change a non-fully connected NBMA to a point-to-multipoint network;

4) NBMA sends messages with unicast, and you need to configure neighbors manually. Point-to-multipoint uses multicast to send messages; because the link layer protocol of the device is Ethernet, OSPF considers the network type to be broadcast.

in general, please do not change its network type. Please perform the following configurations under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the interface type	ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }	Defaults to the broadcast type
Restore the default interface type	undo ip ospf network	

[Example]

! Set VLAN interface 100 to broadcast type

```
[GPON-vlanInterface-100]ip ospf network broadcast
```

41.2.7 Configure the interface to ignore MTU checks

By default, when performing DD message exchange, the device checks the MTU size of DD messages. The device supports enabling or disabling the check MTU function. Please perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the interface to ignore MTU checks	ip ospf mtu-ignore [*ipaddress*]	
Cancel Interface Ignore MTU Check	undo ip ospf cost mtu-ignore [*ipaddress*]	The default configuration is to check the MTU size

[Example]

ipaddress: interface IP address, when no IP address is specified, it means to set all IP addresses of the interface;

The system enables MTU checking for interfaces by default, i.e., MTU checking is not ignored.

[Example]

! Enable MTU checking on VLAN interface 100

```
[GPON-vlanInterface-100] ip ospf mtu-ignore
```

41.2.8 Configuring Interface Overhead

The system supports setting the overhead for an interface to send messages. otherwise OSPF defaults to an overhead of 10 for the interface. perform the following configuration in Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring Interface Overhead	ip ospf cost *cost*	The cost configuration range is 0-65535, and the default value is 10
Restore the default interface type	undo ip ospf cost	

[Example]

! Set the cost of VLAN interface 100 to 20

```
[GPON-vlanInterface-100] ip ospf cost 20
```

41.2.9 Configuring Interface DR Priority

The priority of a router interface determines its eligibility for election as a Designated Router, with the higher priority being considered first in the event of an election conflict. The Designated Router (DR) is not assigned artificially, but is elected by all routers in the segment. All routers in the segment with Priority > 0 are candidates. Among all the routers claiming to be the DR, the one with the largest priority value is elected; if the priority values of two routers are equal, the one with the largest Router ID is elected as the DR. The ballot is the Hello message, and each router writes its elected DR into the Hello and sends it to each router on the network segment. When two routers connected to the same segment simultaneously

announce that they are the Designated Router (DR), the one with the highest priority wins. If the priorities are equal, the router with the largest router ID wins. If a router has priority 0, it is not elected as the Designated Router (DR) or Backup Designated Router (BDR). If the DR fails due to some kind of failure, the routers in the network must re-elect the DR and synchronize with the new DR. This takes a long time, during which time the routes are calculated incorrectly. To shorten this process, OSPF introduced the concept of a BDR (Backup Designated Router), which is actually a backup to the DR, and elects the BDR at the same time as the DR, which also establishes adjacencies and exchanges routing information with all routers in the network segment. When the DR fails, the BDR becomes the DR immediately, and the process is very short because there is no need to reelect and the neighbor relationship has been established beforehand. Of course, a new BDR needs to be reelected, which takes a longer time but does not affect the route calculation. Please perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring Interface DR Priority Overhead	ip ospf priority *priority*	The priority configuration range is 0-255, and the default value is 1
Restore the default interface type	undo ip ospf priority	

[Example]

! Set the DR priority of VLAN interface 100 to 100

[GPON-vlanInterface-100] ip ospf priority 100

Attention:

- The DR in a network segment is not necessarily the router with the largest priority; similarly, the BDR is not necessarily the router with the second largest priority. If a new router joins after the DR and BDR have already been selected, it will not become the DR in the segment even if it has the largest priority value.
- DR is a mid-segment concept that is specific to a router's interfaces. A particular router may be DR on one interface, BDR on another, or DROther.
- DR is only elected for broadcast or NBMA type interfaces, and is not required on point-to-point or point-to-multipoint type interfaces.

41.2.10 Configure the interface Hello message sending interval

The Hello message is the most common type of message that is periodically sent to neighboring routers for the purpose of discovering and maintaining neighbor relationships, electing DRs and BDRs.The user can set the value of the hello-interval at which the Hello message is sent.The smaller the hello-interval, the faster a change in the network will be detected, but the more network transmissions it will take to send the hello-interval to the neighboring routers. network transmission. Routers on the same network segment must have the same hello-interval. When a router first boots up, it sends Hello messages only to neighbors with priority greater than 0 (those routers that are likely to be elected as DRs, BDRs). After the DRs and BDRs in the segment are elected, the DRs and BDRs send Hello messages to all neighbors to establish adjacency. Perform the following configuration in Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the interface Hello message sending interval	ip ospf hello-interval *seconds*	seconds is configured in the range of 0-65535 seconds, and the default value is 10 seconds.
Restore the default interface Hello message sending interval	undo ip ospf hello-interval	

[Parameter Description]

seconds: time interval, configuration range is 0-65535

By default the value of the time interval for sending Hello messages for point-to-point, broadcast type interfaces is 10 seconds.

The value of the time interval for point-to-nultipoint, nonbroadcast type interfaces to send Hello messages is 30 seconds.

[Example]

! Set the Hello message sending interval for VLAN interface 100 to 20 seconds

[GPON-vlanInterface-100] ip ospf hello-interval 20

41.2.11 Configure the failure time between neighboring routers of an interface

The expiration time between neighboring routers means that if no Hello message is received from the other side within this time interval, the opposite router is considered to be expired. Users can set the value of dead-interval of neighboring routers. the value of dead-interval is at least 4 times the value of Hello-interval, and the dead-interval of routers in the same network segment must be the same as well. Perform the following configuration in Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the failure time between neighboring routers of an interface	ip ospf dead-interval *seconds*	seconds is configured in the range of 1-65535 seconds, and the default value is 40 seconds.
Restore the default interface neighbor router-to-router failure time	undo ip ospf dead-interval	

[Parameter Description]

seconds: time interval, configurable from 1-65535.

The value of dead-interval is at least four times the value of Hello-interval. by default, the value of dead-interval between neighboring routers for point-to-point and broadcast type interfaces is 40 seconds. the value of dead-interval between neighboring routers for point-to-nultipoint and nonbroadcast type interfaces is 120 seconds. The value of the failure time between neighboring routers for point-to-nultipoint and nonbroadcast type interfaces is 120 seconds.

[Example]

! Set the neighboring router expiration time for VLAN interface 100 to 60 seconds

[GPON-vlanInterface-100] ip ospf dead-interval 60

41.2.12 Configure the interface neighbor router retransmission LSA interval

When a router sends a Link State Announcement (LSA) to its neighbors, it needs to wait for an acknowledgement message from the other side. If no acknowledgement is received within the retransmit-interval, the LSA will be retransmitted to the neighbor. you can set the value of retransmit-interval. Please perform the following configurations under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the interface retransmission LSA interval	ip ospf retransmit-interval *seconds*	seconds is configured in the range of 1-65535 seconds, with a default value of 5 seconds
Restore the default interface retransmission LSA interval	undo ip ospf retransmit-interval	

[Parameter Description]

seconds: time interval, the configuration range is 1-65535, the default value is 5 seconds.

[Example]

! Set the LSA retransmission interval for VLAN interface 100 to 15 seconds

```
[GPON-vlanInterface-100]ip ospf retransmit-interval 15
```

41.2.13 Configure the transmission delay time for LSU messages sent by the interface

The aging time of the link state broadcast (LSA) in LSU messages is increased by a transmission delay time before transmission. The setting of this parameter takes into account the time required to send the message on the interface. the LSAs age with time (plus 1 every second) in the router's Link State Database (LSDB) but not during transmission in the network. it is necessary to increase the aging time by the transmission delay time of the message before transmitting it. and this configuration is more important for low speed networks. Please perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the transmission delay time for LSU messages sent by interface interfaces	ip ospf transmit-delay *seconds*	seconds is configured in the range of 1-65535 seconds, and the default value is 1 second.
Restore the transmission delay time for LSU messages sent by the default interface	undo ip ospf transmit-delay	

[Parameter Description]

seconds: time interval, the configuration range is 1-65535, the default value is 1 second.

[Example]

! Set the transmission delay for VLAN interface 100 to 5 seconds

```
[GPON-vlanInterface-100]ip ospf transmit-delay 5
```

41.2.14 Configuring Interface Message Authentication Function

OSPF supports plaintext authentication or MD5 ciphertext authentication between neighboring router interfaces. Please perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the interface message authentication method	ip ospf authentication [null | *ipaddress* | message-digest [*ipaddress*]]	The default interface does not use any message authentication
Restore the interface default message authentication method	undo ip ospf authentication [*ipaddress*]	
Configure the interface plaintext authentication password	ip ospf authentication-key *password* [*ipaddress*]	The password can be configured up to 8 characters.
Cancel the interface explicit authentication password	undo ip ospf authentication-key [*ipaddress*]	
Configure the interface MD5 authentication password	ip ospf message-digest-key *key-id* md5 *key* [*ipaddress*]	
Cancel interface MD5 authentication password	undo ip ospf message-digest-key *key-id* [*ipaddress*]	

[Parameter Description]

null: Indicates that no message authentication method is used, and the interface is not configured with authentication methods by default;

ipaddress: interface IP address, specifies that a certain IP address of this interface is configured for message authentication, when no IP address is entered, it means that all IP addresses of this interface are configured for this authentication method, this parameter mainly takes into account that Layer 3 interfaces can be configured with multiple IP addresses;

message-digest: MD5 authentication method;

password: plaintext authentication password, configurable from 1-8 strings;

key-id: Keyid of MD5, configurable as an integer from 1-255;

key: The key of the MD can be configured as a string of 1-16;

[Example]

! Set the explicit authentication password for VLAN interface 100 to abcd1234

```
[GPON-vlanInterface-100]ip ospf authentication-key abcd1234
```

41.2.15 Configuring the Interface BFD Monitoring Link Status Function

OSPF uses the Hello protocol to monitor the status of links and is slow to monitor link failures and update neighbors and routes. Enabling BFD improves the speed at which OSPF discovers link failures, dismantles neighbor relationships, and updates routes.See the BFD section for a detailed description of BFD-related features.

This function is not enabled by default. Note that the devices at both ends of the monitored link must enable this function under the corresponding interfaces to successfully detect the status of the link. Please perform the following configuration in Layer 3 interface mode.

manipulate	command	clarification
Go to System View	system-view	

Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Enable interface BFD function	ip ospf bfd	
Disable interface BFD function	undo ip ospf bfd	

[Example]

! Enabling BFD on VLAN interface 100

[GPON-vlanInterface-100] ip ospf bfd

41.2.16 Configure the STUB area for OSPF

STUB areas are specific LSA areas where ABRs in STUB areas do not propagate routes they receive external to the autonomous system, and where the size of a router's routing table as well as the amount of routing information delivered is greatly reduced.

The STUB region is an optional configuration attribute, but not every region qualifies for configuration. Typically, STUB areas are located at the boundaries of an autonomous system and are non-backbone areas that have only one ABR; or the area has multiple ABRs, but there are no virtual connections configured between these ABRs. To ensure that routes to the outside of the autonomous system remain reachable, the ABR in the area generates a default route (0.0.0.0) and advertises this default route to other non-ABR routers in the area.

By default, no STUB area is configured and the cost value of the default route sent to the STUB area is 1. Please configure the following under OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configure an area as a STUB area	area *area-id* stub [no-summary]	
Eliminate the STUB region configuration	undo area *area-id* stub [no-summary]	
Configure the spend value for the default route sent to the STUB area	area *area-id* default-cost *cost*	The cost configuration range is 0-16777215, and the default value is 1
Cancel the spend value sent to the default route in the STUB area	undo area *area-id* default-cost	

[Parameter Description]

cost: The cost configuration range is 0-16777215 and the default value is 1;

no-summary: This parameter is to further reduce the number of Link State Announcements (LSAs) sent into the STUB area. When the no-summary option is configured, the ABR is prohibited from sending SummaryLSAs (LSA type 3) into the STUB area;

[Example]

! Configure area 192.168.1.100 as a STUB area and assign its default route spend to 5

[GPON-router-ospf]area 192.168.1.100 stub

[GPON-router-ospf]area 192.168.1.100 default-cost 5

41.2.17 Configure the NSSA area for OSPF

Since there is no any AS external routing information in the STUB area, reachability to external destinations is guaranteed by default routing. In order to improve networking flexibility while maintaining the advantages of STUB areas, RFC 1587 defines a new type of area: the NSSA area (Not-So-Stubby Area). This type of area enables the introduction of AS external routes in a restricted manner. the NSSA is actually an extension of the STUB area, and it shares many similarities with the STUB area. Perform the following configuration in OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configure an area as an NSSA area	area *area-id* nssa [no-summary]	
Cancel NSSA region configuration	undo area *area-id* nssa [no-summary]	
Configure the spend value for default routes sent to NSSA areas	area *area-id* default-cost *cost*	The cost configuration range is 0-16777215, and the default value is 1
Cancel the spend value for the default route sent to the NSSA area	undo area *area-id* default-cost	

[Parameter Description]

cost: The cost configuration range is 0-16777215 and the default value is 1;

no-summary: This parameter is to further reduce the number of Link State Announcements (LSAs) sent into the NSSA area. When the no-summary option is configured, the ABR is prohibited from sending SummaryLSAs (LSA type 3) into the NSSA area;

[Example]

! Configure area 192.168.1.100 as an NSSA area and assign its default route spend to 5

[GPON-router-ospf]area 192.168.1.100nssa

[GPON-router-ospf]area 192.168.1.100 default-cost 5

41.2.18 Configuring OSPF Area Route Aggregation

Route aggregation means that routing information with the same prefix can be aggregated together by the ABR to publish only one route to other areas. An area can be configured with multiple aggregated segments so that OSPF can aggregate multiple segments. the ABR generates Sum_net_Lsa (Type 3 LSA) on a segment-by-segment basis when it sends routing information to other areas. If there are a number of contiguous segments in the area. you can use the area range command to aggregate these contiguous segments into a single segment. In this way, the ABR sends only one aggregated LSA, and all LSAs that fall within the range of aggregated segments specified by this command are no longer sent out individually, which reduces the size of the link-state database (LSDB) in other areas. Please perform the following configuration under OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configuring OSPF Route Aggregation	area area-id range ip-address/mask-length [advertise | notadvertise] [substitute ip-address/mask-length]	Route aggregation is not configured by default

Deleting an OSPF Route Aggregation	undo area area-id range ip-address/mask-length [substitute ip-address/mask-length]	

[Parameter Description]

ip-address/mask-length: prefix address (dotted decimal) and mask length, such as 192.168.1.0/24;

advertise: advertise the area, advertise is the default;

notadvertise: Do not advertise the area;

substitution: notify this area as another prefix;

[Example]

! Aggregate two routes 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 into one 192.168.0.0 255.255.0.0

[GPON-router-ospf] area 1range 192.168.0.0 255.255.0.0

41.2.19 Configuring OSPF Virtual Connections

After OSPF delineates areas, not all areas are equally related. One area is unique in that it has an area-id of 0.0.0.0 and is commonly referred to as a Backbone Area. OSPF routing updates between non-backbone areas are exchanged through the backbone area.The OSPF protocol states that all non-backbone areas must be connected to the backbone area, i.e., at least one port on the ABR should be in area 0.0.0.0. If an area does not have a direct physical connection to backbone area 0.0.0.0, a virtual connection must be established. If physical connectivity may not be guaranteed due to network topology constraints, this requirement can be met by creating a virtual connection. A virtual connection is a logically connected channel between two ABRs through an area that is not routed within the backbone area. It must have ABRs on both ends and must be configured on both ends simultaneously to take effect. The virtual connection is identified by the ID number of the router on the opposite end. The area that provides a non-backbone intra-area route to both ends of the virtual connection is called the Transit Area, and its area number must also be specified at the time of configuration. The virtual connection is activated after the route through the Transit Area has been calculated, which is equivalent to forming a point-to-point connection between the two endpoints, and therefore, on this connection, as on the physical interface, you can configure the parameters of the interface, such as the sending of HELLO message intervals, and so on.

A "logical channel" means that multiple routers running OSPF between two ABRs only play the role of forwarding messages (since the destination addresses of protocol messages are not those of the routers, these messages are transparent to them, and are just forwarded as normal IP messages), and the routing information is passed directly between the two ABRs. routing information between the two ABRs. The routing information here refers to the type3 LSAs generated by the ABRs, and the synchronization of the routers in the area is not changed as a result.

Note: If the autonomous system is divided into more than one area, one area must be the backbone area and ensure that the other areas are directly or logically connected to the backbone area and that the backbone area itself is connected. You must configure the authentication method for area 0 before you can configure the authentication method for a virtual connection. Perform the following configuration in OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configuring OSPF Virtual Connections	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* } } *]	
Delete the OSPF virtual connection	undo area *area-id* virtual-link *router-id*	

[Parameter Description]

hello-interval: the configuration range is 1-65535, and the default is 10 seconds;
retransmit- interva: Configuration range is 1-65535, default is 5 seconds;
transmit-delay: the configuration range is 1-65535, and the default is 1 second;
authentication-key: authentication password, configurable from 1-8 strings;
key-id: Keyid of MD5, configurable as an integer from 1-255;
key: The key of the MD can be configured as a string of 1-16;
[Example]
! Configure a virtual connection with a translation area of 1.1.1.1 and a router-id of 192.168.1.200 on the opposite end of the router

[GPON-router-ospf] area 1.1.1.1 virtual-link 192.168.1.200

41.2.20 Configure OSPF to introduce external routes

The dynamic routing protocols on a router can share routing information with each other. routes discovered by other routing protocols are always treated as routing information external to the autonomous system due to the nature of OSPF.
OSPF uses four different types of routes, in order of priority: intra-area routes, inter-area routes, Type I external routes, and Type II external routes.
Intra-area and inter-area routing describe the network structure within an autonomous system, while external routing describes how routes to destinations outside the autonomous system should be selected.
The first type of external route refers to the received IGP routes (e.g., RIP, STATIC), because this type of route has a higher degree of confidence, the cost of the calculated external route is of the same order of magnitude as the cost of the internal routes of the autonomous system, and is comparable to the cost of the OSPF own routes, i.e., the cost of the first type of external route = the cost of the corresponding ASBR from this router + the cost of the ASBR to the destination address of the route. value + the cost of the ASBR to the destination address of the route.
The second type of external route is one that receives an EGP route, and because these routes are less reliable, the OSPF protocol considers the cost of traveling from the ASBR to outside the autonomous system to be much greater than the cost of reaching the ASBR within the autonomous system. Therefore, the former will be the main consideration when calculating the route cost, i.e., the cost of the route to the second external route = the cost of the ASBR to the destination address of the route. If this value is equal, then the cost of this router to the corresponding ASBR will be considered. Please perform the following configuration under OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configure OSPF to introduce other protocol routes	redistribute { babel | bgp | connected | isis | kernel | rip | static } [metric *metric-value*] [metric-type { 1 | 2 }] [route-map *map-name*]	
Remove OSPF introduction of other protocol routes	undo redistribute { babel | bgp | connected | isis | kernel | rip | static } [metric *metric*] [metric-type { 1 | 2 }] [route-map *map-name*]	

[Parameter Description]
out: Filter outgoing routing updates;
kernel: core route;
connected: directly connected route;
static: static route;
rip: RIP route;
isis: ISIS routing;

bgp: BGP routing;

babel: Babel route;

metric-value: introduce route spend, configuration range 0-16777214, default is 1;

metric-type: type of external route introduced, type1 or type2, default is type2;

map-name: Name of the route-map to be applied;

[Example]

! Setting up OSPF to introduce RIP routes

[GPON-router-ospf] redistribute rip

41.2.21 Configure OSPF to introduce default routes

Default routes cannot be introduced using the redistribute command; to introduce default routes into the routing table they must be configured using the following commands. Please perform the following configuration under OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configure OSPF to introduce default routes	default-information originate [always] [metric *metric-value*] [metric-type { 1 | 2 }] [route-map *map-name*]	
Remove the OSPF introduction default route	undo default-information originate [always] [metric *metric-value*] [metric-type { 1 | 2 }] [route-map *map-name*]	

[Parameter Description]

always: indicates that the default route is always advertised regardless of whether the default route exists in the device;

metric-value: introduce route spend, configuration range 0-16777214, default is 1;

metric-type: type of external route introduced, type1 or type2, default is type2;

map-name: Name of the route-map to be applied;

[Example]

! Setting up OSPF to introduce default routes

[GPON-router-ospf] default-information originate always

41.2.22 Configuring OSPF to Introduce External Routes Default Spend

When OSPF introduces routing information discovered by other routing protocols into this autonomous system, some additional parameters need to be configured, such as the default spend and default marking of the introduced routes. Route marking can be used to identify protocol-related information, such as the number used to distinguish autonomous systems when OSPF receives BGP. Please perform the following configuration under OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configuring OSPF to Introduce External Route Default Spending	default-metric *metric-value*	
Restore the default OSPF introduction of external routes default spending	undo default-metric	

[Parameter Description]

metric-value: introduce route spend, configuration range 0-16777214, default is 1;

[Example]

! Set the default spend for OSPF introduction of external routes to 10

[GPON-router-ospf] default-metric10

41.2.23 Configuring OSPF Route Filtering

Under a specific Layer 3 interface, policy rules can be configured for both incoming and outgoing routes by specifying a list of address prefixes for OSPF, thus filtering the routes learned and announced by OSPF. Additionally, for incoming routes, you can also learn OSPF routes for a specific device by specifying that the neighboring device learns OSPF routes for the specific device only.

This function is not enabled by default. Note that because OSPF learns routing information by exchanging LSAs in each other's databases between neighbors, when configuring OSPF learned route filtering, regardless of whether the routing information carried by an LSA can pass the filter or not, this LSA will be saved in the corresponding area database. However, the routing information carried by an LSA that does not pass the filter does not generate routes in the routing table and does not flood to other areas, but it still floods in this area. Please perform the following configuration under OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configuring OSPF Route Filtering	distribute-list { *ip-acl-name* | *ip-acl-number* } out { babel | bgp | connected | isis | kernel | rip | static }	
Remove OSPF route filtering	undo distribute-list { *ip-acl-name* | *ip-acl-number* } out { babel | bgp | connected | isis | kernel | rip | static }	

[Parameter Description]

ip-acl-name|ip-acl-number: references the IP-ACL of the matching routing table entry, related configuration is described in section 392.3;

out: Filter outgoing routing updates;

kernel: core route;

connected: directly connected route;

static: static route;

rip: RIP route;

isis: ISIS routing;

bgp: BGP routing;

babel: Babel route;

[Example]

! Configure filtering of routes on the 192.168.1.0/24 network segment

[GPON-router-ospf]ip acl 1 deny 192.168.1.0 0.0.0.255

[GPON-router-ospf]distribute-list 1 out rip

41.2.24 Configuring OSPF Routing Administrative Distance

The device supports configuring the route administrative distance of the OSPF protocol. Route administrative distance is used to select routes when there are two routes of different routing protocols to reach the same destination address. the smaller the administrative distance of a routing protocol is, the more reliable the route obtained by the protocol is. the

default route administrative distance of OSPF is 110, and the default route administrative distance of RIP is 120, so that the routes learned by OSPF have a higher priority. Perform the following configuration in OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configuring OSPF Routing Administrative Distance	distance [{ ospf | distanceip-address / mask-length [ip-acl-name | ip-acl-number] }]	Default distance value is 110, configuration range is 1-255
Restore the default OSPF routing administrative distance	undo distance [{ ospf | distanceip-address / mask-length [ip-acl-name | ip-acl-number] }]	

[Parameter Description]

distance: routing administrative distance, configured in the range of 1-255;

ip-address/mask-length: prefix address (dotted decimal) and mask length, such as 192.168.1.0/24;

ip-acl-name|ip-acl-number: references the IP-ACL of the matching routing table entry, related configuration is described in section 39.2.3;

Only routes that meet the ip-address/mask-length or ip-acl-name|ip-acl-number conditions set the corresponding distance.

[Example]

! Configure the OSPF routing administrative distance to 150

```
[GPON-router-rip] distance 150
```

41.2.25 Configuring OSPF Neighbor Routers for Interconnected NBMA Networks

The device supports configuring OSPF neighbor routers that configure interconnected NBMA networks. Please perform the following configurations under OSPF view.

manipulate	command	clarification
Go to System View	system-view	
Enter OSPF view	router ospf	
Configuring OSPF Routers for Interconnected NBMA Networks	neighbor *ipadress* [priority *priority* | poll-interval *interval*]	
Remove OSPF routers from the interconnected NBMA network	undo neighbor *ipadress*	

[Parameter Description]

ipadress: the NBMA interconnect router IP address;

priority: neighbor priority, default value is 0, range 0-255;

interval: default value is 120s, the polling time between router links that have not formed a neighbor relationship, in the range of 1-65535; configure neighbors manually on the NBMA network Using this command, you should configure a neighbor entry for each known non-broadcast network neighbor router. The configured neighbor address should be the primary address of the interface. poll-interval should have a higher value than the hello-interval is much larger.

[Example]

! Configure the OSPF neighbor router for the interconnected NBMA network to be 192.168.1.200, with a neighbor priority of 10

```
[GPON-router-ospf]neighbor 192.168.1.200 priority 10
```

41.2.26 OSPF Monitoring and Maintenance

You can display OSPF-related configuration and operational information in any view.

manipulate	command	clarification
Display OSPF information	display ip ospf	
Displaying Router ID Information	display router id	
Displaying Router ID Information	display ip ospf neighbor	
Display the OSPF LSDB database	display ip ospf database	
Display OSPF virtual connection information	display ip ospf virtual-link	
Display OSPF Border Route Information	display ip ospf border-routers	
Display OSPF interface information	display ip ospf interface	
Display OSPF routing table information	display ip route ospf	

[Example]

! Display OSPF information

[GPON] display ip ospf

! Display OSPF neighbor information

[GPON] display ip ospf neignbor

! Display OSPF routing table information

[GPON] display ip route ospf

Chapter 42 BGP Configuration

42.1 BGP Introduction

42.1.1 Introduction to the BGP Protocol

BGP (Border Gateway Protocol) is a dynamic routing protocol between autonomous systems, and its basic function is to automatically exchange loop-free routing information between autonomous systems, and to construct the topology of autonomous systems by exchanging network layer reachable information with path attributes of autonomous systems (AS). BGP has been in use since 1989, and its three earliest releases were RFC1105 (BGP-1), RFC1163 (BGP-2), and RFC1267 (BGP-3), with the most popular currently in use being RFC1771 (BGP-4). This device currently supports BGP-4.

BGP-4 is suitable for distributed architectures and supports Classless InterDomain Routing CIDR (Classless InterDomain Routing). User-configured policies can also be enforced using BGP.BGP-4 is rapidly becoming the de facto standard for Internet external routing protocols. the BGP-4 features are as follows:

1) BGP is an external routing protocol, unlike internal routing protocols such as OSPF and RIP, BGP does not discover and compute routes, but it can control the propagation of routes and select the best routes;

2) The problem of routing loops can be completely solved by carrying AS path information in the update routes;

3) Using TCP as its transport layer protocol improves the reliability of the protocol, using UDP port number 179;

4) BGP-4 supports Classless Inter-Domain Routing CIDR, an important improvement over BGP-3, which takes a new approach to IP addresses, no longer distinguishing between Class A, Class B, and Class C. For example, an illegal Class C network address 192.168.0.0 (255.255.0.0) becomes a legal address using the CIDR representation 192.168.0.0/16. For example, an illegal Class C network address 192.168.0.0 (255.255.0.0) becomes a legal super network by using the CIDR representation 192.168.0.0/16, in which /16 means that the subnet mask consists of 16 bits starting from the left end of the address.The introduction of CIDR simplifies the route aggregation (Route). The introduction of CIDR simplifies route aggregation (Route Aggregation), which is actually the process of merging several different routes, thus reducing the overhead of the BGP table and network bandwidth consumption by changing from the advertisement of several routes to the advertisement of a single route;

4) When routing updates are made, BGP sends only incremental routes, which greatly reduces the bandwidth occupied by BGP propagating routes and is suitable for propagating large amounts of routing information over the Internet;

5) For management and security considerations, each autonomous system wants to be able to control the routes in and out of the autonomous system, BGP-4 provides a wealth of routing policies, can realize flexible filtering and selection of routes, and is easy to expand to support the new development of the network;

42.1.2 Overview of BGP operation

Unlike the RIP and OSPF protocols, the BGP protocol is connection-oriented.To exchange routing information between BGP devices, a connection must be established before routing information can be exchanged.The operation of the BGP protocol is message-driven, and its messages can be categorized into a total of four types:

1. Open Message - is the first message sent after a TCP connection is established. It is used to establish a BGP connection between BGP peers. some of the parameters in the Open message are used to negotiate whether a connection between BGP neighbors can be established.

2. Keepalive Message - a message used to check the validity of the connection. Generally, it is sent periodically to maintain the BGP connection. If this message or Update message is not received within the holdtime, the BGP connection is closed.

3. Update Message - is the most important message in the BGP system and is used to exchange routing information between peers. In addition to devices exchanging updated routing information, it also exchanges information about routes that are unavailable or have been canceled. It consists of three parts: unreachable routes, NLRI Network Layer Reachability Information, and Path Attributes.

4. Notification Message - is an error notification message. When a BGP speaker receives such a message, it closes the BGP connection with its neighbor.

BGP runs as a high-level protocol on a specific router. A BGP router exchanges routing information with a peer by sending the entire BGP table when the protocol starts, and then only processes changed routes by exchanging update messages. The protocol operates by receiving and sending keepalive messages to detect whether the connection to each other is normal;

The router that sends the BGP message is called the BGP speaker, which continuously receives or generates new route information and advertises it to other BGP speakers. When a BGP speaker receives a new route advertisement from another autonomous system, it advertises the route to all other BGP speakers in the autonomous system if the route is better than currently known routes or if there are no currently accepted routes. the BGP speaker also refers to other BGP speakers with whom it exchanges messages as peers;

BGP operates on routers in two ways:

->IBGP (Internal BGP);

->EBGP (External BGP);

When BGP operates within the same autonomous system (AS), it is referred to as IBGP, and when BGP operates between different autonomous systems, it is referred to as EBGP.

42.1.3 Routing Policies for BGP

Route Selection Policies for BGP When a BGP advertisement is received from multiple neighbors about the same route, the optimal route needs to be considered for selection after route filtering. This process is called the BGP routing process.The BGP routing process starts only when the following conditions are met:

1. The routing of the device must be next-hop reachable. That is, there are routes in the routing table that can reach the next-hop address;

2. BGP must be synchronized with IGP (unless set to asynchronous, which is limited to IBGP);

The BGP routing process is based on BGP attribute values. When there are multiple routes that specify the same destination, BGP then selects the best route to reach the destination. The decision process is as follows:

1. Prioritize routes with maximum weight;

2. If the weights are equal, the route with the highest local preference is preferred;

3. If the local priorities are the same, the route originating from the local device is preferred.

4. if the local priorities are the same and there are no routes originating from the local device, the route with the shortest AS path is preferred;

5. If the AS paths are the same, the route with the lowest origin type (IGP<EGP<INCOMPLETE) is preferred;

6. if the origin types are the same. the route with the lowest MED attribute is preferred. unless the bgp always-compare-med command is activated. such comparisons are made only between routes from the same neighboring AS;

7. If the MED attributes are the same, EBGP is preferred to external to the federation and external to the federation is preferred to IBGP;

8. If all the previous conditions are the same, the NEXT_HOP attribute of these routes is judged and the route with the lowest route cost corresponding to the route to reach its next hop address in the IGP routing table is preferred;

9. If there is still a tie at this point, the BGP device ID (router ID) is used to break the balance. The best route comes from the device with the smallest BGP Router-ID;

42.2 Configuration of BGP

42.2.1 BGP Configuration Task List

In each configuration task, you must start BGP and enter the BGP view before you can configure other functional features. The list of BGP configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable BGP function	compulsory	42.2.2
Configure network routes for local BGP announcements	compulsory	42.2.3
Create/delete BGP peer groups	compulsory	42.2.4
Configuring BGP Peer Autonomous System Numbers	selectable	42.2.5
Add/remove BGP peer group members	selectable	42.2.6
Configure to allow connections to EBGP peers on networks that are not directly connected to each other	selectable	42.2.7
Configuring BGP Peer Timers	selectable	42.2.8
Configure the interval at which BGP peers send routing update messages	selectable	42.2.9
Configure a BGP peer to use its own address as the next hop when it advertises a route	selectable	42.2.10
Configuring BGP Peer Route Filtering Policies Based on IP Prefix Control Lists	selectable	42.2.11
Configuring BGP Peer Route Filtering Policies Based on IP Access Control Lists	selectable	42.2.12
Configuring BGP Peer Route Filtering Policies Based on AS Path Lists	selectable	42.2.13
Configuring Route-map-based Route Mapping Policies for BGP Peers	selectable	42.2.14
Configure whether BGP peers do not send unsolicited connection requests	selectable	42.2.15
Shutting down BGP peer connections	selectable	42.2.16
Configuring BGP Global Timers	selectable	42.2.17
Configuring BGP Local Priority	selectable	42.2.18
Configure whether BGP compares the MED values of different ASes	selectable	42.2.19
Configuring BGP Route Aggregation	selectable	42.2.20
Configure BGP to introduce IGP protocol routes	selectable	42.2.21
Configure the BGP Router ID	selectable	42.2.22
BGP Monitoring and Maintenance	selectable	42.2.23

42.2.2 Enable/disable the BGP feature

The local autonomous system number should be specified when starting BGP. After starting BGP, the local router listens for and receives BGP connection requests from neighboring routers. To enable the local router to initiate BGP connection requests to neighboring routers, refer to the configuration of the neighbor command. When shutting down BGP, BGP disconnects all established BGP connections. Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Initiate BGP protocol	router bgp *as-number*	The as-number configuration range is 1-65535
Disabling the GBP protocol	undo router bgp *as-number*	

[Parameter Description]

as-number: local autonomous system number, the configuration range is 1-65535;

[Example]

! Start the BGP protocol

```
[GPON]router bgp 400
```

42.2.3 Configure network routes for local BGP announcements

Use the network command to specify the network route that BGP wants to advertise to peers, and also to specify the mask for this network route.

Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configure routes for local announcements	network ip-address [mask address-mask]	
Deleting locally advertised routes	undo network ip-address [mask address-mask]	

[Parameter Description]

ip-address: IP address or network segment to be advertised;

The network command injects a route with ip-address as the destination into the BGP table and then advertises the route to the BGP peer. Only routes that already existed in the IP routing table before the network command was configured are injected into the local BGP table and advertised to peers via Update messages.

Routes that are posted using the network command are exact match routes, that is, the prefix and mask must match the configuration exactly to be posted correctly. If no mask is specified, the exact match is done according to the natural network segment.

By default, local BGP does not advertise any network routes.

[Example]

! Notification network 192.168.1.0

```
[GPON-router-bgp]network 192.168.1.0
```

42.2.4 Create/delete BGP peer groups

Two BGP speakers exchanging BGP messages form a peer.

By configuring a peer group, a group of peers with the same attributes can be configured at the same time to reduce the workload of the configurator. perform the following configurations in BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configuring BGP Peer Groups	neighbor *neighbor-name* peer-group	
Deleting a BGP Peer Group	undo neighbor *neighbor-name* peer-group	

[Parameter Description]

neighbor-name: Peer name, up to 32 configurable characters;

[Example]

! Configure neighboring BGP peers abcd

```
[GPON-router-bgp]neighbor abcd peer-group
```

42.2.5 Configuring BGP Peers Autonomous System Number

Two BGP speakers exchanging BGP messages form a peer.

When configuring BGP peers as neighbors, you first need to specify the autonomous system number to which the other party belongs. Routing information can be exchanged only after both parties have specified the autonomous system number to which the other party and themselves belong. Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configure to establish a neighbor relationship and develop a peer AS number	neighbor { neighbor-address | neighbor-name } remote-as as-number	
Deleting established neighbor relationships	undo neighbor { neighbor-address | neighbor-name } remote-as	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

If the command neighbor remote-as matches the autonomous system number specified by the command router bgp, the configured neighbor is internal and is referred to as IBGP; otherwise, it is external and is referred to as EBGP.

BGP neighbors are generated entirely through command configuration, and both sides have to configure each other in order to truly establish a neighbor relationship. When configuring, you have to specify the AS number of the opposite end; if the AS number is not correct, you cannot establish a neighbor relationship either. If it is inside the AS, the AS number of the opposite end is the same as that of the local end.

[Example]

! Configure BGP peer 192.168.1.100 with AS number 100

```
[GPON-router-bgp] neighbor 192.168.1.100 remote-as 100
```

42.2.6 Add/remove BGP peer group members

This function mainly adds/removes peer members to/from a peer group. perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Adding a BGP Peer Group Member	neighbor neighbor-address peer-group neighbor-name	
Deleting a BGP Peer Group Member	undo neighbor neighbor-address peer-group neighbor-name	

[Parameter Description]

neighbor-address: peer IP address, i.e., peer member;

neighbor-name: Peer name;

[Example]

! Add BGP peer abcd group member 192.168.1.100

```
[GPON-router-bgp]neighbor 192.168.1.100 peer-group abcd
```

 Description:

You can only add a peer member to a peer if you first specify the autonomous system number of the peer.

42.2.7 Configure to allow connections to EBGP peers on networks that are not directly connected to each other

Normally, EBGP peers must be physically directly connected to each other. By default, the device only allows connections to peers on the directly connected network. Please make the following configurations under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configure to allow connections to EBGP peers on networks that are not directly connected to each other	neighbor { *neighbor-address* | neighbor-name} ebgp-multihop [*ttl*]	
Configure to allow connections only to EBGP peers on the directly connected network.	undo neighbor { neighbor-address | neighbor-name } ebgp-multihop	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

ttl: number of connection hops, the configuration range is 1-255, the default is 255;

Without configuring this command, it is required that the EBGP peers must be in the same network segment. After configuring this command, the peer addresses can be out of the same network segment, and the allowable TTL (number of hops) can be set. if this parameter is omitted, it is 255.

[Example]

! Three devices, 192.168.1.100 (AS100) and 192.168.2.200 (AS200), are connected to the interfaces 192.168.1.123 and 192.168.2.123 of another device (with no BGP activated), respectively, and routes on both sides of the static configuration ensure that 192.168.1.100 and 192.168 .2.200 IGP reachable by statically configuring routes on both sides. Establish the neighbor relationship between 192.168.1.100 and 192.168.2.200. If configured directly, both remain in ACTIVE state respectively. Neighbor relationship can be established only after the following commands are configured on both sides respectively:

Configured on 192.168.1.100.

```
[GPON-router-bgp]neighbor 192.168.2.200 ebgp-multihop
```

Configured on 192.168.2.200.

```
[GPON-router-bgp]neighbor 192.168.1.100 ebgp-multihop
```

After configuration, devices that are not on the same network segment can establish BGP neighbor relationships.

42.2.8 Configuring the BGP Peer Timer

Use the neighbor timers command to configure timers for a specified BGP peer, including specifying the Keepalive message sending interval and the hold timer. The so-called hold time is the time interval during which no message is received from the peer and the connection is still considered to be sustained, and beyond which the connection is interrupted. Please make the following configurations under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	

Configure the timer for the specified peer	neighbor { neighbor-address | neighbor-name } timers keepalive-interval hold-time	
Restore the default specified peer timer	undo neighbor { neighbor-address | neighbor-name } timers	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

keepalive-interval: Keepalive message sending interval, the configuration range is 0-21845 seconds, the default is 30 seconds;

hold-time: hold timer, the configuration range is 0-65535 seconds, the default is 180 seconds;

[Example]

! Configure peer 192.168.1.100 Keepalive messages to be sent at an interval of 50 seconds with a hold timer of 200 seconds

```
[GPON-router-bgp]neighbor 1.1.1.1 timers 50 200
```

42.2.9 Configure the interval at which BGP peers send routing update messages

This function command is used to configure the time interval for sending routing update messages to a specified peer.

Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configure the interval at which peers send routing update messages	neighbor { neighbor-address | neighbor-name } advertisement-interval seconds	
Restore the default interval for peers to send routing update messages by default	undo neighbor { *neighbor-address* | *neighbor-name* } advertisement-interval	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

seconds: hold timer, the configuration range is 1-600 seconds. By default, the time interval for IBGP peers to send routing update messages is 15 seconds, and the time interval for EBGP peers to send routing update messages is 30 seconds;

[Example]

! Configure peer 192.168.1.100 to send routing update messages at an interval of 50 seconds

```
[GPON-router-bgp]neighbor 192.168.1.100 advertisement-interval 50
```

42.2.10 Configure a BGP peer to use its own address as the next hop when it advertises a route

This function command is used to require BGP peers to point to this end for the next hop of routes sent from this end. In an EBGP environment, the next hop automatically points to the source neighbor, but in an IBGP environment, the original next hop remains unchanged if the route is on the same network segment. However, if it is not a broadcast network, there is a problem, so you can use this command to force the use of itself as the neighbor's next hop as long as it is under IBGP.

Please do the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configure to publish routes with its own address as the next hop	neighbor { neighbor-address | neighbor-name } next-hop-self	
Unpublishing a route with its own address as the next hop	undo neighbor { neighbor-address | neighbor-name } next-hop-self	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

By default, this command is not configured and the default method of processing the next hop is used.

[Example]

! Configure peer 192.168.1.100 to use its own address as the next hop when publishing routes

[GPON-router-bgp]neighbor 192.168.1.100 next-hop-self

42.2.11 Configuring BGP Peer Route Filtering Policies Based on IP Prefix Control Lists

This feature command is used to configure the policy applied by peers to send and receive routing updates, based on IP prefix control lists for route filtering. Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configuring Peer Route Filtering Policies Based on IP Prefix Control Lists	neighbor { neighbor-address | neighbor-name } prefix-list list-name { in | out }	
Remove peer-based IP prefix control list route filtering policy	undo neighbor { neighbor-address | neighbor-name } prefix-list list-name { in | out }	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

list-name: References the IP-Prefix list of matching routing table entries;

in: indicates filtering for update routes coming from the opposite end;

out: Indicates filtering of routes from this end to the opposite end;

By default, peers do not perform route filtering based on IP prefix control lists.

[Example]

! Set the filtering of routes destined for 192.168.2.0 in routes sent to peer 192.168.1.100

[GPON-router-bgp]ip prefix-list abcd deny 192.168.2.0/24

[GPON-router-bgp]neighbor 192.168.1.100 prefix-list abcd in

42.2.12 Configuring BGP Peer Route Filtering Policies Based on IP Access Control Lists

This function command is used to configure the policy applied by peers to send and receive routing updates. route filtering is performed based on IP access control lists. the BGP route matching is accomplished through network segments and masks. For successful matches, deny or permit decides whether to accept the route. After you define a BGP route access

control list and then apply it with the neighbor distribute-list command to realize the BGP policy routing function. Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configuring Peer Route Filtering Policies Based on IP Access Control Lists	neighbor { *neighbor-address* | *neighbor-name* } distribute-list { ip-acl-name | ip-acl-number } { in | out }	
Remove peer-based IP access control list route filtering policy	undo neighbor { *neighbor-address* | *neighbor-name* } distribute-list { ip-acl-name | ip-acl-number } { in | out }	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

ip-acl-name |ip-acl-number: references the IP-ACL of the matching routing table entry;

in: indicates filtering for update routes coming from the opposite end;

out: Indicates filtering of routes from this end to the opposite end;

By default, peers do not perform route filtering based on IP access control lists.

[Example]

! Set the filtering of routes destined for 192.168.2.0 in routes sent to peer 192.168.1.100

```
[GPON-router-bgp]ip acl 1 deny 192.168.2.0 0.0.0.255
[GPON-router-bgp]neighbor 192.168.1.100 distribute-list 1 out
```

42.2.13 Configuring BGP Peer Route Filtering Policies Based on AS Path Lists

This function command is used to configure the policy applied by a peer to send and receive routing updates, and route filtering based on the AS path list.

Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configuring Peer Route Filtering Policies Based on AS Path Lists	neighbor { neighbor-address | neighbor-name } filter-list aspath-list-number { in | out }	
Remove the peer's route filtering policy based on AS path lists	undo neighbor { neighbor-address | neighbor-name } filter-list aspath-list-number { in | out }	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

aspath-list-number: references the access list of the IP AS-PATH that matches the routing table entry;

in: indicates filtering for update routes coming from the opposite end;

out: Indicates filtering of routes from this end to the opposite end;

By default, peers do not perform route filtering based on AS path lists.

[Example]

! Configure the AS-PATH access control list so that routes with an AS number of 200 cannot be updated to the peer

```
[GPON-router-bgp]ip as-path acl 1 deny 200
```

[GPON-router-bgp]neighbor 192.168.1.100 filter-list 100 out

42.2.14 Configuring Route-map-based Route Mapping Policies for BGP Peers

This function command is used to configure the policy applied by a peer to send and receive routing updates, based on Route-map for route mapping policy. Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configure a peer's Route-map-based route-mapping policy	neighbor { neighbor-address | neighbor-name } route-map map-name { in | out }	
Deleting a peer's Route-map-based route-mapping policy	undo neighbor { neighbor-address | neighbor-name } route-map map-name { in | out }	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

map-name: References the Route-map route mapping policy control of the matching routing table entry;

in: indicates mapping for updated routes coming from the opposite end;

out: Indicates mapping for routes sent from this end to the opposite end;

By default, peers do not perform route mapping based on Route-map.

[Example]

! Configure Route-map route mapping to filter routes for route Metric 10

[GPON-router-rip]route-map abcd deny 12345

[GPON-router-routemap]match metric 10

[GPON-router-bgp]neighbor 192.168.1.100 route-map abcd in

42.2.15 Configure whether BGP peers do not actively send connection requests

This function is used to configure whether this party does not send connection requests actively during the connection with the specified peer, and the default configuration is to send connection requests actively. Please make the following configurations under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configure not to send unsolicited connection requests	neighbor { neighbor-address | neighbor-name } passive	
Restore the default proactive connection request	undo neighbor { neighbor-address | neighbor-name } passive	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

When this attribute is configured and the connection is re-established, the local end does not attempt to establish a connection but is immediately in the ACTIVE state, waiting for a response to the peer's TCP connection request.

[Example]

! Configure not to initiate a connection request when establishing a connection with peer 192.168.1.100

[GPON-router-bgp]neighbor 192.168.1.100 passive

42.2.16 Shutting down BGP peer connections

This function is used to close the connection of BGP peers, and the default configuration is not to close the connection. Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Shutting down BGP peer connections	neighbor { neighbor-address | neighbor-name } shutdown	
Restore default open BGP peer connections	undo neighbor { neighbor-address | neighbor-name } shutdown	

[Parameter Description]

neighbor-address: peer IP address;

neighbor-name: Peer name;

[Example]

! Regarding the connection to peer 192.168.1.100

[GPON-router-bgp]neighbor 192.168.1.100 shutdown

42.2.17 Configuring BGP Global Timer

When a BGP connection is established between peers, they send Keepalive messages to the peer at regular intervals to prevent the router from thinking that the BGP connection has been broken. If the router does not receive a Keepalive message or any other type of message from the peer within a set connection holdtime, the local router assumes that this BGP connection has been disconnected, and thus exits this BGP connection and processes the routes received from this BGP connection accordingly. Therefore, the interval between sending Keepalive messages and the BGP connection hold time are two very important parameters in the BGP mechanism.

When a BGP router and its peer establish a BGP connection, they need to negotiate a keepalive time that is the smaller of the BGP router's keepalive time or the peer's keepalive time. If the result of the keepalive negotiation is 0, no Keepalive message is sent and the Holdtime timeout is no longer detected. Set to support peer-based configuration of timers as well as global configuration of timers. this feature refers to the configuration of global-based timers. the peer timer takes precedence when both the peer and the global are configured with a timer. Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configuring BGP Global Timers	timersbgp keepalive-interval hold-time	
Restore the default BGP global timer	undo timers bgp	

[Parameter Description]

keepalive-interval: Keepalive message sending interval, the configuration range is 0-21845 seconds, the default is 30 seconds;

hold-time: hold timer, the configuration range is 0-65535 seconds, the default is 180 seconds;

The sending interval cannot be less than 1 second. If Holdtime is configured not to be 0, it is at least 3 seconds. If the keepalive interval is greater than 1/3 of the negotiated holdtime, the keepalive interval is automatically set to 1/3 of the negotiated holdtime.

[Example]

! Configure the global Keepalive message sending interval to 60 seconds and the hold timer to 360 seconds

[GPON-router-bgp] timers bgp60 360

42.2.18 Configuring BGP Local Priority

BGP routing can be influenced by configuring different local priorities. When a router running BGP gets routes with the same destination and different next hops through different Internal Peers, the route with the highest local priority is selected. The local priority is sent only when Update messages are exchanged between IBGP peers and is not sent outside of this autonomous system.

Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configuring BGP Local Priority	bgp default local-preference vlaue	
Restore the default BGP local priority	undo bgp default local-preference	

[Parameter Description]

vlaue: local priority, the configuration range is 0-4294967295, the default priority is 10;

Higher priority values represent higher priority

[Example]

! Configure the BGP local priority to 100

[GPON-router-bgp]bgp default local-preference 100

42.2.19 Configure whether BGP compares MED values of different ASes

When an autonomous system running BGP gets multiple routes from different autonomous systems with the same destination and different next hops, it can run the Compare MED value function, and the route with the smaller MED is preferred as the external route of the autonomous system, all other conditions being equal. Normally, BGP compares the MED only when the ASes are the same. with this setting, you can compare the MED of routes originating from different ASes. do the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configuring the BGP Compare MED	bgp always-compare-med	
Cancel BGP Compare MED	undo bgp always-compare-med	

[Parameter Description]

By default, comparison of MED attribute values from different AS neighbor paths is not allowed.

Do not use this configuration unless you can confirm that different autonomous systems use the same IGP and routing method.

The system local default MED value is 0.

[Example]

! Enable BGP Compare MED function

[GPON-router-bgp]bgp always-compare-med

42.2.20 Configuring BGP Route Aggregation

BGP CIDR supports route aggregation. The aggregate command aggregate-address is an aggregation of BGP local routes. Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configuring BGP Route Aggregation	aggregate-address { *ip-address mask* | *ip-address / mask-length* } [summary-only] [as-set]	
Cancel BGP route aggregation	undo aggregate-address { ip-address mask | ip-address / mask-length }	

[Parameter Description]

ip-address mask: IP address and mask for aggregation;

ip-address/mask-length: prefix address (dotted decimal) and mask length, such as 192.168.1.0/24;

summary-only: means that only aggregation is sent and specific routes are ignored;

as-set: represents the ASes on the path as a list, each AS appears only once;

The device does not configure route aggregation by default.

[Example]

! Configuring BGP Route Aggregation, 192.168.0.0 network segment, mask 16 bits

[GPON-router-bgp]aggregate-address 192.168.0.0 255.255.0.0

42.2.21 Configure BGP to introduce IGP protocol routes

BGP can send information about the internal network of this autonomous system to other autonomous systems. For this purpose, information about the internal network of the system obtained by the local router through the IGP routing protocol can be sent out through BGP.

Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configure BGP to introduce routes for IGP protocols	redistribute { babel | connected | isis | kernel | ospf | rip | static } [metric *metric* [route-map *route-map*]]	
Canceling BGP routes that introduce IGP protocols	undo redistribute { babel | connected | isis | kernel | ospf | rip | static }	

[Parameter Description]

babel: introduced from the Babel route;

conneted: introduced from a directly connected route;

isis: introduced from the ISIS route;

kernel: introduced from the core route;

ospf: introduced from OSPF routing;

rip: introduced from RIP routing;

static: introduced from static routes;

metric: The route weight assigned to the introduced route, ranging from 0-4294967295;

route-map: pointer to the route map used to introduce routes, configurable up to 32 characters;

By default, BGP will not introduce routes from other protocols.

[Example]

! Enable BGP to introduce IGP OSPF protocol routes

```
[GPON-router-bgp]redistribute ospf
```

42.2.22 Configure the BGP Router ID

BGP can configure the local router ID, or Router ID, to identify the BGP router.

Please perform the following configuration under BGP view.

manipulate	command	clarification
Go to System View	system-view	
Enter BGP view	router bgp *as-number*	
Configuring the Router ID	bgp router-id *ipaddress*	
Delete Router ID	undo bgp router-id	

[Example]

! Configure the BGP Router ID to 192.168.1.100

```
[GPON-router-bgp]bgp router-id 192.168.1.100
```

42.2.23 Monitoring and Maintenance of BGP

You can display BGP-related configuration information in any view:

manipulate	command	clarification
Display BGP peer details	display ip bgp neighbors *neighbor-address* [vpn-instance *instance*]	vpn-instance is a vpn-related feature that is not yet implemented, and is reserved on the command line for merging into the feature in subsequent releases.
Display BGP peer summary information	display ip bgp summary [vpn-instance *instance*]	

[Example]

! Display information about BGP peer 192.168.1.200

```
[GPON]display ip bgp neighbors 192.168.1.200
```

Chapter 43 BFD Functional Configuration

43.1 Introduction to BFD

43.1.1 Introduction to the BFD Protocol

BFD (Bidirectional Forwarding Detection) is a set of network-wide unified detection mechanisms for quickly detecting and monitoring the connectivity status of links in a network. In order to improve the performance of an existing network, protocol neighbors must be able to quickly detect communication failures, so that alternate channels can be established more quickly to resume communication.

BFD provides a generic, standardized, media-independent and protocol-independent fast fault detection mechanism for each upper-layer protocol such as routing protocols, MPLS, etc. to uniformly and quickly detect faults in the bidirectional forwarding path between two network devices.

BFD establishes a session on two network devices, which is used to monitor the bidirectional forwarding path between the two network devices and serve the upper layer protocols.BFD itself does not have a discovery mechanism, but rather relies on the served upper layer protocols to notify it of who to establish a session with, and after the session is established, if no BFD control message is received from the opposite end within the detection time, then it is considered to be a failure, and notifies the served upper layer protocols, which carry out the the served upper layer protocol, and the upper layer protocol handles the situation accordingly.

BFD periodically detects the state of the other side of the session to find session abnormalities, and when session abnormalities are found, the corresponding routing protocol is immediately notified, and the routing protocol carries out the corresponding operation for fast rerouting. As the detection period of BFD is generally less than 1s, which shortens the convergence time of routing protocols, BFD can assist OSPF, RIP, BGP, and other routing protocols in discovering the reachability of the neighbors or in detecting link failures, so that fast rerouting can be performed and link reliability can be ensured. Therefore, BFD can assist routing protocols such as OSPF, RIP, and BGP in discovering neighbor accessibility or detecting link failures, which can quickly reroute and ensure link reliability.

43.1.2 BFD Protocol Flow

1. BFD message format

The detection messages sent by the BFD are UDP messages defining two types of messages: control messages and echo messages.

1) BFD control message

The BFD control message is encapsulated in UDP and has a destination port number of 3784 and a source port number in the range of 49152 to 65535. the meaning of each field of the BFD control message is shown in the following table:

field	hidden meaning
Vers	BFD protocol version number, currently version 1
Diag	Diagnostic code indicating the reason for the sender's most recent session Down
Sta	The current state of the sender's BFD session, take the value: 0 for AdminDown, 1 for Down, 2 for Init, 3 for Up
P	Set when session parameters change
F	If the P field of the received BFD control message is set, set the F field of the next transmitted BFD control message as an answer
C	This field is set to indicate that the BFD implementation is independent of the control plane
A	This field is set to indicate that the message contains an authentication section and the session requires authentication

D	This field is set to indicate that the sender wishes to operate in query mode, and is not set to indicate that query mode is not desired or not supported
R	Reserved bit, set to 0 when sending, ignore this field when receiving
Detect Mult	Detection Time Multiplier
Length	BFD control message length in bytes
My Discriminator	A unique non-zero value generated by the sender to identify different BFD sessions
Your Discriminator	If a BFD control message has been received from a session neighbor, the value is My Discriminator in the received message, otherwise it is 0.
Desired Min TX Interval	The minimum BFD control message sending interval supported by the sender, in microseconds.
Required Min RX Interval	Minimum BFD control message reception interval supported by the sender, in microseconds
Required Min Echo RX Interval	The minimum BFD Echo message reception interval supported by the sender, in microseconds. A value of 0 indicates that BFD Echo messages are not supported.
Auth Type	Certification Type
Auth Len	Optional authentication section length, including Auth Type and Auth Len fields, in bytes

2) BFD Echo Message (Echo)

BFD protocol does not define the format of the echo message, but for the echo message, its format is only locally relevant, the remote end only need to return this message in the reverse channel, for the local system must be able to according to the corresponding content of the message to the appropriate separation of the session (so for the sending of echo packets, and its reception processing in the protocol are not defined). The protocol defines the UDP destination port number for echo packets as 3785.

The BFD Echo message is encapsulated in UDP, the destination port number is 3785, the destination IP address is the address of the sending interface, and the source IP address is generated by the configuration (the configured source IP address should avoid generating an ICMP redirection).

2. BFD session establishment

Before BFD detection, a peer-to-peer session needs to be established at both ends of the channel, and after the session is established, BFD control messages are sent to the opposite end at a negotiated rate to realize fault detection. The path for session detection can be a labeled switching path, other types of tunnels or Ethernet.

The session establishment process is a three times handshake process, after this process the two ends of the session becomes Up state, in this process at the same time negotiated the corresponding parameters, the subsequent state changes is based on the defect detection results and do the corresponding processing.

3. BFD detection mode

The BFD protocol describes the mechanism for realizing bidirectional detection, which can be divided into two kinds: asynchronous mode, query mode, and in addition there is an auxiliary function, echo function, which can be used in combination with these two modes. The essential difference between asynchronous mode and query mode is that the location of detection is different. In asynchronous mode, the local sends BFD control messages according to a certain period, and it is necessary to detect the BFD control messages sent by the local device at the remote device.

1) Asynchronous mode

In asynchronous mode, devices send BFD control messages to each other periodically, and if a device does not receive a BFD control message from the opposite end within the detection time, it declares the session as Down.

2) Query Mode

In query mode, it is assumed that each device has its own independent method for verifying its connectivity to other devices. Once a BFD session is established, the device stops sending BFD control messages unless a device needs to explicitly verify connectivity, in which case the device sends a short series of BFD control messages, declares the session to be

Down if no return message is received within the detection time, and is silent again if it receives a response message from the other end of the BFD protocol.

3) Echo function

The local sends a series of BFD echo messages and the remote device loops the echo messages back through its forwarding channel. If the local device does not receive several echo messages in a row, the session is declared Down. the echo function can be used in conjunction with the two detection modes described above. the echo function can be used instead of the task of detecting BFD control messages, which reduces the sending period of the control messages (in asynchronous mode) or eliminates the BFD control messages altogether (in query mode).

43.2 BFD Functional Configuration

43.2.1 BFD Function Configuration Task List

The list of major BFD configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable BFD function	compulsory	43.2.2
Enable/disable OSPF BFD function	compulsory	43.2.3
Configure the minimum sending interval of control messages expected by BFD	selectable	43.2.4
Configure the minimum receive interval for BFD control messages	selectable	43.2.5
Configure the detection multiplier for BFD control messages	selectable	43.2.6
Configuring BFD Session Mode	selectable	43.2.7
Configuring BFD Detection Mode	selectable	43.2.8
Clear BFD session packet statistics	selectable	43.2.9
BFD Monitoring and Maintenance	selectable	43.2.10

43.2.2 Enable/disable BFD function

The device supports globally enabling/disabling the BFD function, and the related BFD function configuration takes effect only after the BFD function is globally enabled, and the device disables the BFD function by default. Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Initiate BFD function	bfd enable	
Disable BFD function	bfd disable	

[Example]

! Enable BFD function

[GPON]bfd enable

43.2.3 Enable/disable OSPF BFD function

Please enable/disable the OSPF BFD function in Layer 3 interface mode.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Enable OSPF BFD function	ip ospf bfd	
Disable the OSPF BFD feature	undo ip ospf bfd	

[Parameter Description]

By default OSPF BFD function is off.

[Example]

! Enabling OSPF BFD on VLAN interface 100

[GPON-vlanInterface-100] ip ospf bfd

43.2.4 Configure the minimum sending interval of control messages expected by BFD

This function is used to configure the minimum interval that the sender wants to use when sending BFD control messages, and the actual sending interval needs to be negotiated with the other party, and the BFD control message sending interval is finally negotiated by confirming the minimum receiving interval of the other party's BFD control message. Perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the BFD control message sending interval	bfd min-transmit-interval *interval*	
Restore the default BFD control message sending interval	undo bfd min-transmit-interval	

[Parameter Description]

interval: minimum sending interval, the configuration range is 200-1000 milliseconds, the default value is 400 milliseconds;

[Example]

! Configure the minimum sending interval for BFD control messages for VLAN interface 100 to 500 milliseconds

[GPON-vlanInterface-100]bfd min-transmit-interval 500

43.2.5 Configure the minimum receive interval for BFD control messages

This function is used to configure the interval between receiving two BFD control messages that the sender can support. Please perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring the Minimum Receive Interval for BFD Control Messages	bfd min-receive-interval *interval*	

Restore the default minimum receive interval for BFD control messages	undo bfd min-receive-interval	

[Parameter Description]

interval: receive interval time, the configuration range is 200-1000 milliseconds, the default value is 400 milliseconds;

[Example]

! Configure the minimum receive interval for BFD control messages on VLAN interface 100 to 600 milliseconds

```
[GPON-vlanInterface-100] bfd min-receive-interval 600
```

43.2.6 Configure the detection multiplier for BFD control messages

This function is used to configure the detection multiplier for BFD control messages. The detection time multiplier, which is the maximum number of consecutive packet losses that the receiver allows the sender to send messages, is used to detect whether the link is normal. Please perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the BFD control message detection multiplier	bfd detect-multiplier *value*	
Restore the default BFD control message detection multiplier	undo bfd detect-multiplier	

[Parameter Description]

value: detection multiplier, the configuration range is 3-50, the default value is 5;

[Example]

! Configure the detection multiplier for BFD control messages on VLAN interface 100 to 10

```
[GPON-vlanInterface-100]bfd detect-multiplier 10
```

43.2.7 Configuring BFD Session Mode

There are two modes, active and passive, before a BFD session is established. If a device is in active mode, it will actively send BFD control messages before the session is established, regardless of whether or not it receives BFD control messages from the peer. If a device is in passive mode, it does not send BFD control messages before the session is established until it receives a BFD control message from the other end. At least one of the two ends of a BFD session must be in active mode for the session to be successfully established.

Please perform the following configurations under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the BFD session mode to active mode	bfd session init-mode active	Default is active mode
Configure the BFD session mode to passive mode	bfd session init-mode passive	

[Parameter Description]

active: active mode;

PASSIVE: Passive mode;

[Example]

! Configure the BFD session mode of VLAN interface 100 to passive mode

[GPON-vlanInterface-100]bfd session init-mode passive

43.2.8 Configuring BFD Detection Mode

The default BFD detection mode of the device is asynchronous mode, which can be configured and modified to query mode. Please perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the BFD detection mode to query mode	bfd demand on	
Restore the default BFD detection mode to asynchronous mode	bfd demand off	

[Parameter Description]

on: configure the detection mode as query mode;

off: Configure the detection mode as asynchronous;

[Example]

! Configure the BFD detection mode for VLAN interface 100 as query mode

[GPON-vlanInterface-100]bfd demand on

43.2.9 Clear BFD session packet statistics

This function mainly clears the statistics of the number of BFD session messages sent and received. Please perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Clear BFD message statistics	clear bfd session statistics	

[Example]

! Clear the send and receive statistics of BFD session messages on VLAN interface 100

[GPON-vlanInterface-100]clear bfd session statistics

43.2.10 BFD Monitoring and Maintenance

You can display BFD-related configuration information in any view.

manipulate	command	clarification
View information on all BFD sessions	display bfd session [verbose]	
View BFD configuration data under each interface	display bfd interface [verbose]	

[Example]

! View BFD session details

[GPON] display bfd session verbose

! View BFD configuration data details under each Layer 3 interface of the BFD

[GPON] display bfd interface verbose

Chapter 44 VRRP Configuration

44.1 Introduction to VRRP

44.1.1 Introduction to VRRP Protocol

In a network based on the TCP/IP protocol, routes must be specified in order to ensure communication between devices that are not directly physically connected. Currently there are two commonly used methods for specifying routes: one is dynamic learning through routing protocols (e.g., internal routing protocols RIP and OSPF); the other is static configuration. In each terminal are running dynamic routing protocols is unrealistic, most of the client operating system platforms do not support dynamic routing protocols, and even if they do, they are subject to management overhead, convergence, security and many other issues. Therefore, it is common to use static routing configuration for terminal IP devices, generally assigning one or more default gateways to terminal devices. The static routing approach simplifies the complexity of network management and reduces the communication overhead of end devices, but it still has a drawback: if the router that serves as the default gateway is damaged, all communication using that gateway for the next hop hosts is bound to be interrupted. Even if multiple default gateways are configured, it is not possible to switch to a new gateway without restarting the end device. The shortcomings of statically specified gateways can be well avoided by using the Virtual Router Redundancy Protocol (VRRP).

44.1.2 VRRP Basic Concepts

There are two important sets of concepts in the VRRP protocol: the VRRP routers and virtual routers, and the master and backup routers.

1. VRRP routers and virtual routers

A VRRP router is a router running VRRP, a physical entity, and a virtual router is created by the VRRP protocol, a logical concept. A group of VRRP routers work together to form a virtual router (also called a backup group). This virtual router appears externally as a logical router with a unique fixed IP address and MAC address.

2. Primary and backup routers

Routers in the same VRRP group have two mutually exclusive roles: a master router and a backup router. there is only one router in a VRRP group in the master role, and there can be one or more routers in the backup role. the VRRP protocol uses a selection policy to choose one router from the group to act as the master, which is responsible for the ARP response and forwarding of IP packets, while other routers in the group are in standby mode as backups. The other routers in the group are on standby as backups. When the master router fails for some reason, the backup router can be upgraded to the master router after a delay of a few seconds. This switchover is very fast and transparent to the end-user system because it does not require any change of IP address or MAC address.

44.2 VRRP Configuration

44.2.1 VRRP Feature Configuration Task List

The list of major VRRP configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Adding or Removing Virtual IP Addresses	compulsory	44.2.2
Setting the priority of a backup group	selectable	44.2.3
Setting the preemption method and delay time for backup groups	selectable	44.2.4
Setting the timer for a backup group	selectable	44.2.5

Configure the monitor interface for the backup group	selectable	44.2.6
VRRP Monitoring and Maintenance	selectable	44.2.7

▪

44.2.2 Add/remove virtual IP addresses

This function refers to assigning a local segment IP address to a virtual device (also known as a backup group) or removing an assigned to a backup group virtual IP address from the virtual address list. Please perform the following configurations under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Adding a virtual IP address	ip vrrp *vrid vip*	
Deleting a virtual IP address	undo ip vrrp *vrid* [*vip*]	

[Parameter Description]

vrid: backup group number, configuration range 1-255;

vip: virtual IP;

The virtual IP address can be an unassigned IP address in the network segment where the backup group is located, or it can be the IP address of an interface belonging to the backup group. However, if this address is an IP address used by the device itself, it can also be configured. In this case, the device is called an IP Address Owner. When the first IP address is assigned to a backup group, the system creates the backup group, and when a virtual IP address is assigned to the backup group later, the system simply adds the address to the list of virtual IP addresses in the backup group. After the last virtual IP address in the backup group is deleted, this backup group will also be deleted at the same time. That is, there is no more backup group on this interface, and all configurations of this backup group are no longer valid.

[Example]

! Configure the VRRP backup group 1 virtual IP address for VLAN interface 100 to 192.168.1.100

```
[GPON-vlanInterface-100]ip vrrp 1 192.168.1.100
```

44.2.3 Configure the priority of the backup group

The status of each device participating in a backup group is determined in VRRP based on priority. the switch with the highest priority in the backup group will become the Master. perform the following configuration in Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring Backup Group Priority	vrrp priority *vrid priority*	
Restore the default backup group priority	undo vrrp priority *vrid*	

[Parameter Description]

vrid: backup group number, configuration range 1-255;

priority: backup group priority, the configuration range is 1-254, and the default priority is 100;

Priority ranges from 0 to 255 (the higher the value the higher the priority) but is configurable from 1 to 254. priority 0 is reserved by the system for special use and 255 is reserved by the system for the IP address owner.

[Example]

! Configure the VRRP backup group 1 priority of VLAN interface 100 to 200

[GPON-vlanInterface-100] vrrp priority 1 200

 Attention:

The IP address owner's backup group priority is not configurable; the priority is always the maximum value of 255.

44.2.4 Configure the preemption method and delay time for backup groups

Once a device in a backup group becomes a Master, as long as it does not fail, other devices will not become Masters even if they are subsequently configured with a higher priority, unless they are set up in a preemptive manner.

If a device is set to preempt, it will become a Master once it realizes that its priority is higher than that of the current Master, and accordingly, the original Master will become a Backup. while setting preemption, you can also set a delay time. In addition, you can also set a delay time, so that the Backup can delay for a period of time to become the Master.

The purpose of setting the delay time is: in a network with unstable performance, if the Backup does not receive the message from the Master on time, it will become the Master (and the reason for the Backup not receiving the message is due to the network congestion, not due to the Master not working properly). Then wait for some time to receive messages from the Master, thus avoiding frequent state transitions. Perform the following configuration under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the backup group for preemption	vrrp preempt *vrid*	Backup groups are preempted by default
Configure the backup group to be non-preemptive	undo vrrp preempt *vrid*	
Configuring the Backup Group Preemption Delay Time	vrrp preempt *vrid* delay *delay*	Delay time configuration range 0-255 seconds, the default delay time is 0 seconds

[Parameter Description]

vrid: backup group number, configuration range 1-255;

delay: preemption delay time, configuration range 0-255 seconds, the default is preemption mode, the default preemption delay time is 0 seconds;

[Example]

! Configure VRRP backup group 1 on VLAN interface 100 to be preempted with a preemption delay of 10 seconds

[GPON-vlanInterface-100] vrrp preempt 1

[GPON-vlanInterface-100] vrrp preempt 1delay 10

44.2.5 Configuring Timers for Backup Groups

The Master device in a VRRP backup group sends VRRP messages at regular intervals (time interval is adver_interval) to notify the devices in the group that it is working properly. If the Backup does not receive VRRP messages from the Master for more than a certain period of time (the interval is master_down_interval), it is considered to be no longer working properly. At the same time it will change its state to Master.

Users can adjust the interval adver_interval for the Master to send VRRP messages by using the command to set the timer. while the interval of master_down_interval for Backup is three times that of adver_interval. Factors such as excessive

network traffic or differences in timers on different devices can cause the master_down_interval to time out abnormally and a state transition to occur. This situation can be solved by extending the interval of the adver_interval and setting the delay time. the time unit of the adver_interval is second. Make the following configurations under Layer 3 interface view.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring the Backup Group Timer	vrrp timer vrid adver-interval	Timer configuration range 1-255 seconds, default is 1 second
Restore default backup group timer	undo vrrp timer *vrid*	

[Parameter Description]

vrid: backup group number, configuration range 1-255;

adver-interval: timer, configuration range 1-255 seconds, default timer is 1 second;

[Example]

! Configure the VRRP backup group 1 timer for VLAN interface 100 to be 5 seconds

```
[GPON-vlanInterface-100] vrrp timer 1 5
```

44.2.6 Configure the monitor interface for the backup group

Users can configure the monitored interface for each backup group. When the monitored interface is in down state, the priority of the backup group will be reduced. You can specify the priority reduction value while configuring the monitor interfaces. Each backup group can be configured with up to 8 monitoring interfaces, and the priority reduction value is 10 by default. when more than one monitored interface is in the down state, the priority reduction value will be cumulative, but the maximum reduction is 1.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the monitor interface and priority reduction for the backup group	vrrp track *vrid* { vlan-if | supervlan-if } *vlan-id* [reduced *priority*]	Reduced priority is configured in the range of 1-254, with a default of 10
Restore default backup group timer	undo vrrp track *vrid* { all | vlan-if | supervlan-if }	When all is selected, all monitored interfaces are deleted.

[Parameter Description]

vrid: backup group number, configuration range 1-255;

vlan-id: vlan-id of the vlan or Supervlan interface;

priority: monitor interface reduced priority, configuration range 1-254, default is 10;

[Example]

! Configure VRRP backup group 1 of VLAN interface 100 to monitor interface 200, lowering the priority to 20

```
[GPON-vlanInterface-100] vrrp track 1 vlan-if 200 reduced 20
```

44.2.7 VRRP Monitoring and Maintenance

VRRP configuration and status information can be viewed at any attempt.

manipulate	command	clarification
View VRRP configuration and status information	display vrrp [vlan-interface | supervlan-interface *vlan-id* [*vrid*]	Displayed information includes: status information of the device, as Master or Backup router, virtual IP configuration, priority configuration, preemption mode and preemption delay time configuration, timer and monitor interface configuration

[Example]

! To view VRRP configuration information for interface 100

[GPON] display vrrp vlan-interface 100

Chapter 45 DLF Message Forwarding Control

45.1 Introduction to DLF Message Forwarding Control

The system supports the DLF message forwarding control function, which is used to restrict the forwarding of unknown unicast and unknown multicast messages. This ensures that such unknown messages are not flooded into the network, which is conducive to optimizing the network environment.

DLF message forwarding control is only for unknown unicast and unknown multicast messages. The unknown unicast control is realized in the inbound direction of the port, that is, after the port disables the DLF message forwarding function, the unknown unicast messages coming in from the port will be discarded and will not be forwarded out from any port.

Unknown multicast message control is based on global control. When the global control is turned on, unknown multicast service messages will be forwarded when they are received; otherwise, when the unknown multicast message forwarding function is turned off, unknown multicast messages will be discarded and not forwarded.

45.2 DLF Message Forwarding Control Configuration

45.2.1 DLF Message Forwarding Control Configuration Task List

The DLF message forwarding control configuration tasks are as follows:

Configuration tasks	clarification	Detailed Configuration
Configure unknown unicast message forwarding control	compulsory	45.2.2
Configure unknown multicast message forwarding control	compulsory	45.2.3
Display the DLF message forwarding control configuration	selectable	45.2.4

45.2.2 Configure unknown unicast message forwarding control

The port is configured with unknown unicast message forwarding control. perform the following configuration under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable unknown unicast message forwarding	dlf-forward unicast	Unknown unicast packet forwarding is enabled on the port by default
Disable unknown unicast message forwarding	undo dlf-forward unicast	

[Example]

! Disable unknown unicast packet forwarding on Ethernet port 1

[GPON-ethernet-0/0/1]undo dlf-forward unicast

45.2.3 Configure unknown multicast message forwarding control

The port is configured with unknown multicast message forwarding control. perform the following configurations in global view.

manipulate	command	clarification

Go to System View	system-view	
Enable unknown multicast message forwarding	dlf-forward multicast	Unknown multicast packet forwarding is enabled on the port by default
Disable unknown multicast message forwarding	undo dlf-forward multicast	

[Example]

! Disable unknown multicast message forwarding

[GPON]undo dlf-forward multicast

45.2.4 Display the DLF message forwarding control configuration

The DLF message forwarding control configuration can be viewed at any attempt.

manipulate	command	clarification
View the unknown multicast message forwarding control configuration	display dlf-forward global	
View unknown unicast message forwarding control configuration	display dlf-forward interface [ethernet *interface-list*]	

[Example]

! View the DLF message forwarding control configuration for Ethernet port 1

[GPON]display dlf-forward interface ethernet 0/0/1

Chapter 46 BPDU message forwarding control

46.1 Introduction to BPDU message forwarding control

The system supports the BPDU message forwarding control function, which is used to control the forwarding or discarding of BPDU messages. When discard BPDU messages is enabled, the device receives BPDU messages and discards them. This function is mainly used to prohibit BPDU messages from flooding the network and optimize the network environment. BPDU message forwarding control, which can be configured on a global and port basis, takes effect only when the function is enabled both globally and on the port.

46.2 BPDU Message Forwarding Control Configuration

46.2.1 BPDU Message Forwarding Control Configuration Task List

The BPDU message forwarding control configuration tasks are as follows:

Configuration tasks	clarification	Detailed Configuration
Configure global BPDU message forwarding control	compulsory	46.2.2
Configure port BPDU message forwarding control	selectable	46.2.3
Display the BPDU message forwarding control configuration	selectable	46.2.4

46.2.2 Configure global BPDU message forwarding control

To configure global BPDU forwarding control, perform the following configuration under system view.

manipulate	command	clarification
Go to System View	system-view	
Enable to discard BPDU messages	bpdu-discard	The drop BPDU message function is not enabled globally by default
Disable dropping of BPDU messages	undo bpdu-discard	

[Example]

! Enable the function of dropping BPDU messages

[GPON]bpdu-discard

46.2.3 Configure port BPDU message forwarding control

To configure global BPDU forwarding control, perform the following configuration under system view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable to discard BPDU messages	bpdu-discard	The default port does not enable the drop BPDU message function
Disable dropping of BPDU messages	undo bpdu-discard	

[Example]

! Enable Ethernet port 1 to drop BPDU messages

[GPON-ethernet-0/0/1]bpdu-discard

46.2.4 Display the BPDU message forwarding control configuration

You can view the BPDU message forwarding control configuration under any attempt.

manipulate	command	clarification
Viewing DLF Message Forwarding Control Configuration	display bpdu-discard interface [ethernet *interface-list*]	

[Example]

! View the BPDU message forwarding control configuration for Ethernet port 1

[GPON]display bpdu-discard interface ethernet 0/0/1

Chapter 47 bpdu-tunnel configuration

47.1 Introduction to bpdu-tunnel

In a VPN network, it is necessary to encapsulate certain protocol messages received at the edge of the service-provider network according to a specific format, so that the internal devices of the SP network can recognize this encapsulation and ensure that the messages penetrate through the SP network unchanged, and on the other side of the SP network the encapsulation will be lifted and the messages will be restored, so that the peer entities connected to the edge of the SP network can communicate normally. The peer entities connected to the edge of the SP network can communicate normally.

47.2 bpdu-tunnel configuration

47.2.1 bpdu-tunnel configuration task list

The bpdu-tunnel configuration task list is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable bpdu-tunnel function	compulsory	47.2.2
Configure bpdu-tunnel discard thresholds	selectable	47.2.3
Display bpdu-tunnel configuration information	selectable	47.2.4

▪

47.2.2 Enable/disable bpdu-tunnel function

Configure which protocol packets need to be tunneled when they enter this port. perform the following configuration under port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable the bpdu-tunnel function of the port and configure the protocols that need to be tunneled	bpdu-tunnel [cdp | pagp | lacp | stp | udld | vtp]	The bpdu-tunnel function is not enabled on the default port
Remove the bpdu-tunnel function from the port.	undo bpdu-tunnel [cdp | pagp | lacp | stp | udld | vtp]	

[Parameter Description]

cdp: Tunnel cdp messages to cisco.

pagp: tunneling of cisco's pagp messages

lacp: tunnel on lacp packets

stp: tunnel on stp packets

udld: Tunnel udld messages for cisco

vtp: tunneling of cisco's vtp packets

[Example]

! Configure tunnel for cdp messages received on Ethernet port 1

```
[GPON-ethernet-0/0/1] bpdu-tunnel cdp
```

47.2.3 Configure the bpdu-tunnel message destination MAC

To configure the destination MAC address of Layer 2 protocol tunnel packets, perform the following configuration under

system view.

manipulate	command	clarification
Go to System View	system-view	
Configure the destination MAC address for bpdu-tunnel messages	bpdu-tunnel dmac *mac-address*	
Restore the destination MAC address of the default bpdu-tunnel message	undo bpdu-tunnel dmac	The default destination MAC address for bpdu-tunnel messages is 01:00:0c:cd:cd:d0

[Parameter Description]

mac-address: destination MAC address of the bpdu-tunnel message;

[Example]

! Configure the destination MAC address for bpdu -tunnel messages to be 01:00:0c:cc:cc:cc

```
[GPON] bpdu-tunnel dmac 01:00:cc:cc:cc:cc
```

47.2.4 Display bpdu -tunnel configuration information

The bpdu -tunnel related configuration information can be viewed at any attempt:

manipulate	command	clarification
Display L2-tunnel configuration information	display bpdu-tunnel interface [ethernet *interface-list*]	

[Example]

! Viewing bpdu-tunnel configuration information for Ethernet port 1

```
[GPON] display bpdu-tunnel interface ethernet 0/0/1
```

Chapter 48 Local-Switch Function

48.1 Local-Switch Function Introduction

The local-switch function is used to enable the local switching feature of an Ethernet port. After the local-switch function is enabled, when a port receives a packet with an unknown destination MAC, such as a broadcast packet, an unknown unicast packet, or an unknown multicast packet, in addition to the normal flooding of the packet to the other ports, the packet will also be sent back a copy of the packet from that packet-receiving port. Unicast packets with a known destination are not affected by this feature and are sent directly to the destination port.

48.2 Local-Switch Function Configuration

48.2.1 Local-Switch Configuration Task List

The list of Local-Switch configuration tasks is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable Local-Switch function	compulsory	48.2.2
Displaying Local-Switch Configuration Information	selectable	48.2.3

48.2.2 Enable/disable Local-Switch function

Please enable/disable the Local-Switch function in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Open the port local-switch function	local-switch	
Disable the port local-switch function	undo local-switch	

[Example]

! Turn on local switching on Ethernet port 1

[GPON-ethernet-0/0/1]local-switch

! Disable local switching on Ethernet port 1

[GPON-ethernet-0/0/1]undo local-switch

48.2.3 Displaying Local-Switch Configuration Information

Local-Switch configuration information can be viewed under any attempt.

manipulate	command	clarification
Viewing Local-Switch Configuration Information	display local-switch interface [ethernet *interface-list*]	

[Example]

! To view the Local-Switch configuration information for Ethernet port 1

[GPON]display local-switch interface ethernet 0/0/1

Chapter 49 Port Utilization Alerts

49.1 Introduction to Port Utilization Alerts

The system can monitor the rate at which a port receives messages, and if it finds that the rate at which a port receives messages exceeds the exceed threshold, it sends a port traffic overload alarm, and the port is in the port traffic overload state. In this state, if the rate at which a port receives messages is found to be lower than the port traffic normal threshold, a port traffic normal alarm is sent. This function enables the system to proactively report to the user the current rate of messages received by the port.

49.2 Port Utilization Alert Configuration

49.2.1 Port Utilization Alert Configuration Task List

The list of major configuration tasks for port utilization is as follows.

Configuration tasks	clarification	Detailed Configuration
Global open/close port utilization alerts	compulsory	49.2.2
Port Enable/Disable Port Utilization Alert	compulsory	49.2.3
Configure the overrun and normal thresholds for port utilization alarms	selectable	49.2.4
Display port utilization alarm configuration information	selectable	49.2.5

▪

49.2.2 Global open/close port utilization alerts

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Enable port utilization alerts	alarm all-packets	On by default
Turn off port utilization alerts	undo alarm all-packets	

[Example]

! Turn on port utilization alerts globally

[GPON]alarm all-packets

49.2.3 Port Enable/Disable Port Utilization Alert

Please make the following configurations in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Enable port utilization alerts	alarm all-packets	On by default
Turn off port utilization alerts	undo alarm all-packets	

[Example]

! Enable port utilization alarm for Ethernet port 1

[GPON-ethernet-0/0/1] alarm all-packets

49.2.4 Configure the overrun and normal thresholds for port utilization alarms

Please make the following configurations in port view.

manipulate	command	clarification
Go to System View	system-view	
Enter port view	interface { { ethernet interface-num } | interface-name }	
Configuring overrun thresholds and normal thresholds	alarm all-packets threshold [exeed *exceed*] [normal *normal*]	
Restore default overrun thresholds and normal thresholds	undo alarm all-packets threshold	

[Parameter Description]

exceed: overrun threshold, the configuration range is 1-1000 for GE ports and 1-10000 for 10GE ports;

normal: normal threshold, the configuration range is 1-1000 for GE ports and 1-10000 for 10GE ports;

Note that the condition of exceed > normal needs to be satisfied. By default, the GE port traffic overrun threshold is 850 Mbps and the normal threshold is 600 Mbps. the 10GE port traffic overrun threshold is 8500 Mbps and the normal threshold is 6000 Mbps.

[Example]

! Configure the port utilization alarm overrun threshold for Ethernet port 1 to be 500 Mbps and the normal threshold to be 300 Mbps

```
[GPON-ethernet-0/0/1]alarm all-packets threshold exceed 500 normal 300
```

49.2.5 Display port utilization alarm configuration information

You can view the port utilization alarm configuration information in any view mode.

manipulate	command	clarification
Display port utilization alarm configuration information	display alarm all-packets [interface [ethernet *interface-list*]]	The display includes global and port utilization alarm switch configuration, as well as overrun and normal threshold configurations

[Example]

! Displays port utilization alarm information for Ethernet port 1

```
[GPON]display alarm all-packets interface ethernet 0/0/1
```

Chapter 50 CPU Utilization Alerts

50.1 Introduction to CPU Utilization Alerts

The system can monitor the CPU utilization and send a CPU busy alarm if the CPU utilization is found to exceed the CPU busy threshold, in which case the CPU is in the busy state. In this state, if the CPU utilization is found to be below the cpu unbusy threshold, a cpu busy alert is sent. This feature allows the system to proactively report the current CPU utilization to the user.

50.2 CPU Utilization Alert Configuration

50.2.1 CPU Utilization Alert Configuration Task List

The list of main configuration tasks for CPU utilization is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable/disable CPU utilization alarm	compulsory	50.2.2
Configuring CPU Utilization Busy Thresholds and Not Busy Thresholds	selectable	50.2.3
Display CPU utilization alert configuration information	selectable	50.2.4

▪

50.2.2 Enable/disable CPU utilization alarm

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Enable CPU utilization alerts	alarm cpu	On by default
Turn off CPU utilization alerts	undo alarm cpu	

[Example]

! Enable CPU utilization alerts

[GPON]alarm cpu

50.2.3 Configuring Busy Thresholds and No-Busy Thresholds for CPU Utilization Alerts

Please make the following configurations under system view.

manipulate	command	clarification
Go to System View	system-view	
Configure busy thresholds and no-busy thresholds	alarm cpu threshold [busy *busy-threshold*] [unbusy *unbusy-threshold*]	
Restore default busy thresholds and no-busy thresholds	undo alarm cpu threshold	

[Parameter Description]

busy-threshold: busy threshold, configuration range 0-100;

unbusy-threshold: unbusy threshold, configuration range 0-100;

Note that the condition busy-threshold > unbusy-threshold needs to be met.

By default, the CPU busy threshold is 90 and the CPU not busy threshold is 60.

[Example]

! Configure the CPU utilization busy threshold to 80 and not busy threshold to 40

[GPON]alarm cpu threshold busy 80 unbusy 40

50.2.4 Display CPU utilization alert configuration information

You can view the CPU utilization alarm configuration information in any view mode.

manipulate	command	clarification
Display CPU utilization alert configuration information	display alarm cpu	

[Example]

! Display CPU utilization alarm messages

[GPON]display alarm cpu

Chapter 51 IS-IS Function Configuration

51.1 IS-IS Functional Overview

IS-IS (Intermediate System-to-Intermediate System) was originally designed by ISO as a dynamic routing protocol for its CLNP (Connection-Less Network Protocol).

In order to provide routing support for IP, the IETF (Internet Engineering Task Force) in RFC1195 on the IS-IS expansion and modification, so that it can be used in both TCP / IP and OSI environment, known as the integrated IS-IS (Integrated IS-IS or Dual IS-IS).

IS-IS belongs to IGP (Interior Gateway Protocol) and is used inside the autonomous system.IS-IS is a link-state protocol that uses SPF (Shortest Path First) algorithm for routing.

51.1.1 basic concept

1. Basic IS-IS routing protocol terminology

IS (Intermediate System): intermediate system. Equivalent to the router in TCP/IP, it is the basic unit for generating and disseminating routing information in the IS-IS protocol. In the following, IS and router have the same meaning.

ES (End System): end system, equivalent to the host system in TCP/IP. Equivalent to the host system in TCP/IP. ES does not participate in the processing of IS-IS routing protocols, and ISO uses the specialized ES-IS protocol to define the communication between the end system and the intermediate system.

RD (Routing Domain): routing domain. Multiple ISs in a routing domain exchange routing information through the same routing protocol.

Area: an area, a subdivision of a routing domain, IS-IS allows the entire routing domain to be divided into multiple areas.

LSDB (Link State DataBase): link state database. The states of all the links in the network form a link state database, and there is at least one LSDB in each IS. ISs use the SPF algorithm to generate their own routes using the LSDB.

LSPDU (Link State Protocol Data Unit): link state protocol data unit, abbreviated as LSP. in IS-IS, each IS generates LSP, which contains all the link state information of this IS.

NPDU (Network Protocol Data Unit): Network Protocol Data Unit is a network layer protocol message in OSI, equivalent to IP message in TCP/IP.

DIS (Designated IS): the Designated Intermediate System elected on the broadcast network, which can also be referred to as the Designated IS.

NSAP (Network Service Access Point): a network service access point, i.e., the address of the network layer in OSI, is used to identify an abstract network service access point and describe the network address structure of the OSI model.

2. IS-IS address structure

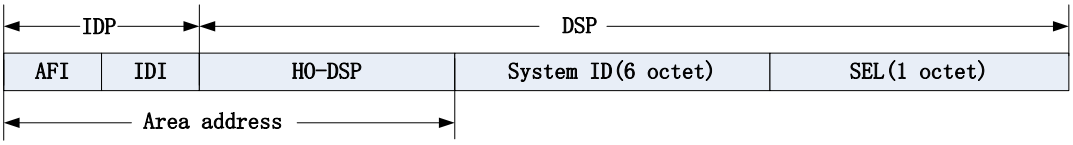
(1) NSAP

As shown in the figure, the NSAP consists of an IDP (Initial Domain Part) and a DSP (Domain Specific Part.) The IDP is equivalent to the primary network number in an IP address, and the DSP is equivalent to the subnet number and host address in an IP address.

The IDP section is defined by ISO and consists of an AFI (Authority and Format Identifier), which indicates the address assignment authority and address format, and an IDI, which identifies the domain.

The DSP consists of three parts: HO-DSP (High Order Part of DSP), SystemID and SEL. HO-DSP is used to partition the area, SystemID is used to distinguish between hosts, and SEL indicates the service type.

Both the IDP and the DSP have variable lengths, with the NSAP total length being a maximum of 20 bytes and a minimum of 8 bytes.



Schematic of the address structure of the Is-is protocol

(2) Regional address

IDPs, along with HO-DSPs in DSPs, are capable of identifying both routing domains and areas within routing domains and are referred to as area addresses. The same area address is not allowed in two different routing domains.

In general, a router needs to be configured with only one area address, and all nodes in the same area should have the same area address. To support smooth merging, splitting, and translation of areas, a router can be configured with up to three area addresses.

(3) System ID

The System ID is used to uniquely identify a host or router within an area. It has a fixed length of 48 bits. In practice, the Router ID is generally used to correspond to the System ID, but it is important to ensure that it uniquely identifies the host or router.

(4) SEL

SEL is sometimes written as N-SEL (NSAP Selector), which is similar to the "protocol identifier" in IP, and corresponds to different SELs for different transport protocols. in IP, SEL is always 00.

(5) Routing method

Because this address structure clearly defines the area, Level-1 routers can easily recognize messages destined for areas other than their own, which are required to be forwarded to Level-1-2 routers.

Level-1 routers use the System ID for intra-area routing and forward the message to the nearest Level-1-2 router if they find that the destination address of the message does not belong to their area.

Level-2 routers perform inter-area routing based on area addresses.

3. NET

NET (Network Entity Title) indicates the network layer information of the IS itself, excluding the transport layer information, and can be regarded as a special class of NSAPs, i.e., NSAP addresses with SEL 0. Therefore, the length of NET is the same as that of NSAPs, which is 8 to 20 bytes. Therefore, the length of NET is the same as that of NSAP, which is 8 to 20 bytes.

NET consists of three parts:

Area ID: It is variable in length from 1 to 13 bytes.

System ID: Used to uniquely identify a host or router within an area, its length is fixed at 6 bytes.

SEL: 0, its length is fixed to 1 byte.

For example, if the NET is: ab.cdef.1234.5678.9abc.00, then the Region ID is ab.cdef, the System ID is 1234.5678.9abc, and the SEL is 00.

Normally, a router can be configured with one NET, but when an area needs to be re-divided, such as merging multiple areas or dividing an area into multiple areas, configuring more than one NET can ensure correct routing when reconfiguring. Since a router can be configured with a maximum of three area addresses, it can only be configured with a maximum of three NETs, and when configuring multiple NETs, you must ensure that they all have the same System ID.

51.1.2 IS-IS region

1. Two-tier structure

To support large-scale routing networks, IS-IS uses a two-level hierarchical structure within the routing domain. A large routing domain is usually divided into multiple areas (Areas). Generally, we deploy Level-1 routers within Areas, Level-2 routers between Areas, and Level-1-2 routers in the middle of Level-1 routers and Level-2 routers.

2. Level-1 and Level-2

(1) Level-1 Router

The Level-1 router is responsible for routing within the area. it forms neighbor relationships only with Level-1 and Level-1-2 routers belonging to the same area. it maintains a Level-1 LSDB that contains routing information for the area. messages to outside the area are forwarded to the nearest Level-1-2 router.

Level-1 routers belonging to different areas cannot form neighbor relationships.

(2) Level-2 Router

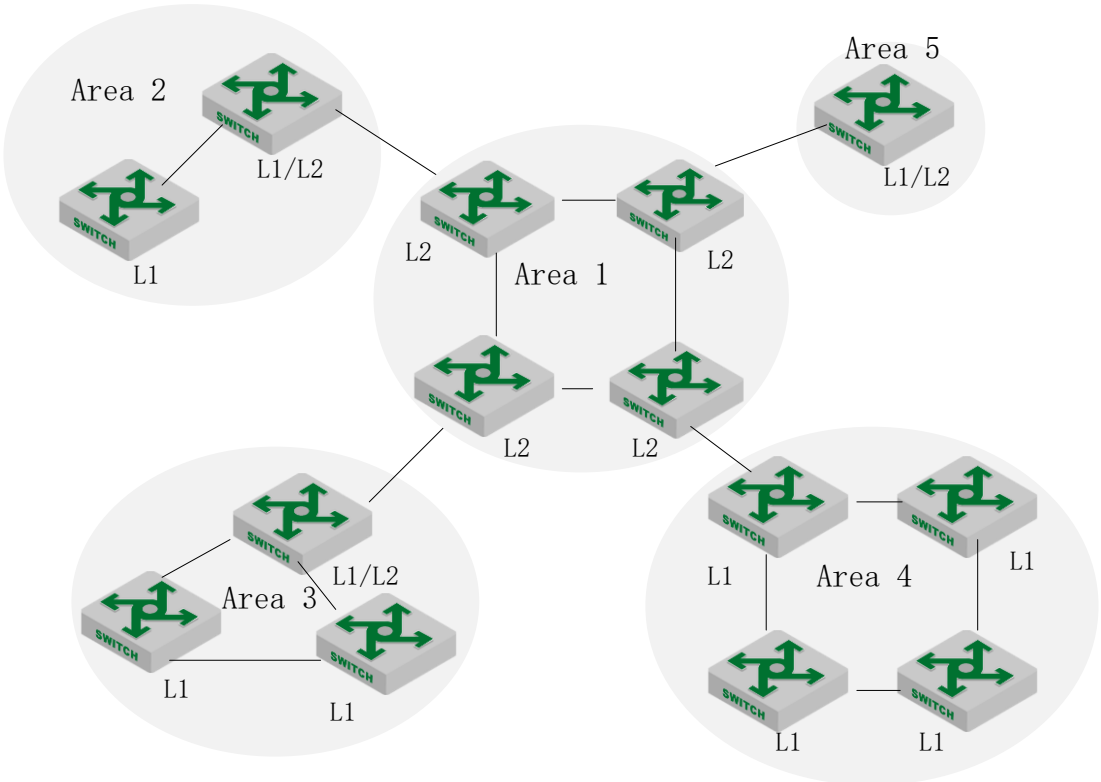
Level-2 routers are responsible for inter-area routing and can form neighbor relationships with Level-2 and Level-1-2 routers in the same area or other areas, maintaining a Level-2 LSDB that contains inter-area routing information. All Level-2 routers and Level-1-2 routers form the backbone of the routing domain and are responsible for communicating between different areas; the backbone must be physically continuous.

Whether Level-2 routers form neighbor relationships is independent of the area.

(3) Level-1-2 Router

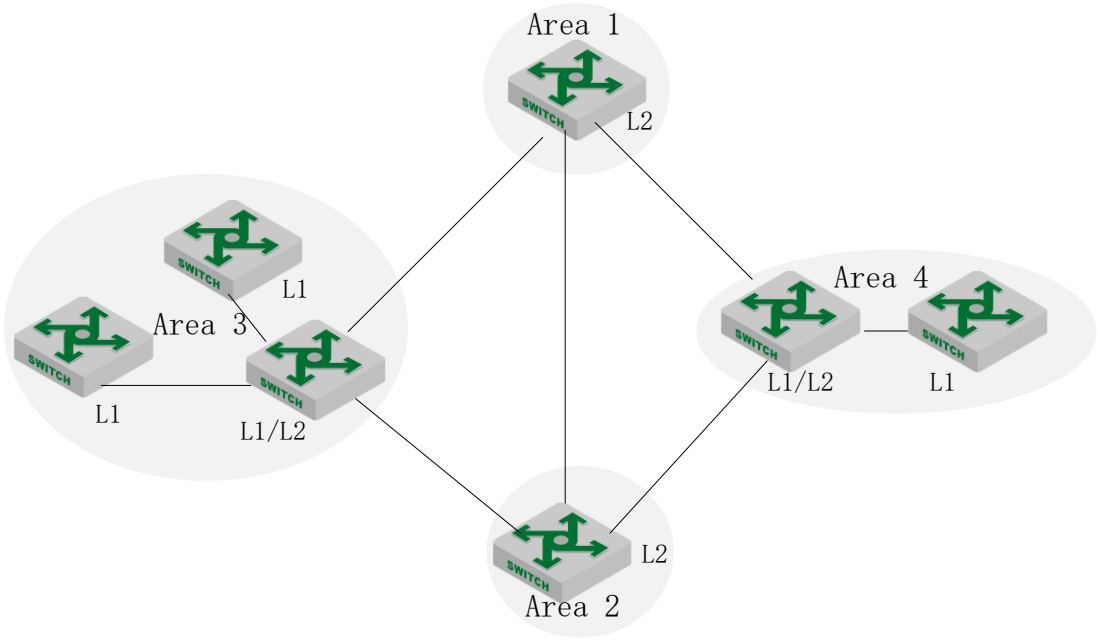
Routers that belong to both Level-1 and Level-2 are called Level-1-2 routers and can form Level-1 neighbor relationships with Level-1 and Level-1-2 routers in the same area, or Level-2 neighbor relationships with Level-2 and Level-1-2 routers in the same or other areas. Level-1 routers must pass through Level-1-2 routers in order to connect to other areas.Level-1-2 routers maintain two LSDBs, Level-1's LSDB for intra-area routing and Level-2's LSDB for inter-area routing.

The following figure shows a network running the IS-IS protocol, where Area 1 is the backbone area and all the routers in this area are Level-2 routers. The other four areas are non-backbone areas, and they are connected to the backbone routers through Level-1-2 routers.



One of the Is-is topology diagrams

The above figure shows another topology diagram of IS-IS. In it, Level-1-2 routers are not only used to connect Level-1 and Level-2 routers, but also form the backbone of IS-IS together with other Level-2 routers. In this topology, there is no specification of which area is the backbone area. All Level-2 routers and Level-1-2 routers make up the IS-IS backbone. they can belong to different areas but must be physically contiguous. the IS-IS backbone does not refer to a specific area.



Is-is topology diagram bis

IS-IS, whether Level-1 or Level-2 routing, uses the SPF algorithm to generate the Shortest Path Tree (SPT), respectively.

3. Routing penetration

Typically, routing within an area is managed through Level-1 routers. All Level-2 routers and Level-1-2 routers form a Level-2 area. Therefore, an IS-IS routing domain can contain multiple Level-1 areas, but only one Level-2 area.

Level-1 areas must be, and can only be, connected to Level-2 areas; different Level-1 areas are not connected to each other.

Routing information in the Level-1 area is advertised to the Level-2 area through the Level-1-2 router; therefore, the Level-2 router knows the routing information of the entire IS-IS routing domain. However, by default, Level-2 routers do not publish routing information that they know about other Level-1 areas and Level-2 areas to the Level-1 area. As a result, the Level-1 router will not know the routing information outside the area, and the Level-1 router only sends the messages to other areas to the nearest Level-1-2 router, so it may not be able to select the best route for the destination address outside the area.

To solve the above problem, IS-IS provides a route penetration feature that enables Level-1-2 routers to publish routing information from other Level-1 areas and Level-2 areas that they know to the specified Level-1 area.

51.1.3 IS-IS network types

1. Types of networks

IS-IS supports only two types of networks, which can be categorized depending on the physical link:

Broadcast links: e.g. Ethernet, Token-Ring, etc.

Point-to-point links: e.g. PPP, HDLC, etc.

2. DIS and pseudo-nodes

In a broadcast network, IS-IS needs to elect one router out of all the routers as the DIS.

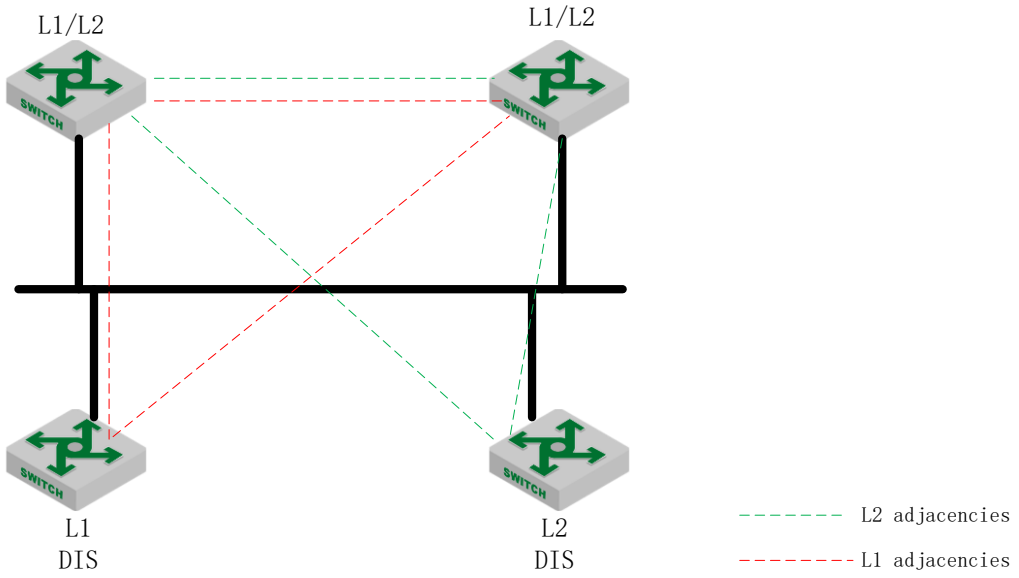
Level-1 and Level-2 DISs are elected separately, and users can set different priorities for DIS elections at different levels. the higher the DIS priority value, the more likely it is to be elected. If there are more than one router with the highest priority, the router with the largest SNPA (Subnetwork Point of Attachment) address (SNPA address in a broadcast network is a MAC address) will be selected. Different levels of DIS can be the same router or different routers.

Differences from OSPF:

The router with priority 0 also participates in the DIS election;

When a new router is added and meets the criteria to become a DIS, this router is selected to become the new DIS and this change causes a new set of LSP floods.

In an IS-IS broadcast network, adjacencies are formed between routers of the same class on the same segment, including all non-DIS routers. As shown in the following figure.



DIS and Neighborhood for Is-is Broadcast Networks

DIS is used to create and update Pseudonodes and is responsible for generating LSPs for Pseudonodes that describe which routers are on this network. A pseudonode is a virtual node used to simulate a broadcast network and is not a real router. In IS-IS, pseudo-nodes are identified with the System ID of the DIS and a one-byte Circuit ID (non-zero value). The use of pseudo-nodes simplifies the network topology and reduces the resource consumption of SPF.

51.1.4 IS-IS messages

1. PDU

IS-IS messages are directly encapsulated in the frame structure of the data link layer.The PDU (Protocol Data Unit) can be divided into two parts, the header and the variable length field part. Among them, the header can be further divided into generic header and specialized header. The generic header is the same for all PDUs, but the specialized header differs according to the PDU type, as shown in the following table:

PDU common header	PDU specific header	Variable length fields (CLV)

PDU message format

typed value	PDU type	acronyms
15	Level -1 LAN IS-IS Hello PDU	L1 LAN IIH
16	Level -2 LAN IS-IS Hello PDUs	L2 LAN IIH
17	Point-to-Point IS	P2P IIH
18	Level -1 Link State PDU	L1 LSP
20	Level -2 Link State PDU	L2 LSP
24	Level-1 Complete Sequence Numbers PDUs	L1 CSNP
25	Level-2 Complete Sequence Numbers PDUs	L2 CSNP
26	Level-1 Partial Sequence Numbers PDUs	L1 PSNP
27	Level-2 Partial Sequence Numbers PDUs	L2 PSNP

PDU Type Correspondence Table

2. Hello messages

Hello messages: used to establish and maintain neighbor relationships, also known as IIH (IS-to-IS Hello PDUs). In this case, Level-1 routers in a broadcast network use Level-1 LAN IIHs, Level-2 routers in a broadcast network use Level-2 LAN IIHs, and routers in a point-to-point network use P2P IIHs.

3. LSP messages

LSP message: used to exchange link status information. there are two types of LSPs: Level-1 LSP and Level-2 LSP. the Level-1 router transmits Level-1 LSP, the Level-2 router transmits Level-2 LSP, and the Level-1-2 router transmits both of the above LSPs.

4. SNP messages

SNPs (Sequence Number PDUs) synchronize the LSDB by describing all or some of the LSPs in the database, thus maintaining the integrity and synchronization of the LSDB.

SNPs include CSNP (Complete SNP, Full Timing Message) and PSNP (Partial SNP, Partial Timing Message), which are further categorized into Level-1 CSNP, Level-2 CSNP, Level-1 PSNP, and Level-2 PSNP.

The CSNP includes summary information about all LSPs in the LSDB so that synchronization of the LSDB can be maintained between neighboring routers. On a broadcast network, the CSNP is sent periodically by DIS (the default sending period is 10 seconds); on a point-to-point link, the CSNP is sent only when the first neighbor relationship is established.

PSNP enumerates only the sequence number of the most recently received LSP or LSPs, and it is capable of acknowledging multiple LSPs at once. PSNP is also used to request neighbors to send new LSPs when LSDBs are found to be out of sync.

5. CLV

The variable length field portion of the PDU is multiple CLV (Code-Length-Value) triples. Its format is shown in the following figure:

	NO of Octets
Code	1
Length	1
Value	Length

CLV format

The CLVs contained in different PDU types are different, as shown in the following table.

CLV Code	name (of a thing)	Type of PDU applied
1	Area Addresses	IIH, LSP
2	IS Neighbors (LSP)	LSP
4	Partition Designated Level-2 IS	L2 LSP
6	IS Neighbors (MAC Address)	LAN IIH
7	IS Neighbors (SNPA Address)	LAN IIH
8	Padding	IIH
9	LSP Entries	SNP
10	Authentication Information	IIH, LSP, SNP
128	IP Internal Reachability Information	LSP
129	Protocols Supported	IIH, LSP
130	IP External Reachability Information	L2 LSP
131	Inter-Domain Routing Protocol Information	L2 LSP
132	IP Interface Address	IIH, LSP

PDU type and contained CLV name

Among them, CLVs with Code values from 1 to 10 are defined in ISO 10589 (there are two categories not listed in the above table), and several other CLVs are defined in RFC 1195.

51.2 IS-IS Function Configuration

51.2.1 IS-IS Feature Configuration Task List

The list of major configuration tasks for the IS-IS feature is as follows.

Configuration tasks	clarification	Detailed Configuration
Enable IS-IS function	compulsory	51.2.2
Configure the Level level of the router and the link adjacency type of the interface	selectable	51.2.3
Configure the interface network type	selectable	51.2.4
Configuring the ISIS Link Overhead Type	selectable	51.2.5
Configuring ISIS Link Overhead	selectable	51.2.6
Configure the Hello message sending interval	selectable	51.2.7
Configure the number of Hello message failures	selectable	51.2.8
Configuring Hello Message Filling	selectable	51.2.9
Configuring the CSNP message sending interval	selectable	51.2.10
Configure the PSNP message sending interval	selectable	51.2.11
Configure the DIS priority of the interface	selectable	51.2.12
Disables the interface from sending and receiving IS-IS messages	selectable	51.2.13
Configuring LSP Parameters	selectable	51.2.14
Configuring SPF Parameters	selectable	51.2.15
Configure the LSDB overload flag bit	selectable	51.2.16
Configuring IS-IS Hostname Mapping	selectable	51.2.17
Configure output switches for neighbor state changes	selectable	51.2.18
Configuring Neighborhood Authentication	selectable	51.2.19
Configuration area validation	selectable	51.2.20
Configuring Routing Domain Authentication	selectable	51.2.21
IS-IS display and maintenance	selectable	51.2.22

▪

51.2.2 Enable IS-IS

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	
Configuring Network Entity Names	net network-entity	
Deleting network entity names	undo net network-entity	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Specify the interface to enable IS-IS	ip router isis	
Specifies that the interface shuts down IS-IS	undo ip router isis	

51.2.3 Configure the Level level of the router and the link adjacency type of the interface

It is recommended that users configure the router type when configuring IS-IS:

If there is only one area, it is recommended that the user set all routers to Level-1 or Level-2, as there is no need for all routers to maintain two identical LSDBs at the same time.

When used in an IP network, it is recommended that all routers be set to Level-2 to facilitate future expansion.

When the router type is Level-1 (Level-2), the link adjacency type of the interface can only be Level-1 (Level-2), and when the router type is Level-1-2, the link adjacency type of the interface is Level-1-2 by default, when the router needs to establish only Level-1 (Level-2) adjacencies with the peer. You can configure the link adjacency type of an interface as Level-1 (Level-2) to limit the adjacencies that can be established on the interface, such as Level-1 interfaces can only establish Level-1 adjacencies, and Level-2 interfaces can only establish Level-2 adjacencies, so that the interface only sends and receives Level-1 (Level-2) type of Hello messages, which reduces the router's processing time and saves bandwidth.

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	
Configure the Level level of the router	is-level { level-1 | level-1-2 | level-2 }	
Restore the Level level of the default router	undo is-level	Default level-1-2
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the link adjacency type of an interface	ip isis circuit-level { level-1 | level-1-2 | level-2 }	
Restore the interface's default link adjacency type	undo ip isis circuit-level	Default level-1-2

51.2.4 Configure the interface network type

The working mechanism is slightly different for different types of interface networks, such as: when the network type is broadcast network, it is necessary to elect DIS and realize LSDB synchronization by flooding CSNP messages; when the network type is P2P, it is not necessary to elect DIS, and the LSDB synchronization mechanism is different.

When only two routers are connected to the same broadcast network, configuring the interface network type as P2P enables IS-IS to operate according to the working mechanism of P2P instead of broadcast network, avoiding DIS election and CSNP flooding, which saves the network bandwidth and accelerates the convergence speed of the network.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the network type of the interface	ip isis network point-to-point	
Restore the default network type of the interface	undo ip isis network point-to-point	Default broadcast type

51.2.5 Configuring the IS-IS Link Overhead Type

For different overhead types, the range of interface overhead values varies, as does the range of received routing overhead values.

narrow Type: interface overhead value ranges from 1 to 63. the maximum value of the received route overhead is 1023.

wide Type: the interface overhead value ranges from 1 to 16777215. when configured to the maximum value of 16777215, the neighbor TLVs generated on the link (with a cost of 16777215) cannot be used for route calculation and are only used to pass TE-related information. The maximum received routing overhead value is 0xFFFFFFFF.

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	
Configuring the type of IS-IS overhead value	metric-style { narrow | transition | wide }	
Configuring the type of IS-IS overhead value	undo metric-style	Default narrow

51.2.6 Configuring IS-IS Link Overhead

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the link overhead of an interface	ip isis metric *metric-value*	
Restore the interface's default link overhead	undo ip isis metric	Default 10

51.2.7 Configure the Hello message sending interval

If a router does not receive a Hello message from a neighboring router within the Neighborhood Hold Time (i.e., the product of the number of Hello message failures and the Hello message sending interval), it will declare a Neighborhood Failure. By setting the number of Hello message failures and the Hello message delivery interval, you can adjust the neighbor relationship hold time, i.e., how long it takes for the neighboring router to be able to monitor that the link has failed and to re-route.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the sending interval for Hello messages	ip isis timer hello-interval *value*	
Restore the default Hello message sending interval	undo ip isis timer hello-interval	Default 3s

51.2.8 Configure the number of Hello message failures

The number of Hello message failures, i.e., the number of neighbor Hello messages that IS-IS did not receive before declaring the neighbor failure.

If a router does not receive a Hello message from a neighboring router within the Neighborhood Hold Time (i.e., the product of the number of Hello message failures and the Hello message sending interval), it will declare a Neighborhood Failure. By setting the number of Hello message failures and the Hello message delivery interval, you can adjust the neighbor relationship hold time, i.e., how long it takes for the neighboring router to be able to monitor that the link has failed and to re-route.

On a broadcast link, Level-1 and Level-2 Hello messages are sent separately, and the number of Hello message failures needs to be set separately; on a point-to-point link, Level-1 and Level-2 Hello messages are sent in the same point-to-point Hello message, so there is no need to specify Level-1 or Level-2.

manipulate	command	clarification
Go to System View	system-view	

Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the number of Hello message failures	ip isis timer hello-multiplier *value*	
Restore the default number of Hello message failures	undo ip isis timer hello-multiplier	Default 10

51.2.9 Configuring Hello Message Filling

The IS-IS protocol message is encapsulated directly behind the link layer header, which cannot realize the automatic fragmentation of the protocol message at the IP layer. Therefore, when the router running IS-IS establishes a neighbor relationship with the router at the opposite end, it sends a Hello message that reaches the MTU size of the link, and the two sides carry out MTU size negotiation to ensure the consistency of the MTUs of the interfaces of the two sides that establish the neighbor relationship to avoid the inconsistency of the MTUs between the two sides that leads to the fact that smaller PDUs can be passed, but larger PDUs cannot be passed.

When both neighboring routers have the same MTU size, in order to avoid wasting bandwidth by sending too large Hello messages, you can configure the interface to send small Hello messages without adding padded CLVs.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring Hello Message Filling	ip isis hello-padding	
Disable Hello message padding	undo ip isis hello-padding	Enabled by default

51.2.10 Configuring the CSNP message sending interval

CSNP messages are messages sent by the DIS (Designated IS) to synchronize the link state database LSDB on a broadcast-type network. If Level-1 or Level-2 is not specified in the command, the default is to set the CSNP message broadcast interval for the level to which the current interface belongs. By default, the interval for sending CSNP messages is 10 seconds.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring the CSNP message sending interval	ip isis timer csnp-interval *value*	
Restore the default CSNP message sending interval	undo ip isis timer csnp-interval	Default 10 seconds

51.2.11 Configure the PSNP message sending interval

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure the PSNP message sending interval	ip isis timer psnp-interval *value*	
Restore the default PSNP message sending interval	undo ip isis timer psnp-interval	Default 2 seconds

51.2.12 Configure the DIS priority of the interface

In a broadcast network, IS-IS needs to elect one router out of all the routers as the DIS.

For IS-IS, Level-1 and Level-2 DISs are elected separately, and different priorities can be set for DIS elections at different levels. The higher the priority value, the more likely it is to be elected. If all routers have the same DIS priority, the router with the largest MAC address will be selected as the DIS.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring DIS Priority	ip isis priority *value*	
Restore the default DIS priority	undo ip isis priority	Default 64

51.2.13 Disables the interface from sending and receiving IS-IS messages

By prohibiting an interface from sending and receiving IS-IS messages, the interface is prohibited from establishing neighbor relationships with adjacent routers, but routing information for the network directly connected to the interface can still be placed in LSPs to be advertised from other interfaces. Since there is no need to establish neighbor relationships, bandwidth and router processing time can be saved, and at the same time, other routers can also know the routing information to the network directly connected to the interface.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	interface { vlan-interface | supervlan-interface } *vlan-id*	
Configure to disable sending and receiving IS-IS messages	ip isis passive	
Disable the prohibition of sending and receiving IS-IS messages.	undo ip isis passive	IS-IS messages are allowed to be sent and received by default.

51.2.14 Configuring LSP Parameters

Each LSP has a maximum survival time, which decreases over time. When the maximum survival time of an LSP is 0, IS-IS initiates the process of removing the expired LSP.

The router must refresh its own generated LSPs at regular intervals to prevent the maximum survival time of the LSPs from decreasing to 0. Additionally, by refreshing the LSPs at regular intervals the LSPs can be synchronized throughout the area. In addition to regular refresh to regenerate LSPs, the router will be triggered to regenerate LSPs when there are changes in the network topology, such as up or down of neighboring routers, changes in the interface Metric value, System ID, or area address, etc. In order to prevent frequent changes in the network topology that lead to frequent regeneration of LSPs, the user can configure the time interval for generating LSPs to suppress excessive bandwidth and router resources caused by frequent changes in the network. In order to prevent frequent changes in the network topology from causing frequent LSP regeneration, users can configure the LSP generation interval to prevent the network from taking up too much bandwidth and router resources due to frequent changes.

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	

Configuring LSP Maximum Survival Time	timer max-lsp-lifetime *value*	
Restore default LSP maximum survival time	undo timer max-lsp-lifetime	Default 1200s
Configuring the LSP Refresh Cycle	timer lsp-refresh-interval *value*	
Restore the default LSP refresh cycle	undo timer lsp-refresh-interval	Default 900s
Configure the LSP regeneration interval	timer lsp-generation-interval *value*	
Restore the default LSP regeneration interval	undo timer lsp-generation-interval	Default 30s

51.2.15 Configuring SPF Parameters

According to the locally maintained LSDB, the router running IS-IS protocol calculates the shortest path tree rooted at itself through the SPF algorithm, and decides the next hop to the destination network based on this shortest path tree. By adjusting the calculation interval of SPF, the excessive bandwidth and router resources that may be consumed by frequent network changes can be suppressed.

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	
Configuring the LSP Transmit Interval	timer spf-interval *value*	
Restore the default LSP sending interval	undo timer spf-interval	Default 1s

51.2.16 Configure the LSDB overload flag bit

By configuring the LSDB overload flag bit, IS-IS will place the OL bit in the LSP messages it sends to notify other routers that there is a problem with the current router and that it cannot perform routing and message forwarding correctly.
When a router running IS-IS is unable to record the complete LSDB due to insufficient memory or other reasons, it will result in miscalculation of the area routes. During the troubleshooting process, you can temporarily isolate the suspected faulty router from the IS-IS network by setting the overload flag bit to facilitate fault localization.

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	
Configuring the Overload Flag Bit	set overload-bit	
Cancel overload flag bit	undo set overload-bit	Close by default

51.2.17 Configuring IS-IS Hostname Mapping

IS-IS uses System ID to uniquely identify a host or router within an area, and the length of System ID is fixed at 6 bytes. The hexadecimal representation of System ID and LSP identifiers is not intuitive or convenient for network administrators to view when checking the status of IS-IS neighbor relationships, IS-IS routing tables, and the contents of the LSDB.
Hostname Mapping provides a service that maps System IDs to hostnames. Routers running IS-IS maintain a table of hostname-to-System ID mappings, which makes using hostnames more intuitive and easier to remember than using System IDs for maintenance and administration and network troubleshooting.
After enabling the dynamic host name mapping function, each router in the IS-IS network only needs to configure its own host name on its own machine, and the configured host name will be published through the dynamic host name CLV, and finally the routers that enable the dynamic host name mapping function in the IS-IS network will collect the mapping

relationship between the System IDs of the other routers and the host name and generate the mapping table.
You can also configure LAN names for DISs in the broadcast network to represent pseudo-nodes in this broadcast network, making it easy for network administrators to determine which DIS generated the LSPs when viewing the LSDB contents.

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	
Enable Dynamic Hostname Mapping	dynamic hostname-mapping	Enabled by default
Turn off dynamic hostname mapping	undo dynamic hostname-mapping	

51.2.18 Configure output switches for neighbor state changes

When the neighbor status output switch is turned on, log messages are generated and sent to the information center of the device when the IS-IS neighbor status changes.

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	
Turn on the output switch for neighbor state change	log-adjacency-changes	
Turn off neighboring state change output switches	undo log-adjacency-changes	Close by default

51.2.19 Configuring Neighborhood Authentication

After neighbor relationship verification is configured, the verification password will be encapsulated in the Hello message according to the set method, and the verification password will be checked on the received Hello message, and the neighbor relationship will be formed only if it passes the check; otherwise, the neighbor relationship will not be formed, which is used to confirm the correctness and validity of the neighbor and to prevent the formation of neighbors with untrustworthy routers.
Both routers must be configured with the same authentication method and authentication password to form a neighbor relationship.

manipulate	command	clarification
Go to System View	system-view	
Enter Layer 3 interface view	Interface { vlan-interface | supervlan-interface } *vlan-id*	
Configuring Neighborhood Authentication Methods and Passwords	ip isis authentication mode { clear | md5 } *password-string*	
Delete Neighborhood Authentication Method and Password	undo ip isis authentication mode	Disable authentication by default

51.2.20 Configuration area validation

Configuring area authentication prevents routing information learned from untrusted routers from being added to the local Level-1 LSDB.
After configuring area authentication, the authentication password will be encapsulated into Level-1 messages (LSP, CSNP, PSNP) as set, and the authentication password will be checked on the received Level-1 messages.
Routers in the same area must be configured with the same authentication method and authentication password.

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	
Configure the region authentication method and authentication password	area authentication mode { clear | md5 } *password-string* [snp { send-only | validate }]	
Turning off regional authentication methods and authentication password	undo area authentication mode	Disable authentication by default

51.2.21 Configuring Routing Domain Authentication

By configuring routing domain validation, you can prevent untrustworthy routing information from being injected into the current routing domain.

After configuring routing domain authentication, the authentication password will be encapsulated into Level-2 messages (LSP, CSNP, PSNP) as set, and the authentication password will be checked on the received Level-2 messages.

All backbone (Level-2) routers must be configured with the same authentication method and authentication password.

manipulate	command	clarification
Go to System View	system-view	
Enter IS-IS configuration mode	router isis	
Configure the routing domain authentication method and authentication password	domain authentication mode { clear | md5 } *password-string* [snp { send-only | validate }]	
Turn off routing domain authentication methods and authentication passwords	undo domain authentication mode	Disable authentication by default

51.2.22 Display and maintenance of IS-IS

manipulate	command	clarification
Viewing IS-IS Interface Configuration Information	display ip isis vlan-interface *vlan-id*	
View basic IS-IS configuration information	display ip isis	
Viewing IS-IS Neighbor Information	display ip isis neighbor	
View IS-IS LSDB Information	display ip isis database [detail | level-1 | level-2]	
Viewing IS-IS Routing Information	display ip route isis	
Viewing Dynamic Hostname Mapping Configuration Information	display ip is hostname-mapping	
View IS-IS LSDB	display ip isis database	

Chapter 52 ERPS configuration

52.1 Introduction to the ERPS protocol

52.1.1 Introduction to the ERRP Protocol

ERPS (Ethernet Ring Protection Switching) is a standard protocol for G.8032 ring network issued by ITU-T. The convergence speed can reach the requirement of telecommunication level reliability, and interoperability can be realized if all the equipments in the ring network support this protocol.

52.1.2 ERPS Basic Concepts

The concepts of the ERPS protocol mainly include ERPS rings, nodes, port roles, and port states.

1. Examples of ERPS

Unlike spanning tree instances, it is similar to the concept of domains in ERRP. A group of devices configured with the same instance ID and control VLAN and connected to each other constitutes an ERPS instance.

2. Control VLAN

The control VLAN is the transmission VLAN for ERPS protocol messages and serves the same purpose as the control VLAN in ERRP. the protocol message carries the TAG corresponding to the control VLAN.

3. RPL

Ring Protection Link (Ring Protection Link), when the ring is in the Idle state, by blocking the forwarding capacity of a port on the link, to achieve the purpose of preventing the generation of network loops.

4. ERPS ring

It consists of a group of Layer 2 switching devices configured with the same control VLAN and interconnected, and is the basic unit of the ERPS protocol.

5. Nodes

Layer 2 switching devices that join an ERPS ring are called nodes. Each node cannot have more than two ports in the same ERPS ring. Nodes are classified into four categories: RPL Owner, Neighbour, Next Neighbour, and Common.

6. Port Roles

The ERPS protocol specifies that there are four main types of port roles: RPL Owner , Neighbour , Next Neighbour and Common port:

1) RPL Owner: An ERPS ring has only one RPL Owner port, which is determined by the user configuration, and prevents loops from being generated in the ERPS ring by blocking the RPL Owner port. A node with an RPL Owner port becomes an RPL Owner node.

2) RPL Neighbour: There is only one RPL Neighbour (neighbor) port for an ERPS ring, which is configured by the user, and it must be the port connecting to the RPL Owner port , which blocks with the RPL Owner port when the network is normal to prevent loops from being generated in the ERPS ring. A node with an RPL Neighbour port becomes an RPL Neighbour node.

3) RPL Next Neighbour: An ERPS ring can have up to two RPL Next Neighbour ports, configured by the user, which must be ports connecting to either the RPL Owner node or the RPL Neighbour node, and the node with the RPL Next Neighbour port becomes the RPL Next Neighbour node.

4) Common: Common ports, ports other than RPL Owner , Neighbour ,Next Neighbour ports are Common ports, if a node has only Common ports, then the node becomes a Common node.

7. Port Status

In the ERPS ring, there are three types of port states that initiate the ERPS protocol.

1) Forwarding: in the Forwarding state, the port forwards user traffic as well as receives/sends R-APS messages, and can also forward R-APS messages from other nodes.

(2) Discarding: In Discarding state, the port can only receive/send R-APS messages and cannot forward R-APS messages

from other nodes.

3) Disable: the state when the port is Linkdown.

8, Wrok Mode: ERPS working mode

There are revertive and non revertive.

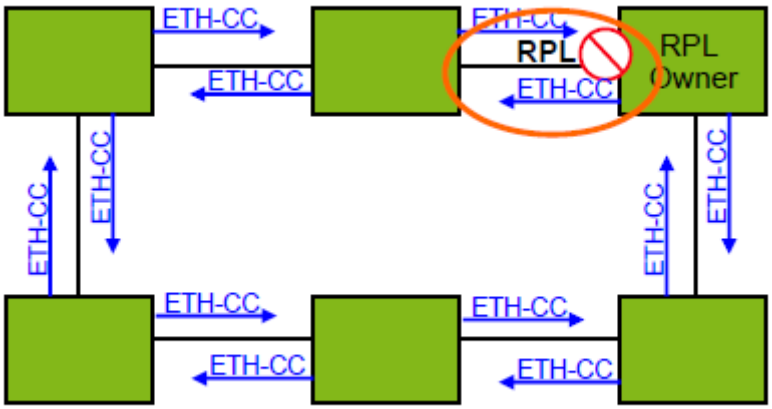
1) REVERTIVE mode, when the link fails, the RPL link is released from protection, and then when the failed link returns to normal, the RPL link is re-protected to prevent loops;

2) non revertive mode, after the fault recovery, the faulty node remains faulty (does not enter the Forwarding), the RPL link is always in the released protection state.

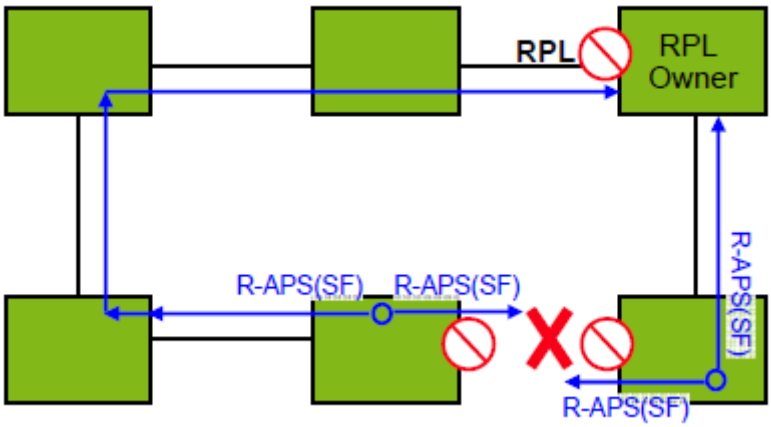
52.1.3 ERPS Ring Protection Mechanism

ERPS uses ETH CFM for link monitoring; when the network is normal, blocking links are set up on the ring network to prevent devices from ringing the network into a ring; when the network fails, the blocking backup links are opened to ensure unimpeded communication between each node. The general process is as follows:

1. As shown in the figure below, when 6 devices are connected into a ring and the link is normal (the ring is IDLE state), the ring is eliminated by setting the RPL link and BLOCKING a port on the ring (RPL Owner port).

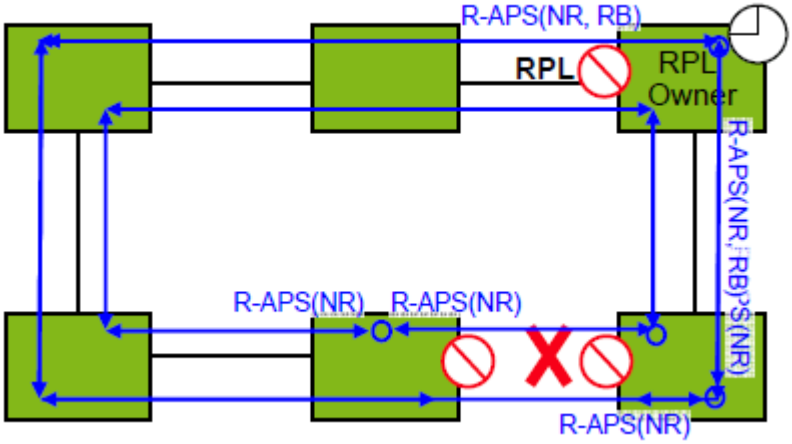


2. When a node on the link is detected to be faulty, immediately block the faulty node port and inform all other devices on the ring of the fault message (R-APS (SF) message), all other nodes receive the message and refresh the FDB table entries, the RPL Owner port receives the fault message, and the port switches to the forwarding state, and the ERPS ring enters into the protection state. As shown in the following figure:



3. As shown in the following figure, when the link of the faulty device is restored, it will send RAPS (NR) message to other devices on the ring to tell them that there is no local request now, and when the RPL Owner receives the message, it will

block out the port again after a period of time and send R-APS (NR, RB) message, and the other nodes will refresh the FDB table entries when they receive the message, and the port blocked out by the faulty node will return to forwarding state, and the ring will become IDLE state again. The port blocked off by the previously failed node will be restored to the forwarding state, and the ring will change to IDLE state again.



52.2 ERPS Functional Configuration

52.2.1 ERPS Function Configuration Task List

Each configuration parameter is valid only when the ERPS protocol is on and the ring is active.

Configuration tasks	clarification	Detailed Configuration
Turn on ERPS	compulsory	52.2.2
Configuring an ERPS Instance	compulsory	52.2.3
Configuring ERPS Link Connectivity Detection	selectable	52.2.4
Configure ERPS-related timers	selectable	52.2.5
ERPS Display and Maintenance	selectable	52.2.6

52.2.2 Enable/disable ERPS function

Please perform ERPS protocol on/off configuration under system view.

manipulate	command	clarification
Go to System View	system-view	
Enable ERRP function	erps	The erps function is disabled by default
Disabling the ERRP function	undo erps	

[Example]

! Enable ERRP function

[GPON]erps

52.2.3 Configuring an ERPS Instance

Please configure it in system view.

manipulate	command	clarification
Go to System View	system-view	
Configuring an erps instance	erps instance *instance-id*	
Configure control-vlan	control-vlan *vlan id*	
Configure work-mode	work-mode { revertive | non revertive }	Default revertive mode
Configure the ring id	ring ring id	
Configuring the ring level	Ring *level*	0 for main ring, 1 for sub ring
Configure the ring port role	{ port0 | port1 } ethernet *interface-num* [neighbor | next-neighbour | owner]	Not specifying a role means that the configuration is common
Configuring a Protected Instance	protected-instance *inst-list*	Configured as a list of instances
Enable/disable ring	ring [enable | disable]	Ring can be enabled only after the port and control VLAN have been configured.

[Note]

The instance configured by protected-instance is the instance number in the corresponding MSTP, which realizes the ring protection function of ERPS for the specified VLAN channel through the instance-VLAN correspondence of MSTP.

Regarding Ring Id: ERPS Ring ID, the last byte of the DMAC in the R-APS message is the Ring Id. from the application in the G.8032 Recommendation. the ERPS Ring ID can be the same, at which point the control VLAN needs to be different and vice versa. The Ring ID for each instance can be any from 1 to 239. the control VLAN is not allowed to be duplicated.

Before configuring an ERPS port, you must disable the Spanning Tree function of the corresponding port, otherwise it cannot be configured.

[Example]

! Configuring an ERPS Instance

```
[GPON]erps instance 1
[GPON-erps-instnace-1] work-mode revertive
[GPON-erps-instnace-1] ring 1
[GPON-erps-instnace-1] ring level 1
[GPON-erps-instnace-1] control-vlan 100
[GPON-erps-instnace-1] port0 ethernet 0/0/2 owner
[GPON-erps-instnace-1] port1 ethernet 0/0/3
[GPON-erps-instnace-1] protected-instance 0
[GPON-erps-instnace-1]ring enable
[GPON-erps-instnace-1]quit
```

52.2.4 Configuring ERPS Link Connectivity Detection

ERPS does not monitor link connectivity in real time like the HELLO message in ERRP , but uses the CC function in ETH CFM to detect the link connectivity between two ports by sending ETH-CC messages between them quickly, so for the ports

in ERPS you also need to configure CFM CC, and you need to configure MEL (MEG Level) in the ERPS instance.) in the ERPS instance, and it needs to be consistent with the configuration in CFM.

For detailed configuration related to CFM, please refer to the configuration guide related to CFM features. Please make the following configuration under system view.

manipulate	command	clarification
Enter global configuration mode	system-view	-
Configure the erps instance and enter instance configuration mode	erps instance *instance-id*	-
Configuring the MEL	mel level	Level range 0~7

[Example]

Configuration example:

[GPON]cfm md format string name test erps level 1

The level configured by cfm here is the MEG Level, and the MEL in ERPS needs to be configured to with the same value.

[GPON]cfm ma format string name test erps primary-vlan 100

The primary-vlan 100 configured by cfm here needs to be the same as the control VLAN of the ERPS.

In addition, in cfm configuration, mep and rmep need to be one-to-one correspondence, not one mep corresponds to multiple rmep.

52.2.5 Configure ERPS-related timers

ERPS has two timers: the WTR timer and the Guard Timer timer:

1.WTR Timer :

When the RPL Owner port is restored to the Forwarding state due to other device or link faults. if the faults are restored and some ports may not have changed from the Down state to the Up state yet. To prevent blocking the RPL Owner port immediately and causing a blocking point oscillation, when the RPL Owner port receives a no-fault RAPS message from a port, start the WTR Timer. if a faulty RAPS message is received from the other port before the timer times out, shut down the WTR Timer. if a faulty RAPS message is never received from the other port before the WTR Timer times out, shut down the WTR Timer. if a faulty RAPS message is never received from the other port before the WTR Timer times out, shut down the WTR Timer. RAPS message, block the RPL Owner port when the WTR Timer times out and send the RPL Blocking RAPS message. The other ports then set the forwarding state of their own ports to Forwarding state after receiving this message.

2. Guard Timer Timer :

The device involved in a link failure or node failure sends a no-fault R-APS message to other devices after the failure is recovered, and at the same time starts the Guard Timer, which does not process RAPS messages until this timer times out, with the purpose of preventing the receipt of expired faulty R-APS messages. If faulty RAPS messages sent by other ports can still be received after the timer times out, the forwarding state of this port changes to Forwarding state.

manipulate	command	clarification
Go to System View	system-view	
Configure the erps instance and enter instance configuration mode	erps instance *instance-id*	compulsory
Configuring the wtr-timer Timer	wtr-timer timer value	Optional, default is 5min, 1~12min
Configuring the guard-timer Timer	guard-timer *timer value*	Optional, default 500ms range

		0~2s

[Example]

! Configuring the ERPS Timer

[GPON-erps-instnace-1] wtr-timer 10

[GPON-erps-instnace-1] guard-timer 600

52.2.6 ERPS Display and Maintenance

manipulate	command	clarification
Display ERPS information	display erps [instance *instance-id*]	
Display control vlan information	display erps control-vlan [*vid*]	
Show incoming and outgoing packets	display erps [instance *instance-id*] statistics	
Clear send/receive packets	clear erps [instance *instance-id*] statistics	

Chapter 53 ONT Discovery Configuration

53.1 ONT Discovery Overview

ONT discovery is the process by which a newly connected or offline ONT accesses the PON.

53.2 ONT Discovery Configuration

53.2.1 ONT Discovery Configuration

ONT auto discovery is used to configure the ONT discovery function of GPON ports, which is enabled by default.

manipulate	command	clarification
Go to System View	system-view	
Configure the ONT discovery distance	ont-autofind distance min *num* max *num* interface gpon { all | *port-num* }	
Enable ONT auto-discovery	ont-autofind interface gpon { all | *port-num* }	
Configure the ONT discovery interval	ont-autofind interval-time *time* interface gpon { all | *port-num* }	
Enable interface ONT auto-discovery aging	ont-autofind list-age interface gpon { all | *port-num* }	
Configuring ONT Auto Discovery Aging Time	ont-autofind list-age time *num* interface gpon { all | *port-num* }	

[Example]

! Enable PON 1-port ONT auto-discovery function

53.2.2 [GPON]ont-autofind interface gpon 2/1

53.2.3 Config success: 1, failed: 0.

53.2.4 ONT Silent Configuration

When ONT authentication fails, it will enter the silent state. The OLT does not process the SN reported by the ONT during the silence cycle, and the function is off by default.

manipulate	command	clarification
Go to System View	system-view	
Enable Authentication Failure ONT Silence Function	ont-silent auth-fail interface gpon { all | *port-num* }	
Configuring the ONT Quiet Time	ont-silent auth-fail time *num* interface gpon { all | *port-num* }	
Enable offline ONT silent function	ont-silent offline interface gpon { all | *port-num* }	
Configuring Offline ONT Quiet Time	ont-silent offline time *num* interface gpon { all | *port-num* }	

[Example]

! Enable PON 1-port offline ONT silence function

[GPON]ont-silent offline interface gpon 2/1

Config success: 1, failed: 0.

Chapter 54 ONT Template Configuration

54.1 ONT Templates Overview

ONT Template Configuration allows for a uniform configuration of ONT. The templates necessary to configure ONT are the four templates VLAN, DBA, LINE, and RULE.

54.2 Alarm Template Configuration

Alarm template is used to configure the alarm threshold of ONT receiving light. After binding the alarm template in the ONT line template, the corresponding alarm will be generated when the ONT receiving light exceeds the range.

manipulate	command	clarification
Go to System View	system-view	
Creating/entering an alarm template	alarm-profile { *index* [name *name*] | name *name* }	
Configure to send optical power alarms	opm tx-threshold high *tx-power* low *tx-power*	
Configuring Received Optical Power Alarms	opm rx-threshold high *rx-power* low *rx-power*	
Delete Optical Power Alarm	undo opm { tx-threshold | rx-threshold }	
Save the alarm configuration	commit	
View alarm template	display alarm-profile { *index* | *name name* }	
View alarm template binding information	display alarm-profile bound-info { all | *index* }	

54.3 DBA Template Configuration

DBA templates are used to configure the uplink dynamic bandwidth, which are TYPE1 (fixed bandwidth), TYPE2 (guaranteed bandwidth), TYPE3 (guaranteed bandwidth + maximum bandwidth), TYPE4 (maximum bandwidth), and TYPE5 (mixed bandwidth), according to the GPON standard.

manipulate	command	clarification
Go to System View	system-view	
Create/access dba templates	dba-profile { *index* [name *name*] | name *name* }	
Configure type 1	type 1 fix *fixed-bw* [method sr]	
Configure type 2	type 2 assured *assured-bw* [method sr]	
Configure type 3	type 3 assured *assured-bw* max *max-bw* [method sr]	
Configure type 4	type 4 max *max-bw* [method sr]	
Configure type 5	type 5 fix *fixed-bw* assured *assured-bw* max *max-bw* [method sr]	
Save dba configuration	commit	
View dba template	display dba-profile { *index* | *name name* }	
View dba template binding information	display dba-profile bound-info { all | *index* }	

[Example]

! Configure the DBA template to have a maximum bandwidth of 100M and save it

[GPON]dba-profile 1

[GPON-dba-profile-1] type 4 max 100000

Input maximum bandwidth 100000 has been adjusted to 100032 kbps.

[GPON-dba-profile-10]commit

54.4 VLAN Template Configuration

VLAN templates are used to configure servicevlan translation rules. the VLAN template needs to be referenced in the line

template or specific template.

manipulate	command	clarification
Go to System View	system-view	
Enter/create vlan template	vlan-profile { *index* [name *name*] | name *name* }	
Configure the vlan to add rules	add inner-vlan *vlan* [*pri*] outer-vlan *vlan* [*pri*]	
Configure default vlan rules	default vlan *vlan* [*pri*]	
Configure vlan conversion rules	translate cvlan *vlan* [*pri*] svlan *vlan* [*pri*]	
Configure vlan conversion and add rules	translate-and-add cvlan *vlan* [*pri*] svlan *vlan* [*pri*] outer-vlan *vlan* [*pri*]	
Save Configuration	commit	
Viewing VLAN Templates	display vlan-profile { *index* | *name name* }	
View VLAN template binding information	display vlan-profile bound-info { all | *index* }	

! Configure the VLAN template, VLAN 10 to VLAN 10 conversion and save the
[GPON]vlan-profile 1
[GPON-vlan-profile-1]translate cvlan 10 svlan 10
[GPON-vlan-profile-1]commit

54.5 Upstream Template Configuration

The Upstream template is used to configure the ONT's upstream stream rate limit. Referencing this template requires that qos-mode be set to gem-car mode in the line template.

manipulate	command	clarification
Go to System View	system-view	
Accessing/creating upstream flow templates	upstream-profile { *index* [name *name*] | name *name* }	
Configure upstream flow rate limiting	upstream car cir *cir* cbs *cbs* pir *pir* pbs *pbs*	
Save Configuration	commit	
View upstream flow templates	display upstream-profile { *index* | *name name* }	
View upstream flow template binding information	display upstream-profile bound-info { all | *index* }	

54.6 Downstream Template Configuration

The Downstream template is used to configure the ONT downstream stream speed limit. Referencing this template requires that qos-mode be set to gem-car mode in the line template.

manipulate	command	clarification
Go to System View	system-view	
Create/enter downstream flow templates	downstream-profile { *index* [name *name*] | name *name* }	
Configuring Downstream Bandwidth Configuration	downstream car cir *cir* cbs *cbs* [pir *pir* pbs *pbs*] [group *gid*]	group:HQoS usage
View downstream template	display downstream-profile { *index* | *name name* }	
View downstream binding information	display downstream-profile bound-info { all | *index* }	

54.7 Multicast Template Configuration

Multicast templates are used to configure controllable multicast corresponding parameters. Multicast group access control

permissions currently support both preview and allow modes.

manipulate	command	clarification
Go to System View	system-view	
Accessing/Configuring Multicast Templates	multicast-profile { *index* [name *name*] | name *name* }	
Configuring Controlled Multicast Allowed Mode	multicast control index *index* permit mcast-ip *ip* [*end-ip* | bandwidth *bandtidth* | port *port* | source-ip *ip* | vlan *vlan*]	
Configuring Controlled Multicast Preview Mode	multicast control index *index* preview mcast-ip *ip* [*end-ip* | bandwidth *bandtidth* | port *port* | source-ip *ip* | vlan *vlan*]	
Configuring Controllable Multicast Parameters	multicast control index *index* preview mcast-ip *ip* [permit-times *num* reset-time *num* time-interval *num* time-once *num*]	
Saving Multicast Templates	commit	
Viewing Multicast Templates	display multicast-profile { *index* | *name name* }	
Viewing Multicast Template Binding Information	display multicast-profile bound-info { all | *index* }	

54.8 Specific template configuration

The specific template is used to configure ONT-specific configurations. when the specific template conflicts with the configurations in the line template, the specific template's configurations take precedence. the SIP, WAN, and WiFi part of the configurations is a private part, and the specific configurations refer to the private document description.

manipulate	command	clarification
Go to System View	system-view	
Create/configure specific templates	specific-profile { *index* [name *name*] | name *name* }	
Binding alarms and multicast templates	bind { alarm-profile | multicast-profile } { *index* [name *name*] | name *name* }	
Configure the ONT description	description *description*	
Configuring gemport	gem *num* tcont *num* [encrypt | priority-queue *queue* | downstream-profile *index* | upstream-profile *index* | vlan-profile *index*]	
Configuring IPhost to dynamically acquire an IP	ip-config mode dhcp vlan *vlan* [*pri*]	
Configuring IPhost Static IP	ip-config mode static ip-address *ip* mask *mask* gateway *gateway* primary-dns *dns1* secondary-dns *dns2* vlan *vlan* [*pri*]	
Configuring the ONT Port Rate	ont neg-mode speed { 10 | 100 | 1000 | auto } duplex { half | full | auto } [port *num*]	
Configure ONT range compensation	ont ranging-balance { increase | decrease } *num*	
Close the ONT CATV port	ont shutdown { *ont-id* catv-port *num* | catv-port *num* | port *num* }	
Configuring CATV Mode	ont catv-agc mode { rf-based | optical-based } { increase | decrease } *num* catv-port num	
Configuring PoE Maximum Power	poe max-power *power* port *num*	
Configuring PoE Priority	poe priority { critical | high | low } port *num*	

Turn off PoE	poe shutdown port *num*	
Configuring SIP Proxy Server IP	sip agent proxy-server ip [outbound-proxy *ip* | registrar-server *ip* | signal-port *port*]	
Configure SIP digit maps	sip digitmap dial-plan-id *id* dial-plan-token *digitmap*	
Configuring SIP Dynamic IP	sip user mode dhcp vlan vlan [*pri*]	
Configuring SIP Static IP	sip user mode static ip-address *ip* mask *mask* gateway *gateway* primary-dns *dns1* secondary-dns *dns2* vlan *vlan* [*pri*]	
Configure SIP accounts and passwords	sip user *user* description *description* name *name* password *password* telno num	
Configure tcont	tcont *num* dba-profile { *num* | name *name* }	
Save Configuration	commit	
View specific template configurations	display specific-profile { *index* | *name name* }	
View template-specific binding information	display specific-profile bound-info { all | *index* }	

54.9 Line Template Configuration

Line templates are used to configure the ONT service flow mapping method, service flow processing policy and other related parameters.

manipulate	command	clarification
Go to System View	system-view	
Create/access line templates	line-profile { *index* [name *name*] | name *name* }	
Configuring the ONT type	model ont-model	mandatory
Configure tcont	tcont *num* dba-profile { *num* | name *name* }	mandatory
Configuring gemport	gem *num* tcont *num* [encrypt | priority-queue *queue* | downstream-profile *index* | upstream-profile *index* | vlan-profile *index*]	mandatory
Configuring the Flow Mapping Mode	mapping mode { port port-priority | port-vlan | port-vlan-priority | priority | vlan | vlan-priority }	Default VLAN-based mapping
Configuring Business Flow Mapping	mapping *index* { vlan *vlan* | priority *pri* | port { eth *eth* | veip | iphost } } gem *index*	mandatory
Configuring Business Flow Processing Policies	port vlan *index* { eth *num* | iphost | ont } { default vlan *num* [*pri*] | transparent | vlan *num* { trunk | q-in-q | translate } [vlan *num* [*pri*] } }	Configuration required for SFU, not required for HGUs
Configuring Downstream Multicast Flow Processing Policies	multicast downstream { tag *num* [port *num* | *pri*] | untag [port *num*] | translate *vlan* [port *num* | *pri*] }	
De-enable ONT multicast fast leave	multicast fast-leave disable [port *num*]	
Configure the ONT multicast learning number	multicast group-limit *num* [port *num*]	
Configuring ONT Multicast	multicast mode { igmp-snooping | olt-control } [port *num*]	

Mode		
Configure upstream multicast stream processing	multicast upstream { tag *num* [port *num* | *pri*] | translate *vlan* [port *num* | *pri*] }	
Enable ONT FEC/Loop Detection	ont { fec | ring check }	
De-enable port isolation	ont port-switch	
Configuring ONT Flow Control	ont flow-control [port *num*]	
Configure the maximum number of MAC learns for ONT	ont mac-address-table max-mac-count *num* [port *num*]	
Close the ONT CATV port	ont shutdown *ont-id* catv-port *num*	
Configuring the Mapping Mode	qos-mode { gem-car | priority-queue }	
Configuring ONT Port Speed Limiting	port *num* egress cir *cir* pir *pir* cbs *cbs* pbs pbs *pbs*	
Binding alarm/multicast templates	bind { alarm-profile | multicast-profile } { *index* | *name* }	
Save Configuration	commit	
View line templates	display line-profile { *index* | *name name* }	
View line template binding information	display line-profile bound-info { all | *index* }	

54.10 Rule Template Configuration

Rule templates are used to configure ONTs to go online, allowing ONTs that match the rules to go online and issuing the corresponding line template configuration. once-on discovery mode indicates that after the template configuration is complete, the ONT must be registered within a specified period of time, and the ONT is not allowed to be authenticated after the timeout period. the activation process of an ONT is controlled by the OLT, and the activation process is roughly as follows:

1. ONT receives the job parameters via the Upstream_Overhead message;
2. ONT adjusts its own parameters (e.g., transmit optical power) according to the received operating parameters;
3. The OLT discovers the serial number of the new ONT through the Serial_Number Acquisition process;
4. The OLT assigns ONT-IDs to all new ONTs;
5. The OLT measures the equalization delay of the new ONT ;
6. The OLT transmits the measured equalization delay to the ONT;
7. ONT adjusts the starting point of sending its uplink frames according to the equalization delay ;

The above activation process is accomplished by interacting with the up and down flags (flags) as well as PLOAM messages.

manipulate	command	clarification
Go to System View	system-view	
Configuring a rule template	rule-profile { *index* [name *name*] | name *name* }	
Configuring LOID Authentication	loid-auth *loid* [checkcode-auth *code*] line-profile *index* [once-on { aging-time time | no-aging }]	
Configuring Password Authentication	password-auth { string *string* | hex *hex* } line-profile *index* [once-on [aging-time time | no-aging]]	
Configuring SN Authentication	sn-auth { string-hex *sn* | hex *hex* } [password-auth { string *string* | hex	

	hex }] line-profile index	
Saving a RULE template	commit	
View RULE templates	display rule-profile { *index* | *name name* }	
View the number of RULE templates	display rule-profile count interface gpon { *port-list* | all }	
View online ONT rule template information	display rule-profile registered { sn { string-hex *sn* | hex *hex* } | loid *loid* | interface gpon { all | *pon-id* } }	
View offline ONT rule template information	display rule-profile unregistered { sn { string-hex *sn* | hex *hex* } | loid *loid* | interface gpon { all | *pon-id* } }	
View ONT rule template information	display rule-profile register-info { sn { string-hex *sn* | hex *hex* } | loid *loid* | interface gpon { all | *pon-id* } }	

Chapter 55 system management

55.1 Overview of system administration

System Management provides common functions for ONT management operations, including ONT restart, upgrade and auto-configuration.

55.2 System Management Configuration

55.2.1 Reboot ONT

ONT restart is used for OLT remote restart of ONT.

manipulate	command	clarification
Go to System View	system-view	
Reboot ONT	ont reboot ont-list	

[Example]

! Reboot ONT 2/2/1

[GPON]ont reboot 2/2/1

Are you sure you want to proceed with the system reboot(y/n)? [n]y

Reboot ONT success: 1, failed :0(Standby-0 Offline-0).

55.2.2 Upgrade ONT

ONT upgrade is used to upgrade ONT software version, before upgrading ONT, you need to upload ONT upgrade file to OLT via tftp or ftp. upgrade ONT version is divided into two modes: immediate and next-startup. immediate means that after the software version is loaded to ONT, ONT will restart automatically and the software version will take effect immediately. Next-startup means that after the software version is loaded into ONT, ONT will not restart automatically, and you need to restart the software version manually for it to take effect.

manipulate	command	clarification
Go to System View	system-view	
Configuration ONT Upgrade	ont upgrade activemode-immediate { *ont-id* | sn { string-hex *sn* | hex *hex* } }	Version effective immediately
Configure ONT upgrade filtering	ont upgrade activemode-immediate { include | exclude } { equipment-id *id* | software-version *version* }	
Configure ONT upgrade time	ont upgrade activemode-immediate timer { *xx:xx:xx* | *xxxx/xx/xx* | interval *num* } { *ont-id* | sn { string-hex *sn* | hex *hex* } }	Version takes effect after next reboot
Configuration ONT Upgrade	ont upgrade activemode-next-stratup { include | exclude } { equipment-id *id* | software-version *version* }	
Configure ONT upgrade time	ont upgrade activemode-next-startup timer { *xx:xx:xx* | *xxxx/xx/xx* | interval *num* } { *ont-id* | sn { string-hex *sn* | hex *hex* } }	
View the ONT upgrade process	display ont upgrade-progress { image | ont-configuration } { *ont-id* | all }	

55.2.3 Activate/Deactivate ONT

ONT activation is used to activate ONTs. by default all ONT IDs are active. After de-activating an online ONT, the ONT is forcibly kicked offline. If the discovery function of the PON port is enabled, you can view the de-activated ONTs in the discovery list.

manipulate	command	clarification
Go to System View	system-view	
Activate ONT	ont active *ont-id*	
Go activate ONT.	ont deactive *ont-id*	

55.2.4 Auto-configuration of ONT

ONT auto-configuration is available when ONTs of the same type are brought online in batches. You need to enable the ONT auto-configuration function first and then configure the auto-configuration parameters. Different types of ONTs can be issued different line template configurations according to the Equipment ID. the OLT enables auto-configuration by default, and when an ONT is accessed, corresponding configurations are automatically issued according to the SFU or HGU type reported by the ONT.

manipulate	command	clarification
Go to System View	system-view	
Enable ONT auto-configuration	ont auto-config	
Configuring ONT Auto Configuration Parameters	ont auto-config { name *name* | *num* } { all-ont | all-sfu | all-hgu | vendor *id* | equipment-id *id* } line-profile { *index* | auto } [interface gpon]	
Configure ONT for flexible configuration parameters	55.2.5 ont auto-config { name *name* | *num* } all-ont smart-match	After the smart-match parameter is configured, the OLT generates a generic template for VLAN 1 and automatically issues the configuration of SFUs or HGUs based on the type of ONT reporting

55.2.6 Reset ONT

This function is used to reset ONT WAN configuration and WIFI configuration, which is a private protocol and requires ONT support.

manipulate	command	clarification
Go to System View	system-view	
Reset ONT WAN Configuration	ont restore-factory wan *ont-id*	
Reset ONT WIFI Configuration	ont restore-factory wifi *ont-id*	

55.3 ONT Log Management

ONT Log Management is used to configure the ONT logging function. ONT logging prefixes and timestamps can be configured.

manipulate	command	clarification
Go to System View	system-view	
Configuring the ONT Log Server IP	ont-logging *ip*	
Enable ONT logging	ont-logging buffer { all | *ont-id* }	
Enable ONT log printing	ont-logging monitor { *num* | all } { all | *ont-id* }	
Configuring the ONT Log Prefix	ont-logging prefix { sn [*ont-id*] | *ont-id* [sn] }	
Configuring the ONT Log Timestamp	ont-logging timestamps { datetime | notime | rfc5424 | uptime }	
View ONT log records	display ont-logging buffer { all | *ont-id* }	
View ONT Log Function	display ont-logging	

55.4 PON protection

OLT supports typeB protection, and in order to improve network reliability and survivability, the optical link protection inversion mechanism can be used in the GPON system. Optical link protection inversion can be performed in the following two ways:

1. Automatic reversal: triggered by fault discovery, such as signal loss or signal degradation;
2. Forced reversal: triggered by a management event.

manipulate	command	clarification
Go to System View	system-view	
Configuring PON Protection Groups	protect-group *index* type-b work interface gpon *pon-port* protect interface gpon pon-port	
Configuration forced inversion	protect-group *index* force-switch	
View PON Protection Configuration	display protect-group { all | *index* }	

Chapter 56 ONT Information View

56.1 ONT Message View Overview

ONT information view includes the view of optical power, port statistics, status and version information.

56.2 View ONT Optical Power

This function is used to view the ONT receiving luminous power.

manipulate	command	clarification
Go to System View	system-view	
View ONT Optical Power	display ont optical-info { *ont-id* | interface gpon { all | *ont-list* } }	

56.3 View ONT traffic statistics

This function is used to view ONT traffic statistics.

manipulate	command	clarification
Go to System View	system-view	
View ONT traffic statistics	display ont statistics performance *ont-id* [port *num*]	
View ONT traffic statistics	display ont statistics *ont-id* [gem { broadcast | multicast | unicast } | port *num* | traffic]	

56.4 Check ONT port status

This function is used to view the status of the ONT voice, CATV and Ethernet ports.

manipulate	command	clarification
Go to System View	system-view	
Checking Voice Port Status	display ont port-status *ont-id* pots-port *num*	
View CATV port status	display ont port-status *ont-id* catv-port *num*	
View Ethernet port status	display ont port-status *ont-id* port *num*	

56.5 View ONT Multicast

This function is used to view the multicast group table entries learned locally by ONT.

manipulate	command	clarification
Go to System View	system-view	
View ONT Multicast	display ont multicast *ont-id* [port *num*]	

56.6 View ONT details

This function can be used to view the details of the ONT.

manipulate	command	clarification
Go to System View	system-view	
View all ONT information	display ont info { *ont-id* | interface gpon { all | *pon-list* } | sn { string-hex *sn* | hex *hex* } }	
View online/offline ONT information	display ont info { online | offline } { *ont-id* | interface gpon { all | *pon-list* } | sn { string-hex *sn* | hex *hex* } }	
View the number of PON port ONTs	display ont info count interface gpon { all | *pon-list* }	
View primary and backup PON port ONT information	display ont info { active | standby } { *ont-id* | interface gpon { all | *pon-list* } | sn { string-hex *sn* | hex *hex* } }	

56.7 View ONT Templates

This function is used to view the template configuration for ONT bindings.

manipulate	command	clarification
Go to System View	system-view	
	display ont profile *ont-id*	

56.8 View ONT description

This function is used to view the description information of the ONT.

manipulate	command	clarification
Go to System View	system-view	
View ONT description	display ont description { *onu-list* | interface gpon { all | *pon-list* } }	

56.9 View ONT Upgrade Status

This function is used to view the upgrade status of the ONT.

manipulate	command	clarification
Go to System View	system-view	
Check ONT upgrade status	display ont upgrade-progress { image | ont-configuration } { *ont-list* | all }	

56.10 View ONT version

This function is used to view the software version of the ONT

manipulate	command	clarification
Go to System View	system-view	
View ONT version	display ont version interface gpon { *pon-list* | all }	

56.11 View ONT MAC

This function is used to view the MAC address table entries learned by the ONT.

manipulate	command	clarification
Go to System View	system-view	
View ONT MAC address	display ont mac-address-table { *mac* | *ont-id* | interface gpon { all | *pon-id* } }	

56.12 View ONT Competency Levels

This function is used to view the capability level information of the ONT.

manipulate	command	clarification
Go to System View	system-view	
View ONT Competency Levels	display ont capability *ont-id*	

56.13 View ONT PoE Features

This function is used to view the power and status of the ONT PoE.

manipulate	command	clarification
Go to System View	system-view	
View PoE power	display ont poe power *ont-id* port *num*	
Check PoE status	display ont poe status *ont-id* port *num*	

56.14 View Rogue ONT Detection

This function is used to view the rogue ONT detection status.

manipulate	command	clarification
Go to System View	system-view	
View rogue ONT detection configuration	display ont anti-rogueont config interface gpon { *pon-list* | all }	